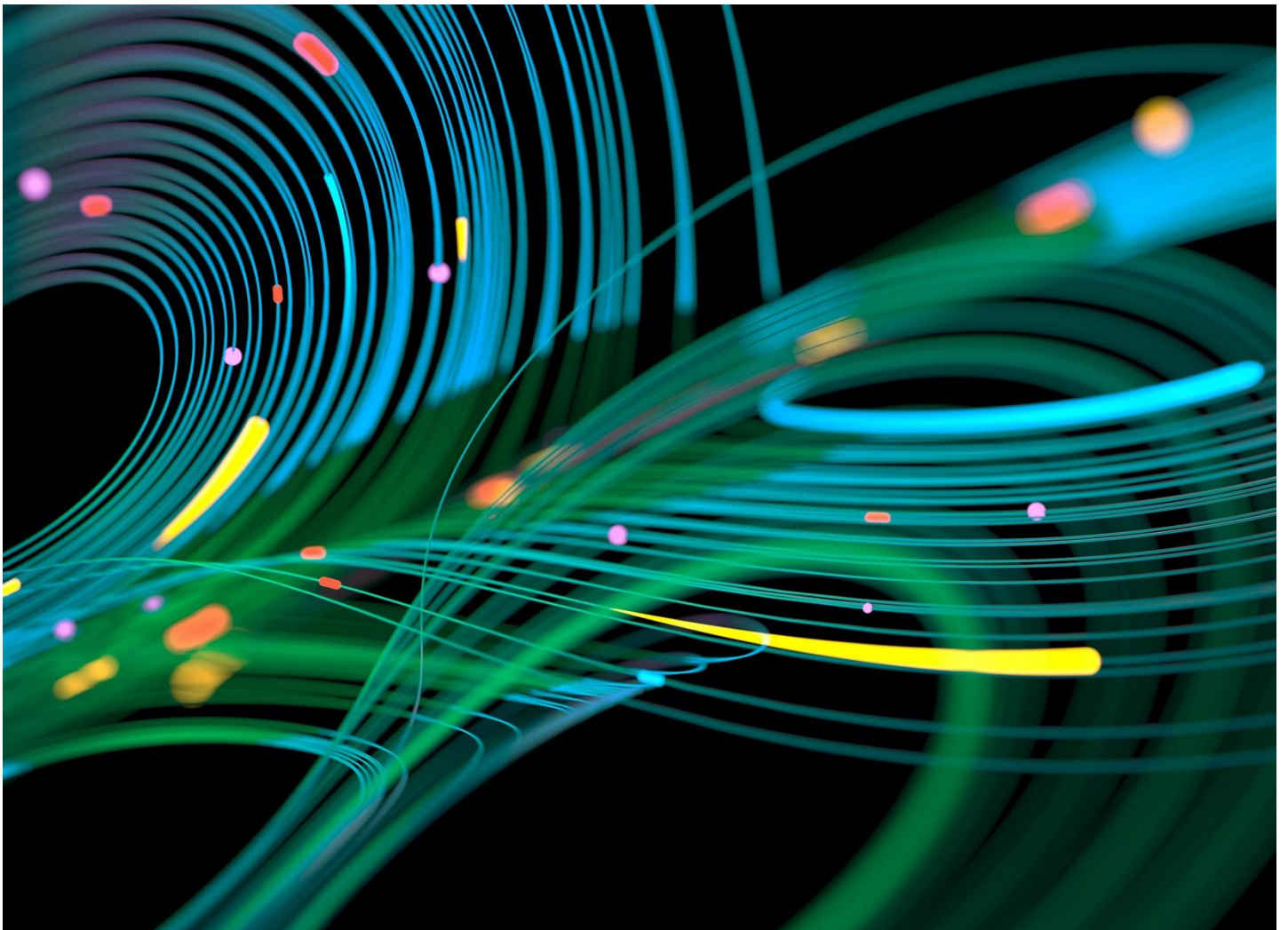


GARRIGUES

Newsletter de Economía del Dato, Privacidad y Ciberseguridad

Abril de 2026

Últimas novedades en derecho digital e innovación tecnológica, con resoluciones recientes y sentencias clave sobre IA, *e-commerce* y normativa tecnológica



El Tribunal Supremo fija el alcance del concepto de “tratamiento” y obliga a cumplir los principios del RGPD desde la solicitud de datos personales



[Álvaro Blanco](#) y [Javier Enebral](#)

El Tribunal Supremo dicta una sentencia clave que sienta doctrina jurisprudencial en relación con el RGPD: la mera solicitud de datos personales constituye "tratamiento" de datos a efectos del RGPD. La sentencia es fruto de un recurso de casación interpuesto por la AEPD bajo la dirección letrada de Garrigues.

La Sala de lo Contencioso-Administrativo del Tribunal Supremo dictó en fecha 26 de marzo de 2026 (notificada el día 21 de abril) una sentencia de especial relevancia en materia de protección de datos personales al pronunciarse, por primera vez en España, sobre el alcance del concepto de "tratamiento" de datos de carácter personal recogido en el artículo 4.2 del Reglamento General de Protección de Datos (RGPD). En este sentido, el Alto Tribunal ha declarado que **el responsable del tratamiento queda sujeto al cumplimiento de los principios reguladores del tratamiento de datos**, incluido el principio de minimización (art. 5.1 c) del RGPD), **desde el mismo momento en que solicita a una persona física la aportación de datos de carácter personal, con independencia de que dichos datos lleguen o no a ser efectivamente facilitados** y ulteriormente recogidos por el responsable del tratamiento.

Antecedentes del caso

El asunto trae causa de un procedimiento sancionador iniciado por la Agencia Española de Protección de Datos (AEPD) contra la Secretaría General de Instituciones Penitenciarias (SGIIPP). Tal como se recoge en los hechos de la sentencia, en 2019 un funcionario del Centro Penitenciario de Lanzarote se ausentó de su puesto de trabajo durante tres días por motivos de salud, presentando el correspondiente justificante médico en el que se indicaba "indisposición". Asimismo, justificó una ausencia parcial posterior con un justificante que acreditaba su asistencia a una consulta médica.

Tras la presentación de dichos justificantes, la Dirección del Centro Penitenciario requirió al funcionario para que aportase el diagnóstico médico concreto y el tratamiento prescrito. El funcionario se negó a facilitar esta información, alegando que su contenido pertenecía a su intimidad personal y no era necesario aportarlo. Como consecuencia de su negativa, se le impusieron sanciones disciplinarias.

La AEPD, tras la instrucción del correspondiente procedimiento sancionador, impuso a la Secretaría General de Instituciones Penitenciarias una sanción de apercibimiento por vulneración del principio de minimización de datos previsto en el artículo 5.1.c) del RGPD, al considerar que la solicitud del diagnóstico médico era excesiva e innecesaria para la finalidad de control del absentismo laboral.

La sentencia de la Audiencia Nacional: la interpretación restrictiva

Frente a la sanción impuesta por la AEPD la SGIIPP formuló recurso contencioso-administrativo ante la Audiencia Nacional, y este tribunal dictó una primera sentencia anulando la sanción impuesta por la AEPD, acogándose a una interpretación formalista y literal del artículo 4.2 del RGPD y considerando que no podía hablarse de "tratamiento" de datos si no hubo en ningún momento una recogida efectiva de los mismos. En su razonamiento, la Sala sostuvo que, dado que el funcionario no llegó a facilitar los datos requeridos, la Administración no pudo iniciar ningún tratamiento y, por tanto, no existía el objeto típico de la infracción respecto del principio de minimización de datos personales.

El recurso de casación y la cuestión de interés casacional

La AEPD recurrió en casación frente a la sentencia de la Audiencia Nacional. La dirección letrada del asunto corrió a cargo, como en la instancia anterior, de profesionales del área de Economía del Dato, Privacidad y Ciberseguridad de Garrigues.

La defensa de la AEPD sostuvo que la interpretación de la Audiencia Nacional era contraria a la doctrina del Tribunal de Justicia de la Unión Europea (TJUE), citando, entre otras, las sentencias de 24 de febrero de 2022 (asunto C-175/20), de 5 de octubre de 2023 (asunto C-659/22) y de 4 de octubre de 2024 (asunto C-548/21). El hilo argumental del recurso giraba en torno a la premisa de que el RGPD exige que cualquier responsable del tratamiento implemente sus procedimientos atendiendo a los principios previstos en el RGPD de manera apriorística y anterior a la manipulación física de cualquier dato personal y que, por tanto, el cumplimiento del RGPD, incluyendo el principio de minimización, se debe producir antes de que el dato sea recibido físicamente por el responsable del tratamiento, en aplicación de los principios de *accountability* (responsabilidad proactiva o rendición de cuentas) y privacidad desde el diseño.

La doctrina fijada por el Tribunal Supremo

En la sentencia aquí comentada, el Tribunal Supremo casa y anula la sentencia de la Audiencia Nacional, realizando los siguientes razonamientos y sentando la siguiente doctrina jurisprudencial:

- **Interpretación amplia y sistemática del artículo 4.2 del RGPD.** La Sala rechaza la interpretación literal y formalista que condicionaba la existencia de un "tratamiento" a la recogida efectiva de los datos. En su lugar, realiza una interpretación sistemática que relaciona la definición del artículo 4.2 con las obligaciones del responsable del tratamiento derivadas de los artículos 5 y 25 del RGPD. El Tribunal concluye que ya existe "tratamiento de datos" en el momento en que la Administración solicita a una persona física la entrega de datos personales, aunque estos no sean finalmente entregados por el interesado, dado el carácter de *numerus apertus* que tiene el listado de actividades descritas en el artículo 4.2 del RGPD como constitutivas de un tratamiento de datos.
- **Protección efectiva de los derechos fundamentales.** El Tribunal Supremo subraya que una protección efectiva de los derechos fundamentales reconocidos en el artículo 8.1 de la Carta de los Derechos Fundamentales de la UE y en el artículo 18 de la Constitución española solo es posible si el tratamiento de datos se entiende ya iniciado cuando se solicita la aportación de datos personales. Condicionar la exigencia del cumplimiento de los principios al momento real de la recepción física de los datos haría difícil la protección de los derechos de los interesados y generaría una incertidumbre incompatible con el principio de seguridad jurídica.
- **Alineación con la jurisprudencia del TJUE.** La sentencia del Tribunal Supremo se alinea expresamente con la doctrina del TJUE, que, en su sentencia de 24 de febrero de 2022 (asunto

C-175/20), ya declaró que el legislador de la Unión quiso dar un "alcance amplio" al concepto de tratamiento, señalando que una solicitud de datos personales por parte de una Administración pública implica un proceso de recogida a efectos del artículo 4.2 del RGPD. Igualmente, invoca la sentencia del TJUE de 5 de octubre de 2023 (asunto C-659/22), que reitera esta interpretación amplia.

Aplicación al caso concreto: vulneración del principio de minimización

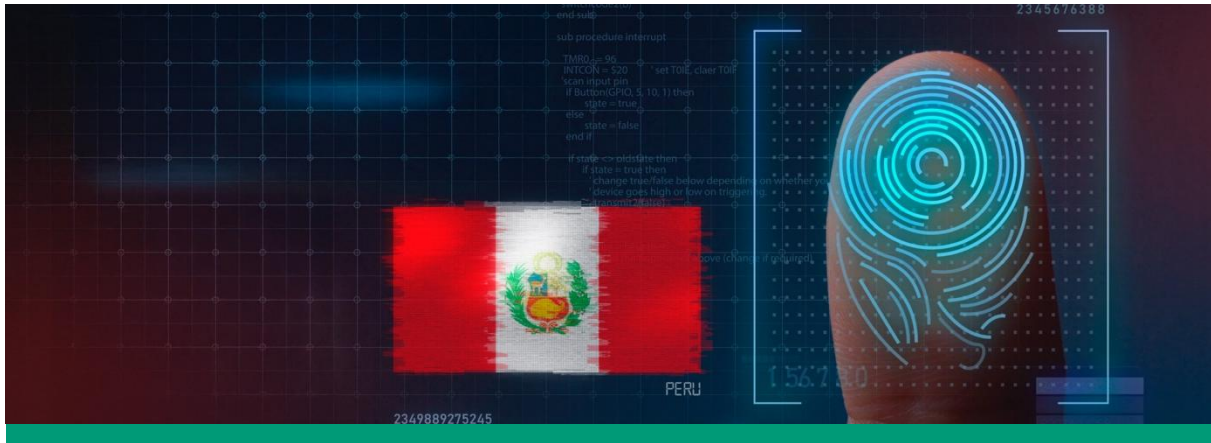
En el caso de referencia, la Sala consideró que el Centro Penitenciario de Lanzarote **vulneró el principio de minimización de datos al solicitar el diagnóstico médico del funcionario, puesto que dicha información no era adecuada, pertinente ni necesaria para el control del absentismo laboral**, que podía ejercerse suficientemente con los justificantes médicos genéricos ya aportados. El Tribunal subrayó que se trataba de datos de salud especialmente protegidos y que, incluso en los supuestos de baja laboral formal, el centro de trabajo no tiene, ni debe tener, acceso al diagnóstico médico del trabajador, pues tanto el INSS como MUFACE excluyen expresamente este dato de los partes comunicados al empleador.

Importancia trascendental del criterio establecido

Esta sentencia constituye un hito en la interpretación del RGPD en España por varios motivos. En primer lugar, porque el Tribunal Supremo sienta por primera vez su criterio jurisprudencial sobre el alcance del concepto de "tratamiento" de datos personales hasta momentos tan iniciales como la propia solicitud, cuestión que hasta ahora no había sido abordada en casación. En segundo lugar, porque alinea la jurisprudencia española con la doctrina que el TJUE venía sosteniendo desde el año 2022 en las sentencias citadas, reforzando la coherencia del sistema de protección de datos en el ámbito europeo. Y, en tercer lugar, porque tiene un impacto práctico de enorme calado: cualquier entidad, pública o privada, que actúe como responsable del tratamiento deberá evaluar el cumplimiento de los principios del RGPD, especialmente el de minimización, antes de formular cualquier solicitud de datos personales y no solo una vez que los datos hayan sido efectivamente recabados.

El criterio sentado por el Tribunal Supremo supone un fortalecimiento del enfoque preventivo y proactivo que inspira el RGPD, reforzando el principio de responsabilidad proactiva (*accountability*) y la protección de datos desde el diseño y por defecto, de modo que las organizaciones están obligadas a diseñar sus procesos de recogida de datos conforme a los principios del reglamento con carácter previo a cualquier actividad de tratamiento.

Evolución de la regulación de datos personales en el Perú: implementación del nuevo reglamento, actuación administrativa y proyecciones normativas



[Franco Muschi](#) y [Mariana Ubidia](#)

La regulación de datos personales en el Perú ha evolucionado con especial dinamismo en los últimos años. Este avance responde tanto al fortalecimiento del marco normativo (impulsado por la entrada en vigencia del nuevo Reglamento de la Ley de Protección de Datos Personales) como a una supervisión cada vez más activa y técnica por parte de la Autoridad Nacional de Protección de Datos Personales. Estas medidas buscan consolidar y modernizar el sistema de protección, reafirmando la protección constitucional que tienen los datos personales en Perú. El resultado es un entorno regulatorio que exige a las entidades públicas y privadas un tratamiento de datos más responsable, seguro y alineado con los estándares internacionales vigentes.

A continuación, presentamos algunos de los avances más significativos en este ámbito.

Marco normativo vigente

Publicación del nuevo Reglamento de Datos Personales

El 30 de noviembre de 2024 se publicó el nuevo Reglamento de la Ley de Protección de Datos Personales (Decreto Supremo No. 016-2024-JUS). Este reglamento entró en vigor el 30 de marzo de 2025, derogando el reglamento anterior, vigente desde el 2013. A continuación, se detallan las principales novedades de la norma:

1. Notificación de incidentes de seguridad

Se establece la obligación de notificar a la Autoridad de Datos Personales dentro de las 48 horas posteriores a la toma de conocimiento del incidente de seguridad. Además, si el incidente afecta directamente al titular de los datos, también se le deberá notificar en el mismo plazo.

Si el incidente ha sido solucionado y/o resuelto internamente, sin que los datos personales hayan sido afectados, la notificación se realiza exclusivamente a la Autoridad de Datos Personales.

Asimismo, se deberá notificar al Centro Nacional de Seguridad Digital cuando el incidente de seguridad se desarrolle en y/o mediante el entorno digital.

Esta obligación es de gran relevancia, dado que, durante el primer semestre de 2025, se registraron más de 748 millones de intentos de ciberataques a nivel nacional.

2. Designación de oficial de datos personales

Se establece la obligación de nombrar un oficial de datos personales (ODP) en las entidades públicas o privadas que manejen grandes volúmenes de datos personales, que puedan impactar a un número significativo de personas o que realicen actividades principales o relacionadas con su negocio que impliquen el tratamiento de datos sensibles.

Esta designación debe formalizarse a nivel interno mediante acuerdo de Directorio y debe comunicarse a la Autoridad de Datos Personales. Además, debe difundirse los datos de contacto del oficial de datos personales en un lugar visible para los titulares de datos en la empresa.

Cabe precisar que la Autoridad de Datos Personales, al cierre de 2025, ha emitido las disposiciones para la designación del ODP, incluyendo exigencias legales que debe seguir el ODP vinculadas con su perfil, experiencia y formación, además de otras precisiones importantes para determinar la aplicación de esta obligación.

La Autoridad ha otorgado un plazo de adecuación de estas nuevas disposiciones hasta junio de 2026.

3. Simplificación del Registro de Banco de Datos Personales

El proceso para inscribir, modificar o cancelar bancos de datos personales ante el registro de la Autoridad de Datos Personales se ha simplificado. En consecuencia, se ha convertido en un procedimiento de aprobación automática sujeto a fiscalización posterior.

Publicación de la metodología para el cálculo de multas en protección de datos personales

El 31 de diciembre de 2025 se publicó la **metodología para el cálculo de multas en protección de datos personales**. Su objetivo es establecer un método claro y objetivo para calcular las multas por infracciones a las normas de protección de datos personales, ya que actualmente se manejan en rangos que representan intervalos amplios para una determinación objetiva. A continuación, a manera de ejemplo, algunas modificaciones en función de las nuevas infracciones incluidas en el nuevo reglamento:

Infracción	Monto propuesto por el proyecto
No comunicar el flujo transfronterizo de datos.	1.08 UIT
Realizar tratamiento de datos personales incumpliendo las medidas de seguridad establecidas, perjudicando al titular del dato o exponiendo sus datos sin su autorización.	7.50 – 37.50 UIT

Infracción	Monto propuesto por el proyecto
Realizar tratamiento de datos personales sensibles incumpliendo las medidas de seguridad establecidas, perjudicando al titular del dato o exponiendo sus datos sin su autorización.	73.33 UIT

Así mismo se establecieron las siguientes modificaciones:

Metodología para el cálculo publicado en 2020	Proyecto de metodología para el cálculo propuesto
Obtendrá un 20% de agravante aquel que cometa una conducta infractora que genere riesgo o daño a más de dos personas o grupo de personas.	Obtendrá un 20% de agravante aquel que cometa una conducta infractora que genere riesgo o daño a más de una persona o grupo de personas.
Obtendrá un 30% de atenuante aquel que realice un reconocimiento de responsabilidad expreso y por escrito de las imputaciones, después de notificado el inicio del procedimiento sancionador.	Obtendrá un 30% de atenuante aquel que realice un reconocimiento de responsabilidad expreso y por escrito de las imputaciones hasta antes del informe final de instrucción.

Actuación de la Autoridad de Protección de Datos Personales: lo que nos dejó el 2025

Sanciones y tendencias en los sectores fiscalizados

Según la Autoridad de Datos Personales, se incrementó el número de sanciones impuestas por el manejo indebido de información personal. A continuación, presentamos las cifras más relevantes al cierre de 2025:

- 11.3 millones de soles en multas por infracciones a la normativa vigente.
- 760 entidades públicas y privadas fueron fiscalizadas, principalmente en los sectores financiero y telecomunicaciones.
- 198 visitas de inspección a nivel nacional.
- 136 nuevos procedimientos administrativos sancionadores.
- 211 resoluciones administrativas en primera y segunda instancia.

Pronunciamientos relevantes: criterios de la Autoridad Nacional de Datos Personales

Las opiniones consultivas emitidas por la Autoridad Nacional de Protección de Datos Personales constituyen pronunciamientos técnicos y no vinculantes que interpretan y aclaran el alcance de la Ley de Protección de Datos Personales y su reglamento, ofreciendo criterios para orientar a entidades públicas y privadas en el cumplimiento de sus obligaciones. En este marco, a continuación presentamos los tres criterios más relevantes emitidos por la ANPD:

¿Quién es el responsable del tratamiento en los servicios públicos concesionados? (Opinión consultiva N° 001-2026-DGTAIPD de febrero de 2026)

Se confirma que la empresa concesionaria, que es quien determina las finalidades, medios y medidas de seguridad del tratamiento, es la responsable del tratamiento de los datos personales de los usuarios en los servicios públicos que ofrece esta concesionaria. En este sentido, cualquier tercero al que se le encargue una operación concreta (e.g. servicios de videovigilancia o soporte) actúa como encargado o, si es subcontratado por este, como subencargado.

Además, aclara que toda puesta a disposición de datos constituye una transferencia, que solo es válida si se encuentra expresamente autorizada por el titular de los datos personales debiendo quedar documentada contractualmente la finalidad, los plazos y las obligaciones, así como las medidas de seguridad y trazabilidad que impidan usos o subtransferencias para fines distintos a los instruidos.

¿Pueden grabarse las sesiones del directorio de una persona jurídica? (Opinión consultiva N° 037-2025-JUS/DGTAIPD de septiembre de 2025)

Esta Opinión establece que la voz de una persona se considera un dato personal que debe analizarse desde dos perspectivas: (i) la información que se transmite a través de ella y (ii) las características físicas asociadas al titular del dato. En cuanto a las grabaciones fonéticas de las sesiones del directorio de una persona jurídica, si estas están reguladas en el estatuto de la entidad, no es necesario obtener el consentimiento de los participantes (directores) para su registro, siempre y cuando se traten asuntos relacionados con la persona jurídica, ya que la persona estaría actuando en su representación.

Una vez cumplida la finalidad de la grabación de una sesión del directorio, cualquier tratamiento posterior de los datos registrados entra dentro del ámbito de la Ley de Protección de Datos Personales, dado que excede el propósito original de la representación de la entidad. El titular de los datos personales tiene derecho a oponerse al tratamiento y a solicitar la cancelación de sus datos, lo cual requerirá una evaluación específica de cada caso en la instancia administrativa correspondiente.

¿Cómo se debe garantizar la veracidad de los datos personales en el tratamiento de información laboral? (Opinión consultiva N° 013-2025-JUS/DGTAIPD de marzo de 2025)

La Opinión establece que los datos contenidos en fuentes accesibles al público deben ser utilizados exclusivamente para los fines para los cuales fueron creados y puestos a disposición. Si se requiere utilizar esos datos para otros fines, será necesario obtener el consentimiento del titular. Los empleadores o potenciales empleadores pueden usar información pública, como noticias o registros públicos, para verificar la veracidad de los datos proporcionados por los postulantes o trabajadores sin necesidad de su consentimiento, siempre que respeten los principios de la LPDP.

Asimismo, reafirma que solo las autoridades con facultades legales pueden tratar datos personales relacionados con infracciones penales o administrativas. Cualquier otra persona o entidad que desee acceder a esa información debe obtener el consentimiento previo, libre e informado del titular. En el caso de los antecedentes penales, policiales o judiciales, la información debe ser solicitada directamente al titular del dato personal.

Agenda 2026

Caso relevante

El inicio del 2026 nos confirma que el sector bancario y financiero será siempre un *target* relevante para la Autoridad Nacional de Datos Personales.

En este sentido, a inicios de año, tres entidades bancarias fueron sancionadas por recolectar, almacenar y utilizar huellas dactilares y minucias biométricas de clientes y no clientes sin consentimiento ni información previa. En esta línea, se comprobó que dichas entidades, pese a contar

con el servicio de verificación biométrica del Registro Nacional de Identificación y Estado Civil (RENIEC), almacenaban adicionalmente los datos biométricos en sus propias bases de datos.

En un primer caso, se impuso una multa de 24,75 UIT (S/ 122,512.50) a una entidad financiera por almacenar las huellas dactilares de una persona sin vínculo contractual con dicha institución, que únicamente acudió a realizar un depósito. Pese a que la entidad utilizaba el servicio de verificación biométrica del RENIEC, conservaba adicionalmente las huellas en sus propios sistemas. La sanción fue confirmada en segunda instancia.

En el segundo caso, otra entidad bancaria recibió una multa de 66 UIT (S/ 326,700.00) al comprobarse que recolectaba huellas dactilares de clientes y no clientes bajo el argumento de validación ante el RENIEC, pero almacenaba las minucias biométricas para un uso adicional no informado a los titulares.

En ambos casos se impusieron multas adicionales de 4,89 UIT y 13,50 UIT, respectivamente, por carecer de políticas de privacidad claras, completas y previas sobre el tratamiento de datos biométricos.

Finalmente, se sancionó a otra institución financiera con 7,5 UIT (S/ 37,125.00) por deficiencias en medidas de seguridad que comprometían la confidencialidad e integridad de la información biométrica de los usuarios.

Datos personales en la Administración Pública hacia 2026: Estrategia Nacional de Gobierno de Datos

A raíz de la digitalización y transformación digital constante, se ha propuesto la Estrategia Nacional de Gobierno de Datos (ENGD), la cual tiene como objetivo mejorar la gestión de los datos públicos en Perú, promoviendo su uso eficiente, accesible y seguro en la administración pública.

Esta estrategia se centra en la gobernanza de datos y la creación de plataformas interconectadas, como DATOS PERÚ, Centro Nacional de Datos y la Plataforma Nacional de Datos Abiertos que faciliten el intercambio de información entre entidades públicas. Además, impulsa la utilización de tecnologías, como la analítica de datos y la inteligencia artificial, para optimizar la toma de decisiones y brindar mejores servicios.

Dicha estrategia vincula al sector privado promoviendo la reutilización económica de los datos públicos, fomentando desafíos de innovación y programas de apoyo empresarial; y garantizando acceso a datos estandarizados. Adicionalmente, propone una interoperabilidad alineada con estándares OCDE, lo que facilita el intercambio seguro entre el Estado y las empresas. j

Además, la estrategia exige construir espacios de datos seguros donde el sector privado participe junto al Estado mediante de los servicios de interoperabilidad y seguridad. También ordena realizar consultas periódicas a empresas para orientar planes de datos abiertos y apoyar iniciativas privadas que usen datos públicos para resolver problemas de política pública.



Actualidad

Dictamen conjunto del Comité Europeo de Protección de Datos y del Supervisor Europeo de Protección de Datos sobre la propuesta de reglamento digital Omnibus para la simplificación del marco regulatorio europeo

El Comité Europeo de Protección de Datos (EDPB) y el Supervisor Europeo de Protección de Datos (EDPS) han elaborado un [dictamen conjunto](#) en respuesta a la propuesta de reglamento denominada “Digital Omnibus”, presentada por la Comisión Europea el 19 de noviembre de 2025. Dicha propuesta legislativa tiene por objeto modificar un amplio conjunto de normas de la Unión Europea en materia digital, entre las que se encuentran el RGPD, la Directiva *ePrivacy*, la Ley de Datos o la Directiva NIS 2, todo ello al objeto de simplificar el marco regulatorio digital de la Unión Europea, reducir la carga administrativa y mejorar la competitividad de las organizaciones europeas.

Así, el EDPB y el EDPS evalúan si la propuesta (i) conduce a una simplificación real y facilita el cumplimiento normativo, (ii) aporta mayor seguridad jurídica y (iii) afecta a los derechos fundamentales de las personas.

En este sentido, se trata de un documento estructurado según secciones en las que se van analizando las modificaciones propuestas con respecto a cada disposición legislativa afectada, formulando recomendaciones específicas en cada materia. De este modo, el EDPB y el EDPS, si bien acogen favorablemente los objetivos de simplificación perseguidos por el Digital Omnibus, advierten sobre la necesidad de garantizar que dichas simplificaciones no menoscaben el elevado

nivel de protección de los derechos y libertades fundamentales de las personas físicas, lamentando, además, que la propuesta no haya sido acompañada de una evaluación de impacto completa.

A este respecto, entre las modificaciones más relevantes contenidas en el Digital Omnibus y abordadas en el dictamen, destacan la modificación de la definición de datos personales (respecto de la cual ambas autoridades expresan serias reservas), la introducción de una definición de investigación científica, nuevas excepciones para el tratamiento de datos biométricos, el uso del interés legítimo en el contexto de la inteligencia artificial, modificaciones en materia de derechos de los interesados (acceso, transparencia y decisiones automatizadas), el régimen de notificación de brechas de seguridad, las evaluaciones de impacto relativas a la protección de datos, la protección de equipos terminales y *cookies*, y diversas disposiciones relativas a la gobernanza y reutilización de datos.

El Consejo de Ministros ha aprobado el anteproyecto de la nueva Ley Orgánica del derecho al honor, a la intimidad personal y familiar y a la propia imagen

Se ha aprobado por el Consejo de Ministros el texto del anteproyecto de la Ley Orgánica de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. Este [anteproyecto](#) sustituye el texto normativo original de 1982, adaptándolo al entorno digital (inteligencia artificial, redes sociales, etc.) y amplía el nivel de protección de estos derechos fundamentales.

El texto propuesto endurece el marco de protección frente a usos no autorizados de la imagen, la voz y otros elementos identificativos, y aborda fenómenos emergentes como los *deepfakes*. El anteproyecto aclara también, en la exposición de motivos, que el hecho de que un ciudadano comparta fotografías o vídeos propios en una red social no autoriza a terceros a reutilizarlos en otros canales o plataformas.

La norma amplía, además, la protección de colectivos especialmente vulnerables. En el caso de los menores, se fija en 16 años la edad mínima para prestar consentimiento válido sobre el uso de su imagen, aunque incluso con consentimiento se considerará ilegítimo si la difusión menoscaba su dignidad o reputación. También se refuerza la protección de las víctimas de delitos, prohibiendo que el autor de los mismos utilice los hechos en perjuicio de la víctima. Asimismo, se prevé la posibilidad de que las personas fallecidas dejen instrucciones para impedir el uso de su imagen o su voz con fines comerciales.

El texto mantiene las excepciones ya reconocidas en la versión actual de la normativa o por la jurisprudencia, especialmente para la libertad de expresión e información. Entre ellas, destaca la posibilidad de utilizar técnicas de inteligencia artificial con fines creativos, satíricos o de ficción cuando afecten a personas con proyección pública, siempre que se identifique claramente el uso de esta tecnología.

Consulta pública sobre el reglamento para la implementación del marco legal de la ciberseguridad en Portugal

El Centro Nacional de Ciberseguridad (CNCS), la autoridad nacional de ciberseguridad de Portugal, ha publicado el proyecto de reglamento de ejecución [del Decreto-Ley nº 125/2025, de 4 de diciembre](#), que aprueba el marco legal para la ciberseguridad (RJC) y traslada la Directiva (UE) 2022/2555 (NIS 2) a la legislación portuguesa.

El reglamento es aplicable a entidades esenciales, importantes y públicas relevantes bajo los términos definidos en el RJC, y densifica las obligaciones ya previstas en dicho diploma, estableciendo normas operativas e instrumentos concretos de cumplimiento.

A continuación, se destacan los principales aspectos del borrador del reglamento:

Plataforma electrónica

Un eje central de la regulación es la creación de una plataforma electrónica gestionada por el CNCS que funcionará como un punto único de registro, cualificación y comunicación entre las entidades cubiertas y las autoridades de ciberseguridad. Esta plataforma será el canal obligatorio para el cumplimiento de varias obligaciones previstas en el RJC, a saber: la autoidentificación y registro de entidades, la notificación de la cualificación de entidades, la comunicación del informe anual, la designación del oficial de ciberseguridad y del punto de contacto permanente, la notificación de incidentes de ciberseguridad y la notificación voluntaria de información relevante, y las notificaciones electrónicas realizadas por las autoridades de ciberseguridad a las entidades.

Marco nacional de referencia de ciberseguridad

El marco nacional de referencia en ciberseguridad (QNRCS), establecido en el anexo I del borrador del reglamento, es la herramienta nacional de referencia para la identificación de normas, estándares y mejores prácticas en ciberseguridad y gestión de la seguridad de la información. De acuerdo con el artículo 14(3) del CJR, será el instrumento de referencia para determinar las medidas de ciberseguridad que adoptarán las entidades cubiertas.

Cabe señalar que el QNRCS y la matriz de riesgos (Anexo II) no están sujetos a consulta pública, por lo que las contribuciones de las partes interesadas se limitarán a los artículos del reglamento y a las medidas contenidas en los anexos III y IV.

Matriz de riesgos y medidas mínimas de ciberseguridad

La regulación define medidas mínimas de ciberseguridad asociadas a tres niveles de cumplimiento - básico, sustancial y alto - determinados por una matriz de riesgo sectorial. Esta matriz, contenida en el anexo II, considera, para cada sector y subsector, la probabilidad e impacto de los escenarios de riesgo dominantes, teniendo en cuenta el tamaño de la entidad (grande, mediana o

pequeña) y la importancia del sector (sectores críticos del anexo I del RJC u otros sectores críticos del anexo II del mismo título).

Los niveles de cumplimiento son acumulativos, por lo que las entidades sujetas al nivel alto también deben cumplir con las medidas previstas para los niveles básico y sustancial. Las medidas mínimas de ciberseguridad se densifican en el anexo III (aplicable a entidades esenciales e importantes) y en el anexo IV (aplicable a entidades públicas relevantes, organizadas en grupo A y grupo B), cubriendo áreas como políticas de ciberseguridad, inventario de activos, gestión de riesgos y vulnerabilidades, gestión de accesos y autenticación multifactor, protección de equipos y red, respaldos, respuesta a incidentes y gestión de la cadena de suministro.

Próximos pasos e implicaciones prácticas

El proyecto de reglamento estuvo en consulta pública hasta el 16 de abril de 2026, con excepción de las disposiciones relativas al QNRCS (anexo I) y a la matriz de riesgo (anexo II). En este momento, el CNCS se encuentra en fase de análisis de las respectivas contribuciones presentadas, y a continuación publicará un informe con un resumen de dichas contribuciones, así como una valoración global sobre las mismas y los fundamentos de las opciones adoptadas en la versión final del reglamento.

El reglamento entrará en vigor al quinto día después de su publicación, sin perjuicio de las disposiciones transitorias previstas en el Decreto-Ley n.º 125/2025.

El reglamento de implementación del RJC es una herramienta clave para la implementación del marco obligatorio de ciberseguridad. Las entidades afectadas deben, a partir de ahora, comenzar el análisis de los requisitos aplicables y preparar los respectivos procesos internos, teniendo en cuenta que algunas obligaciones tendrán periodos de cumplimiento cortos tras la operativización de la plataforma, es decir, la autoidentificación de las entidades, que debe realizarse en un plazo de 60 días.

La AEPD publica una guía sobre el uso de imágenes de terceros en sistemas de inteligencia artificial y sus riesgos

Este [documento](#) analiza los riesgos al subir, transformar o generar contenidos con IA utilizando imágenes de personas, que pueden dividirse entre riesgos visible e invisibles. El texto resulta especialmente útil para realizar análisis de riesgos de sistemas de inteligencia artificial que procesan imágenes de terceros.

Como riesgos visibles identifica aquellos que surgen cuando el contenido generado o modificado se comparte. Entre los factores clave se encuentran la expectativa razonable del uso de la imagen por su titular, la facilidad de difusión en redes o mensajería, la dificultad real de retirar copias y el potencial daño reputacional cuando la imagen atribuye hechos que nunca ocurrieron. Señala especialmente el riesgo elevado vinculado a la generación de contenidos de carácter íntimo o sexualizados, la descontextualización de las imágenes y el uso de imágenes de personas vulnerables, incluidas menores de edad, personas mayores o personas con discapacidad.

En segundo lugar, la AEPD detalla los riesgos menos visibles, que se producen simplemente por cargar una imagen en un sistema de inteligencia artificial. Estos incluyen, entre muchos, la pérdida de control sobre el archivo, la intervención de múltiples actores tecnológicos, la posibilidad de que el proveedor utilice las imágenes con finalidades adicionales o la generación automática de metadatos. También se alerta sobre el riesgo de identificación persistente, la asimetría informativa que dificulta ejercer derechos y la exposición potencial a incidentes de seguridad.

El Consejo General del Poder Judicial aprueba una instrucción sobre el uso de la inteligencia artificial por jueces y magistrados

El 28 de enero de 2026, el Pleno del Consejo General del Poder Judicial (CGPJ) aprobó la [Instrucción 2/2026, sobre la utilización de sistemas de inteligencia artificial en el ejercicio de la actividad jurisdiccional](#) publicada en el BOE el 30 de enero. Su objetivo es establecer

criterios, pautas de uso y principios para la utilización de sistemas de inteligencia artificial (IA) por parte de jueces y magistrados como herramienta de apoyo, garantizando la independencia judicial y los derechos fundamentales, en línea con el Reglamento (UE) 2024/1689 de Inteligencia Artificial (Reglamento de IA).

La instrucción establece nueve principios: control humano efectivo, no sustitución del juez, responsabilidad judicial plena, independencia judicial, respeto a derechos fundamentales, confidencialidad y seguridad, prevención de sesgos algorítmicos, y proporcionalidad y formación continua. Se permite usar IA para la búsqueda de información jurídica, el análisis documental, y clasificación de documentos, la elaboración de esquemas o borradores internos y las tareas organizativas. No obstante, queda prohibido utilizarla para sustituir la toma de decisiones judiciales, incorporar contenidos sin validación crítica o tratar datos especialmente protegidos fuera de los supuestos legalmente autorizados. Solo podrán emplearse sistemas facilitados por las Administraciones competentes o el CGPJ, prohibiéndose los externos salvo para estudio con fuentes abiertas.

Los borradores de resoluciones generados mediante IA requieren revisión y validación crítica del juez o magistrado antes de su validación como resolución judicial o procesal, sin constituir decisiones automatizadas.

El CGPJ supervisará el uso de estos sistemas en lo relativo al tratamiento de datos personales con fines jurisdiccionales y ofrecerá formación especializada. El incumplimiento de la instrucción podrá dar lugar a responsabilidades conforme a la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.

El Consejo de Transparencia y Protección de Datos de Andalucía analiza un sistema de IA para selección de personal

El Consejo andaluz de Transparencia y Protección de Datos ha publicado un [documento técnico](#) en el que analiza la utilización de sistemas de inteligencia artificial para la evaluación de la capacidad profesional en procesos de selección de personal, especialmente en el ámbito público.

El informe aborda, desde una perspectiva práctica, las principales implicaciones del uso de herramientas automatizadas para la valoración de candidaturas, deteniéndose en cuestiones como la determinación de la base jurídica del tratamiento, la posible aplicación del artículo 22 del RGPD, relativo a decisiones individuales automatizadas, y la necesidad de realizar una evaluación de impacto en la protección de datos (EIPD) cuando el sistema pueda generar riesgos elevados para los derechos y libertades de las personas aspirantes.

El documento subraya que, cuando el sistema de IA interviene de forma determinante en la preselección o clasificación de candidaturas, puede estarse ante una decisión automatizada con efectos jurídicos o significativamente similares, lo que exige garantías adicionales, entre ellas el derecho a obtener intervención humana y a impugnar la decisión. Asimismo, analiza las exigencias de transparencia, la minimización de datos y las técnicas de anonimización o seudonimización que podrían aplicarse en fases tempranas del proceso.

El Consejo insiste también en la necesidad de documentar adecuadamente el funcionamiento del algoritmo y de garantizar que no se produzcan sesgos discriminatorios, recordando que la responsabilidad proactiva exige acreditar el cumplimiento normativo antes de la puesta en marcha del sistema.

El Comité Europeo de Protección de Datos alerta a la Comisión Europea de que las nuevas propuestas de modificación del sistema ESTA implican una recopilación desproporcionada de datos de los viajeros europeos

El Comité Europeo de Protección de Datos (CEPD) ha trasladado en [una carta a la Comisión Europea](#) su preocupación ante las propuestas de Estados Unidos para modificar el proceso de solicitud del sistema electrónico de autorización de viaje (ESTA), que permite a los ciudadanos del Espacio Económico Europeo entrar en Estados Unidos sin visado para estancias inferiores a 90 días.

Según el CEPD, las modificaciones previstas representan un cambio sustancial y problemático en el tratamiento de los datos personales de los ciudadanos del EEE, ya que implican la recopilación de un volumen significativamente mayor de información, incluyendo datos especialmente sensibles como la actividad en redes sociales de los últimos cinco años, información de familiares que no guarda relación con el viaje, e incluso, de forma potencial, datos biométricos. El Comité subraya que esta ampliación carece de proporcionalidad y no se ajusta a una necesidad demostrada.

Asimismo, alerta de que la intención de obligar a presentar las solicitudes exclusivamente a través de la aplicación móvil del ESTA reduce la accesibilidad y plantea dudas sobre la transparencia y seguridad del sistema, más aún cuando no se detallan mecanismos efectivos para que los interesados puedan ejercer sus derechos en materia de protección de datos. También señala que no aclara los plazos de conservación ni las condiciones bajo las cuales los datos serán almacenados o utilizados, lo que agrava la falta de garantías disponibles para los ciudadanos europeos y genera incertidumbre sobre el respeto a sus derechos fundamentales derivada de estas propuestas.

El CEPD publica los resultados de la consulta pública sobre plantillas útiles para facilitar el cumplimiento del RGPD por parte de las organizaciones

El Comité Europeo de Protección de Datos ha publicado [un informe sobre los resultados de la consulta pública](#) lanzada entre el 5 de noviembre y el 3 de diciembre de 2025, en la que recabó opiniones sobre qué plantillas podrían facilitar las actividades de cumplimiento del RGPD por parte de las organizaciones. La consulta, dirigida especialmente a las pymes y enmarcada en los compromisos adquiridos en la Declaración de Helsinki para mejorar la claridad, el apoyo y la participación de las partes interesadas, recibió un total de 82 contribuciones procedentes de asociaciones empresariales, delegados de protección de datos, abogados, empresas, autoridades públicas, ONG e instituciones académicas y particulares, de las cuales 71 procedían del EEE y 11 de terceros países. Las plantillas más demandadas por los contribuyentes fueron las

relativas al registro de actividades de tratamiento (RAT), la evaluación de impacto en protección de datos (EIPD), la evaluación del interés legítimo, el aviso o política de privacidad, la evaluación de impacto de las transferencias, el acuerdo de encargo de tratamiento, el formulario de notificación de brechas de seguridad y la evaluación de riesgos de privacidad.

A la vista de las contribuciones recibidas, y teniendo en cuenta que el CEPD ya había decidido trabajar en plantillas para la evaluación de impacto en protección de datos y para las notificaciones de brechas de seguridad, el Comité ha incorporado a su Programa de Trabajo 2026-2027 el desarrollo de tres plantillas adicionales: una plantilla o diagrama de flujo para la evaluación del interés legítimo, una para el registro de actividades de tratamiento y otra de aviso o política de privacidad. El CEPD las desarrollará tomando en consideración las ya disponibles a nivel nacional y armonizándolas, y podría considerar trabajar en plantillas adicionales.

Se aprueba la primera regulación sobre el uso de la inteligencia artificial en el parlamento español

El 16 de febrero de 2026 el Senado aprobó las [Directrices de Uso de Inteligencia Artificial en el Senado](#), estableciendo un marco para el uso responsable, ético y legal de la IA. Su objetivo es mejorar la eficiencia parlamentaria y administrativa, salvaguardando derechos y libertades. Se alinea con el Reglamento (UE) 2024/1689 de Inteligencia Artificial, el RGPD y la LOPDGDD, aplicándose a senadores, personal, grupos parlamentarios y personas en formación. Identifica riesgos para derechos fundamentales (privacidad, sesgos, propiedad intelectual), riesgos operativos, de seguridad, reputacionales y ambientales.

Los principios de actuación incluyen, entre otros: responsabilidad individual en el uso; confiabilidad, robustez y seguridad de los sistemas; respeto a la autonomía humana; transparencia; proporcionalidad y ajuste a las necesidades del Senado; supervisión humana obligatoria; rendición de cuentas, también del proveedor cuando proceda; apertura e interoperabilidad; privacidad; igualdad y no

discriminación; y apertura al avance tecnológico.

En materia de adquisición y despliegue de sistemas de IA, las directrices exigen principalmente: (i) una evaluación previa supervisada por la Comisión de Seguridad de la Información del Senado, (ii) una evaluación de impacto cuando proceda, (iii) documentación técnica detallada, y (iv) la garantía por parte del proveedor del sistema de que la información no pública introducida en el sistema no será utilizada para entrenar ningún modelo.

La Dirección de Tecnologías de la Información y Comunicación es responsable del cumplimiento, en coordinación con el delegado de protección de datos. Existe régimen disciplinario por incumplimientos. La entrada en vigor se produce a los 60 días de su publicación en el BOE y concede un periodo de adaptación de seis meses.

La Comisión Europea abre dos procedimientos para ayudar a Google a cumplir las obligaciones de interoperabilidad e intercambio bajo el Reglamento de Mercados Digitales

La Comisión Europea [ha iniciado](#) dos procedimientos destinados a precisar cómo debe adaptarse Google -designado como "guardián de acceso" conforme al Reglamento de Mercados Digitales (DMA)- a dicho reglamento. Este reglamento establece obligaciones específicas para aquellas plataformas que actúan como intermediarios esenciales entre consumidores y empresas, con el fin de evitar prácticas que puedan limitar la competencia o crear barreras de entrada.

El primer procedimiento se centra en el sistema operativo para dispositivos móviles. La Comisión quiere aclarar cómo debe garantizarse que otros desarrolladores tengan acceso gratuito y efectivo a funcionalidades esenciales del sistema, incluidas aquellas basadas en inteligencia artificial, como los sistemas de generación de contenidos utilizados por la propia plataforma. El objetivo es asegurar que proveedores externos de inteligencia artificial puedan innovar y competir en igualdad de condiciones.

El segundo procedimiento se dirige al servicio de búsqueda. El reglamento exige que los competidores reciban acceso en condiciones justas y no discriminatorias a determinados datos anonimizados relacionados con consultas, clics y visualizaciones. La Comisión evaluará qué información debe incluirse, cómo debe anonimizarse y si proveedores de asistentes conversacionales o sistemas de inteligencia artificial generativa pueden utilizar estos datos para desarrollar alternativas viables.

La Comisión analizará estos aspectos durante los próximos meses, enviará conclusiones preliminares a Google e invitará a terceros a formular observaciones. La apertura de estos procedimientos no implica que exista una infracción, pero tampoco impide que, si finalmente se constata un incumplimiento, la Comisión pueda imponer medidas o sanciones en el futuro.

El Comité Europeo de Protección de Datos y el Supervisor Europeo de Protección de Datos emiten un dictamen conjunto sobre la propuesta de Ley Europea de Biotecnología

El Comité Europeo de Protección de Datos (CEPD) y el Supervisor Europeo de Protección de Datos (SEPD) han adoptado un [dictamen conjunto sobre la propuesta de la Comisión Europea de una Ley Europea de Biotecnología](#), destinada a reforzar los sectores de la biotecnología y la biofabricación en el ámbito sanitario. Ambas instituciones respaldan la creación de una base jurídica única para el tratamiento de datos personales por parte de patrocinadores e investigadores, pero advierten de que la elevada sensibilidad de los datos de salud y genéticos exige garantías reforzadas.

En particular, el dictamen advierte de que las simplificaciones previstas en la propuesta - como la armonización de bases jurídicas, la posibilidad de tratar datos para fines adicionales o la integración de nuevos instrumentos como entornos de prueba regulatorios o el uso de inteligencia artificial en el marco del ensayo- no pueden rebajar los estándares del RGPD. El CEPD y el SEPD recomiendan clarificar las obligaciones de los responsables, limitar los periodos de

conservación, reforzar la seudonimización y garantizar que cualquier acceso por autoridades se limite a lo estrictamente necesario. También solicitan que se definan con mayor precisión los fines del tratamiento y se incorporen salvaguardias adicionales cuando los datos se reutilicen para otros proyectos de investigación.

La Unión Europea y Brasil adoptan decisiones de adecuación mutua que permiten el libre flujo de datos personales

La Comisión Europea ha aprobado una [decisión de adecuación](#) que reconoce que Brasil ofrece un nivel de protección de datos personales equivalente al europeo. Al mismo tiempo, Brasil ha adoptado una decisión recíproca. Este reconocimiento mutuo permite que empresas, administraciones públicas y entidades dedicadas a la investigación intercambien datos personales entre ambas jurisdicciones sin necesidad de garantías adicionales. El objetivo es facilitar un flujo seguro de información y reforzar la confianza en las relaciones económicas y digitales entre ambas regiones.

En conjunto, se crea la mayor zona de transferencia de datos segura del mundo, beneficiando a una población combinada de aproximadamente 670 millones de personas. La aprobación de estas decisiones se enmarca en el contexto del Acuerdo de Asociación entre la Unión Europea y Mercosur y del Acuerdo Comercial Provisional alcanzado recientemente, que busca fortalecer los vínculos económicos y políticos entre ambas regiones. La decisión europea llega tras el dictamen del Comité Europeo de Protección de Datos y la validación de los Estados miembros mediante el procedimiento de comitología.

La Comisión evaluará el funcionamiento práctico de la decisión de adecuación dentro de cuatro años, revisando si se mantienen las garantías necesarias para la protección de los datos personales.

La Comisión Europea designa a WhatsApp como plataforma en línea de muy gran tamaño en virtud de la Ley de Servicios Digitales

La Comisión Europea ha [designado oficialmente](#) a WhatsApp como plataforma en línea de muy gran tamaño según la Ley de Servicios Digitales (DSA). Esta decisión se debe a que su función "Canales" ha superado el umbral de 45 millones de usuarios en la Unión Europea.

Si bien la parte de la aplicación destinada a mensajería privada -los *chats* entre usuarios, notas de voz, fotos, llamadas de voz y vídeo- queda excluida del ámbito de la Ley de Servicios Digitales, la función Canales, que permite difundir información y actualizaciones a una audiencia amplia, sí se considera, en cambio, una plataforma en línea, y, por tanto, está sujeta a las obligaciones de esta ley.

Tras su designación, Meta -la empresa propietaria de WhatsApp- dispone hasta mediados de mayo de 2026 para adaptarse y cumplir con las obligaciones adicionales aplicables a las plataformas de muy gran tamaño. Entre estas obligaciones, se incluye evaluar y reducir riesgos sistémicos, como posibles amenazas a la libertad de expresión, intentos de manipulación electoral, difusión de contenidos ilícitos o problemas de privacidad derivados del uso de la plataforma.

A partir de esta designación, la Comisión Europea será la responsable directa de supervisar el cumplimiento de la Ley de Servicios Digitales por parte de WhatsApp, colaborando con el coordinador irlandés de servicios digitales.

Corea del Sur lanza la primera regulación integral de IA a nivel mundial

En enero [entró en vigor](#) en Corea del Sur el primer conjunto integral de leyes del mundo que regulan la inteligencia artificial, con el objetivo de fortalecer la confianza y la seguridad en el sector.

Con el fin de convertirse en una de las tres principales potencias mundiales en IA, Corea

del Sur espera que su nueva Ley Básica de IA contribuya a posicionar al país como líder en este campo. La legislación en su totalidad ha entrado en vigor antes que la Ley de IA de la UE, que se aplicará por fases hasta 2027.

No obstante, aunque la Ley Básica de IA ya ha entrado en vigor y se ha aplicado, el Gobierno del país asiático ha concedido un periodo de gracia de un año para garantizar o facilitar la

adaptación de esta norma por parte de las empresas y los distintos organismos públicos que deben aplicarla, de manera que, durante esta fase inicial de un año, no llevará a cabo ninguna investigación ni se impondrán sanciones económicas, que, finalizado el plazo, podrán suponer multas de hasta 30 millones de wones surcoreanos.

Resoluciones

La AEPD sanciona a una compañía energética por deficiencias en su protocolo de verificación de identidad de clientes

La AEPD ha impuesto una multa de un millón de euros a una compañía energética por una infracción del artículo 32 del RGPD, relativo a la seguridad del tratamiento de datos personales, ya que carecía de medidas de seguridad adecuadas en su sistema de verificación telefónica de identidad de clientes.

El [procedimiento sancionador](#) se inició a raíz de la reclamación presentada por un cliente, quien denunció que se había vinculado la dirección de correo electrónico de su hija a su contrato de suministro con otra compañía del mismo grupo, sin que ninguno de los dos hubiera facilitado dicho dato ni autorizado tal modificación. Pese a que la reclamada alegó haber efectuado el cambio conforme a su protocolo de verificación de identidad, la investigación de la AEPD evidenció deficiencias significativas en dicho sistema.

La AEPD identificó varios problemas en el protocolo de seguridad de la compañía. En primer lugar, el sistema permitía verificar la identidad del cliente mediante datos que podían ser fácilmente conocidos por terceros, como el nombre completo, el NIF o la dirección postal. En segundo lugar, no existía un registro que garantizara la trazabilidad de los datos aportados durante las verificaciones telefónicas, lo que impedía comprobar con exactitud qué información se había solicitado en cada llamada. En tercer lugar, la selección de los datos a verificar quedaba al arbitrio de cada operador, sin existir un protocolo estandarizado que garantizara un nivel de seguridad homogéneo.

Además de la sanción económica, la resolución ordena a la reclamada adoptar, en un plazo máximo de tres meses, medidas de seguridad técnicas y organizativas adecuadas, incluyendo protocolos que garanticen la verificación de la identidad de los interesados antes de realizar modificaciones en sus contratos.

Un centro sanitario es sancionado por eliminar un CD con resonancias aportadas por un paciente

El paciente que presentó la reclamación ante la AEPD había entregado al centro hospitalario en formato CD unas resonancias magnéticas previamente realizadas, con el fin de que fueran utilizadas como referencia en una nueva prueba diagnóstica. Sin embargo, meses después, al solicitar su recuperación, el centro informó al paciente de que los archivos habían sido eliminados.

La AEPD concluye que estas imágenes constituían documentación clínica a todos los efectos, con independencia de que hubieran sido incorporadas o no a la historia clínica. La Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, obliga a los centros sanitarios a conservar este tipo de documentación durante, al menos, cinco años. Al proceder a su destrucción, el hospital vulneró este deber de custodia, lo que supuso un tratamiento ilícito y sin base legal.

Con base en lo anterior, la [resolución](#) aprecia una triple infracción del RGPD, imponiendo una sanción total de 1.200.000 euros. En primer lugar, declara vulnerado el artículo 9 (categorías especiales de datos) por haber suprimido datos de salud sin concurrir ninguna

de las excepciones que legitimarían su tratamiento, lo que conlleva una sanción de 100.000 euros. En segundo lugar, aprecia una infracción del artículo 6 (licitud del tratamiento), al no disponer el centro de una base jurídica que amparase la eliminación de la documentación clínica, motivando otra multa de 100.000 euros. Por último, se considera vulnerado el artículo 25 (privacidad desde el diseño y por defecto), al no existir un procedimiento adecuado para la gestión de soportes físicos con datos de salud aportados por los pacientes, infracción que se sanciona con 1.000.000 de euros.

La AEPD subraya que este incumplimiento no constituye un incidente aislado, sino que revela una deficiencia estructural en los procedimientos del centro para la gestión, conservación y devolución de la documentación clínica proporcionada por los pacientes.

La AEPD impone una sanción de 500.000 euros a una entidad bancaria por la pérdida de documentación de un cliente

La [resolución](#) se enmarca en un procedimiento sancionador frente a una entidad bancaria, iniciado por la pérdida de la documentación remitida por un cliente para su alta como nuevo interviniente en una cuenta bancaria. Dicha pérdida tuvo lugar a través de un circuito de mensajería contratado por la reclamada. Entre la documentación extraviada se encontraban, entre otros, múltiples datos del reclamante, incluida copia completa de su DNI y del de su pareja. La AEPD considera acreditado que, tras la recogida de la documentación y pese a los avisos del interesado, la entidad reclamada no activó mecanismos eficaces de trazabilidad ni de alerta temprana, limitándose exclusivamente a consultas parciales y tardías, sin identificar al encargado responsable hasta pasados unos meses.

Así, la AEPD aprecia infracción del artículo 32 RGPD, al no haberse implementado medidas técnicas y organizativas adecuadas al riesgo para garantizar la disponibilidad, integridad y confidencialidad de los datos, singularmente en materia de trazabilidad de envíos y sistemas de detección y gestión de brechas, en el marco de la responsabilidad proactiva de los artículos 5.2 y 24 RGPD. Igualmente, la AEPD hace referencia al artículo 28 RGPD en lo relativo a

la selección y control del encargado, sin configurarse como infracción autónoma.

La AEPD destaca la negligencia de la entidad reclamada en el seguimiento del incidente y valora la sensibilidad de algunos de los datos afectados (DNI y cuenta bancaria), imponiendo una sanción de 500.000 euros. El procedimiento termina por pago voluntario de la entidad reclamada, con reducción del importe a 400.000 euros, deviniendo firme la resolución.

La CNIL sanciona con 42 millones de euros a un grupo de telecomunicaciones a causa de una brecha de seguridad

La autoridad francesa de protección de datos (CNIL) ha impuesto dos sanciones que ascienden a 42 millones de euros a dos entidades pertenecientes a un mismo grupo del sector de las telecomunicaciones, tras acreditarse una brecha de seguridad que permitió a un atacante acceder a información de más de 24 millones de contratos de abonados. Entre los datos comprometidos figuraban identificadores bancarios, especialmente sensibles por su carácter personal y por los riesgos asociados a un uso fraudulento.

El [análisis de la autoridad](#) reveló varios incumplimientos del RGPD. En primer lugar, se constató una vulneración del artículo 32 RGPD, al no haberse implantado medidas de seguridad básicas que habrían dificultado el acceso ilegítimo. La autenticación para acceder a los sistemas internos, incluido el acceso remoto de empleados mediante VPN, no era suficientemente robusta, y los mecanismos de detección de comportamientos anómalos resultaron ineficaces.

En segundo lugar, se apreció un incumplimiento del artículo 34 RGPD en relación con la comunicación dirigida a las personas afectadas por la brecha. El mensaje inicial remitido no incluía toda la información necesaria para comprender el alcance del incidente ni las medidas de autoprotección recomendadas, dificultando la reacción inmediata de los usuarios.

Finalmente, en el caso de una de las entidades, responsable de los servicios de telefonía móvil, se observó también una infracción del artículo

5.1.e) RGPD por conservar durante años datos de antiguos abonados sin justificación, más allá del tiempo necesario para cumplir con las obligaciones contables correspondientes.

Sanción a una comercializadora energética por cruzar datos personales de dos clientes

La infracción se produjo cuando un cliente de la comercializadora energética recibió un correo electrónico que contenía datos personales de un tercero, incluyendo su nombre completo, número de contrato, facturas y la existencia de una deuda. La recepción de dicho correo por la parte reclamante estuvo causada por el hecho de que un empleado del encargado del tratamiento de la comercializadora atribuyó erróneamente al cliente tercero la dirección de correo electrónico de la parte reclamante.

El error estuvo propiciado por el hecho de que el empleado atendía simultáneamente a dos usuarios a través del canal de *chat*, lo que llevó a que introdujera por error la dirección de correo del reclamante en la ficha de otro cliente. Este canal, que en 2023 registró más de 15.000 interacciones, permitía a un agente gestionar varias conversaciones a la vez, incrementando significativamente el riesgo de errores. Aunque la parte reclamada eliminó dicho canal en 2024, la AEPD considera que esta actuación fue reactiva y no preventiva.

Aunque la propuesta inicial contemplaba una sanción de un 1.000.000 de euros, la [resolución](#) fija finalmente una multa de 500.000 euros por vulneración del artículo 25 del RGPD, relativo a la protección de datos desde el diseño y por defecto.

Como argumentos, la Agencia concluye que la empresa carecía de medidas técnicas y organizativas adecuadas para evitar inexactitudes en los datos, como controles eficaces para detectar duplicidades o atribuciones incorrectas entre clientes. Los mecanismos existentes solo verificaban aspectos formales, pero no prevenían que un mismo dato pudiera asignarse a dos personas distintas. Esta ausencia de controles y de un análisis de riesgos adecuado evidencia, según la AEPD, un defecto sistémico en el diseño del proceso de actualización de datos, que exponía potencialmente a todos los clientes de la entidad a incidentes similares.

La AEPD impone una sanción a una compañía de telefonía móvil por la suplantación de la identidad del titular de una línea telefónica

La [resolución](#) analiza una reclamación frente a una compañía de telefonía móvil por la pérdida del servicio telefónico y la realización de operaciones bancarias fraudulentas sufridas por la reclamante tras un cambio no consentido de titularidad de la línea y la creación de un duplicado de la tarjeta SIM.

En este caso, se tramitó telefónicamente un cambio de titularidad sin seguir el protocolo interno de la compañía, omitiéndose la verificación reforzada mediante llamada de comprobación a la línea o envío de OTP (*one-time password*) y la comprobación de los últimos dígitos de la factura. La llamada no provenía de la línea afectada. En cuanto al duplicado de la SIM, tampoco se realizó la verificación mediante código temporal o llamada, y el DNI escaneado correspondía a un tercero distinto de la reclamante.

Así, la AEPD considera que no se garantizó la identificación del verdadero titular ni la licitud del tratamiento, permitiéndose un tratamiento sin base jurídica válida en vulneración del artículo 6.1 RGPD. La responsabilidad se fundamenta en la falta de diligencia en la verificación de identidad, el incumplimiento de la responsabilidad proactiva (artículos 5.2 y 24 RGPD) y la doctrina del Tribunal Supremo sobre suplantación de identidad, que basa la responsabilidad en la ausencia de controles para asegurar una base de legitimación suficiente.

Finalmente, la AEPD aprecia unidad de acto al producirse dos operaciones de tratamiento ilícito vinculadas (cambio de titularidad y duplicado de SIM), calificando la actuación como una única infracción del artículo 6.1 RGPD e imponiendo una multa de 300.000 euros.

La AEPD reitera que el móvil personal de los empleados no puede ser usado como herramienta de autenticación en el entorno laboral

La AEPD ha vuelto a declarar ilícita la comunicación de números de teléfono personales de empleados por parte de una empresa del sector de *contact center* a uno de sus clientes internacionales para activar un sistema de doble autenticación necesario para acceder a sus herramientas corporativas. La práctica afectó a más de 200 empleados y se prolongó durante más de un año.

La empresa implantó un sistema de acceso a las herramientas de un cliente internacional que exigía la recepción de claves de autenticación en el teléfono móvil del trabajador. Durante la formación inicial, se pidió a los empleados que escribieran en un folio su número personal y su fecha de nacimiento. Posteriormente, comenzaron a recibir directamente códigos de acceso enviados por el cliente. La representación sindical propuso alternativas como el uso del correo corporativo, pero la empresa respondió que no era viable porque el cliente exigía vincular un número de teléfono para generar un *token* de doble autenticación y no disponía de terminales profesionales suficientes. La propia empresa reconoció que se encontraba en un proceso gradual de transición hacia teléfonos y tarjetas SIM corporativas, indicando que 203 de los 364 trabajadores seguían utilizando su número personal.

La Agencia examina el caso a la luz del artículo 6.1.b) del RGPD, que solo permite el tratamiento de datos personales cuando sea estrictamente necesario para la ejecución del contrato con la persona trabajadora. Para la AEPD, esta exigencia no se cumplía, ya que es el empleador quien debe proporcionar los medios materiales necesarios para el desempeño de la actividad, conforme al principio de ajenidad en los medios propio de la relación laboral. Por ello, y porque existían opciones menos invasivas (correo corporativo o terminales profesionales), el teléfono personal no puede considerarse imprescindible para prestar el servicio.

La [resolución](#) subraya, asimismo, que la empresa era plenamente consciente de la

irregularidad: su delegado de protección de datos había advertido por escrito de que el uso del móvil personal para fines profesionales vulneraba la normativa. Pese a ello, la organización mantuvo el envío de datos al cliente sin proporcionar alternativas técnicas ni adoptar medidas adecuadas de minimización.

Por estos motivos, la autoridad aprecia una infracción del artículo 6 del RGPD e impone una multa de 80.000 euros, reducida finalmente a 48.000 euros por reconocimiento de responsabilidad y pago voluntario. Como nota adicional, la resolución presenta cierta inconsistencia al analizar el rol de la empresa, calificándola inicialmente como encargada del tratamiento y, posteriormente, como responsable.

Posible cambio de criterio de la AEPD en cuanto al uso de tecnologías biométricas

La AEPD [archiva](#) un caso relativo al uso de datos biométricos en el establecimiento de un control de acceso a determinadas áreas productivas por parte una entidad del sector alimentario.

Esta resolución es de especial interés, ya que la AEPD acaba archivando el caso sin apreciar infracción alguna por el uso de tecnologías de identificación biométrica. Esto supone un potencial cambio de criterio por parte de la AEPD, que venía teniendo una aproximación restrictiva en cuanto al uso de estas tecnologías para el control de acceso en el entorno laboral.

En este caso, según consta en la resolución, la entidad justificó la necesidad del control por requisitos sanitarios, evaluó alternativas y restringió el despliegue a la zona productiva, no implementándolo con carácter general e indiscriminado. El control biométrico solo aplicaba a un área de acceso restringido por motivos sanitarios relacionados con el sector alimentario, lo cual podría justificar la necesidad de la medida.

Si bien la AEPD no incluye en la resolución un análisis detallado sobre las bases legales concurrentes ni las posibles habilitaciones al tratamiento de esta información conforme al artículo 9.2. del RGPD, esta resolución es indicativa de un potencial cambio de enfoque en cuanto al uso de estas tecnologías, y señala

unas líneas maestras acerca de los requisitos que han de cumplirse para poder implementar este tipo de tecnologías en los lugares de trabajo.

Sanción por el extravío de reconocimientos médicos en la vía pública

La AEPD ha [sancionado](#) con 100.000 euros a una empresa dedicada a los servicios de prevención de riesgos laborales por la exposición accidental de reconocimientos médicos pertenecientes a agentes de distintos cuerpos policiales. La documentación, que incluía datos especialmente sensibles relativos a la salud, fue localizada abandonada en la vía pública tras ser trasladada desde dependencias oficiales hasta las instalaciones de la entidad.

La investigación acreditó importantes fallos en los procedimientos internos: ausencia de una cadena de custodia, inexistencia de registros sobre el traslado de la documentación y falta de medidas organizativas que garantizaran su confidencialidad. La autoridad concluye que estos hechos constituyen una vulneración del principio de integridad y confidencialidad del artículo 5.1.f del RGPD, lo que justifica la imposición de la sanción.

Además de la multa, la resolución ordena a la entidad implantar medidas que aseguren la trazabilidad y protección de la documentación médica cuando se trate fuera de sus instalaciones. La AEPD recuerda que el tratamiento de datos de salud exige una diligencia reforzada y que los encargados de este tipo de servicios deben garantizar medidas de seguridad proporcionales al riesgo derivado de su actividad.

Se impone sanción a un hotel por exposición indebida de datos personales de clientes

En esta [resolución](#), la AEPD analiza una reclamación trasladada a través del Sistema IMI (Sistema de Información del Mercado Interior) por la Autoridad de Protección de Datos de Suecia contra una empresa hotelera en relación con la exposición indebida de datos personales de propietarios y clientes alojados en un complejo turístico.

El personal de seguridad, actuando como encargado del tratamiento contratado por la sociedad, dejó a la vista listados en papel que contenían datos como nombre, apellidos, país, número de apartamento, pasaporte y DNI, accesibles a terceros, que llegaron incluso a fotografiarlos. La AEPD constató que, a pesar de disponer la sociedad de protocolos genéricos y de haber aportado posteriormente documentación sobre auditorías, protocolos internos y medidas adoptadas, no quedó acreditado que existieran medidas técnicas y organizativas adecuadas para evitar un acceso no autorizado a los datos. Así, la AEPD concluye que se produjo una pérdida de confidencialidad y que las medidas alegadas no eran suficientes ni estaban concretadas para garantizar la seguridad exigida por el RGPD.

Se impone una sanción de 40.000 euros, teniendo en cuenta la naturaleza y gravedad de la infracción, el volumen de datos expuestos, la sensibilidad de la información (DNI y pasaporte) y la vinculación de la actividad del responsable con tratamientos continuos de datos personales. La empresa sancionada se acogió al pago voluntario, aplicándose una reducción del 20%, quedando la cuantía definitiva de la sanción fijada en 32.000 euros, ordenándose, además, que en un plazo de tres meses se acreditara la implantación de medidas adecuadas para evitar nuevos incidentes de este tipo.

Se impone una sanción a una clínica dental por la grabación de imagen y sonido en el interior del gabinete

La [resolución](#) analiza un supuesto en el que una antigua empleada de una clínica dental denunció la captación de imágenes y sonido mediante cámaras de videovigilancia sin información adecuada, alegando que no existía cartel informativo y que los pacientes no eran informados de la grabación durante las intervenciones. La parte reclamada manifestó que disponía de dos dispositivos: una cámara de vídeo en el gabinete dental y una cámara de fotografía en la recepción, ambas con finalidad de seguridad y gestionadas por una empresa, reconociendo que el sistema captaba sonido en el gabinete y que las imágenes se conservaban durante un plazo máximo de siete días.

La AEPD consideró que la captación continuada de pacientes durante tratamientos dentales resulta desproporcionada para los fines de seguridad invocados, vulnerando el principio de minimización de datos (art. 5.1.c) RGPD). La Agencia destacó que la grabación de conversaciones entre pacientes y trabajadores constituye una intromisión ilegítima en el derecho a la intimidad, ordenando la reorientación o retirada de la cámara en un plazo de tres meses.

A efectos sancionadores, se impone una sanción de 2.000 euros, encuadrándose en el artículo 83.5 RGPD (principios básicos y condiciones de licitud), valorando la naturaleza de los hechos, su alcance y la afectación a derechos fundamentales. En fase de tramitación, la clínica se acogió al reconocimiento de responsabilidad y al pago voluntario, por lo que la sanción quedó reducida a 1.200 euros. La AEPD declara la comisión de la infracción, confirma la sanción resultante y acuerda la terminación del procedimiento.

Multa a un sindicato sanitario y a su fundación por una brecha de seguridad y falta de transparencia en su corresponsabilidad

La autoridad de control ha sancionado con 15.000 euros a una organización sindical del sector sanitario y a su fundación, vinculada a la formación en enfermería, tras constatar dos infracciones relevantes en el marco de un ataque de *ransomware* que comprometió los datos de cerca de 198.000 personas. Ambas entidades actuaban como corresponsables del tratamiento en el desarrollo de su programa conjunto de actividades formativas para profesionales sanitarios.

El incidente se produjo cuando un grupo identificado como *Hunters International* accedió a sus sistemas, cifró la información e hizo pública la supuesta venta de bases de datos en espacios de la *dark web*. Aunque en la notificación remitida a la autoridad se indicó que únicamente se habían visto afectados los datos gestionados para formación, la investigación muestra indicios de que otras áreas podrían haber resultado comprometidas. La autoridad señala que no consta la notificación a posibles afectados fuera del ámbito formativo, lo que

genera dudas sobre la correcta delimitación del alcance real de la brecha.

La [resolución](#) aprecia una infracción del artículo 5.1.f) del RGPD, al comprobar que antes del ataque no existía un análisis de riesgos suficiente ni medidas técnicas y organizativas adecuadas. Entre las deficiencias detectadas menciona la ausencia de autenticación multifactor, bases de datos sin cifrar y una capacidad insuficiente para detectar y evaluar adecuadamente el incidente, así como la falta de supervisión sobre su impacto y duración.

Además, la autoridad estima una infracción del artículo 26 del RGPD, al constatar que ambas entidades se declararon corresponsables de los datos mediante un acuerdo genérico y sin concretar de forma transparente sus respectivas responsabilidades. Tampoco se puso dicho acuerdo a disposición de las personas participantes en las actividades formativas, y la información ofrecida en formularios y políticas de privacidad no reflejaba la corresponsabilidad real entre ambas organizaciones.

La AEPD sanciona a un operador de telecomunicaciones por enviar credenciales de acceso al área de clientes en un correo electrónico en texto plano

La AEPD ha dictado [resolución](#) imponiendo una multa de 10.000 euros a un operador de telecomunicaciones por infracción del artículo 32 del RGPD. El procedimiento se inició tras la reclamación de un cliente que recibió un correo electrónico, remitido en texto plano y sin cifrar, en el que la compañía le comunicaba la actualización de su área de clientes incluyendo sus credenciales completas de acceso (usuario y contraseña). El reclamante denunció que dicho portal, que almacena datos como nombre, apellidos, dirección, DNI, teléfono, cuenta bancaria, facturas y detalle de consumos, carecía, además, de autenticación de doble factor.

La entidad sancionada alegó que el incidente fue producto de un error humano puntual, que actuó de forma inmediata reiniciando las contraseñas y contactando con el afectado, y que no se había producido ningún acceso no autorizado ni exfiltración de datos. Sin embargo, la AEPD rechaza estos argumentos,

señalando que el artículo 32 del RGPD impone una obligación de medios que exige adecuación efectiva al riesgo, y que el envío de credenciales en texto plano por correo electrónico evidencia la inexistencia de medidas organizativas suficientes para impedir la divulgación indebida de información de autenticación. La Agencia subraya que no es necesario que se materialice un daño efectivo para que se produzca la infracción, bastando con que las medidas de seguridad resulten inadecuadas al riesgo inherente al tratamiento.

Como circunstancias atenuantes, la AEPD valoró la rápida respuesta de la empresa y la adopción de medidas correctoras. Como agravantes, la negligencia grave en el cumplimiento normativo y la vinculación de su actividad con el tratamiento masivo de datos personales de clientes.

La AEPD sanciona a una entidad de préstamos ‘online’ por exigir a sus clientes una foto con el DNI en la mano para tramitar la cancelación de un préstamo

La AEPD ha dictado [resolución](#) sancionando a una entidad dedicada a la concesión de préstamos *online* por infracción del artículo 5.1.c) del RGPD, relativo al principio de minimización de datos. El procedimiento se inició tras la reclamación de un cliente al que, habiendo solicitado la cancelación anticipada de su préstamo, se le exigió como requisito para tramitarla la aportación de una fotografía en la que apareciese sosteniendo su documento de identidad.

La entidad alegó que dicho procedimiento de identificación respondía a las obligaciones establecidas en la normativa de prevención del blanqueo de capitales. La AEPD rechaza esta justificación señalando que la normativa sectorial invocada no resulta contraria ni incompatible con los principios del RGPD, y que ambos marcos normativos deben aplicarse de forma concurrente. En particular, la Agencia destaca que la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales, establece una obligación de identificación que puede satisfacerse mediante otros medios menos intrusivos, como la firma electrónica cualificada, la copia del documento de identidad expedida por fedatario público, o la verificación mediante los sistemas de identificación ya

habilitados por la entidad para sus clientes. La solicitud de una fotografía del interesado sosteniendo su DNI supone un tratamiento excesivo de datos personales que genera riesgos adicionales de suplantación de identidad.

La sanción inicialmente propuesta fue de 10.000 euros, si bien la entidad se acogió al pago voluntario con la reducción del 20%, quedando establecida en 8.000 euros. Adicionalmente, la AEPD ordenó a la entidad adoptar medidas para que la acreditación de identidad en los procedimientos de cancelación de préstamos se realice en lo sucesivo mediante opciones que garanticen el cumplimiento del principio de minimización.

La AEPD estima una reclamación contra el Servicio de Salud de las Illes Balears por no atender el derecho de acceso de un ciudadano

La AEPD ha resuelto el procedimiento de derechos iniciado tras la reclamación de un ciudadano que ejerció su derecho de acceso frente al Servicio de Salud de las Illes Balears (IBSALUT), sin que su solicitud recibiera la contestación legalmente establecida.

La [resolución](#) de la AEPD recuerda que, de conformidad con lo dispuesto en el artículo 12 del RGPD y en la LOPD-gdd, el responsable del tratamiento debe arbitrar fórmulas y mecanismos para facilitar al interesado el ejercicio de sus derechos, y viene obligado a responder las solicitudes formuladas a más tardar en un mes, debiendo expresar sus motivos en caso de que no fuera a atender dicha solicitud. Recae sobre el responsable la prueba del cumplimiento del deber de responder a la solicitud de ejercicio de derechos formulada por el afectado, y la comunicación que se dirija al interesado deberá expresarse en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.

La AEPD señala que las normas aplicables no permiten que pueda obviarse la solicitud como si no se hubiera planteado, dejándola sin la respuesta que obligatoriamente deben emitir los responsables, aun en el supuesto de que no existan datos del interesado objeto de tratamiento o incluso en aquellos supuestos en

los que la solicitud no reuniera los requisitos previstos. En este caso el destinatario está igualmente obligado a requerir la subsanación de las deficiencias observadas o, en su caso, a denegar la solicitud motivadamente, indicando las causas por las que no procede considerar el derecho de que se trate.

En consecuencia, la AEPD ha estimado la reclamación al considerar que se ha infringido lo dispuesto en el artículo 15 del RGPD, e insta al Servicio de Salud de las Illes Balears a que, en el plazo de diez días hábiles desde que la resolución sea firme y ejecutiva, remita al reclamante certificación por la que se atienda el derecho de acceso ejercido o se deniegue motivadamente indicando las causas por las que no procede atender la petición.

La AEPD sanciona a una empresa de mensajería por subencargos no autorizados en la cadena de tratamiento

La AEPD ha [sancionado](#) a una empresa del sector logístico por diversas irregularidades en la gestión de subencargos dentro de la cadena de tratamiento. El asunto se origina cuando un cliente detecta que, para gestionar un envío, sus datos habían sido comunicados a terceros que no figuraban en la relación autorizada de encargados.

Tras analizar la documentación aportada por las empresas implicadas, la AEPD concluye que se produjeron tres incumplimientos diferenciados del RGPD. En primer lugar, la empresa encargada del tratamiento realizó un subencargo no autorizado a otra compañía especializada en logística, vulnerando el artículo 28.2, que exige el consentimiento previo y específico del responsable. En segundo lugar, no informó adecuadamente al responsable de que, a su vez, ese subencargado contrató a un tercero, lo que refuerza la infracción del mismo precepto. Por último, la AEPD advierte de que no existía un contrato de subencargo válido entre la reclamada y el primer subencargado, incumpliendo el artículo 28.4, que obliga a documentar las obligaciones aplicables al tratamiento.

Cada una de estas infracciones se sanciona con una multa independiente de 5.000 euros, ascendiendo el importe total a 15.000 euros.

Una entidad del sector sanitario envía por error datos personales de pacientes de reproducción asistida a otros usuarios del servicio

En abril de 2023, la AEPD recibió una reclamación en la que un particular denunciaba que la unidad de reproducción asistida del centro donde había sido paciente le había enviado un correo electrónico anunciando la transferencia del servicio a una nueva entidad, en el cual figuraban datos personales de otros pacientes.

La parte reclamada utilizó un sistema automatizado mediante documentos combinados de Word y Excel que contenía datos personales de los pacientes (nombre, apellidos, DNI y correo electrónico), generando PDF enviados automáticamente por correo. El proceso funcionó correctamente para los primeros 299 envíos, pero a partir del documento 300 comenzó a enviar información a destinatarios incorrectos. Por tanto, al menos 237 pacientes recibieron datos personales de otros usuarios (nombre, apellidos, DNI y condición de pacientes de reproducción asistida), de un total de 637 potencialmente afectados. La brecha fue notificada a la AEPD y a los interesados.

La AEPD identificó dos infracciones del RGPD en este [procedimiento sancionador](#): (i) la vulneración del principio de integridad y confidencialidad (art. 5.1.f) por no cifrar las notificaciones pese a ser exigido internamente y (ii) el incumplimiento del artículo 35 por no haber realizado una evaluación de impacto sobre la protección de datos (DPIA) para el tratamiento de datos de salud a gran escala. La AEPD rechazó los argumentos de la reclamada sobre la preexistencia del tratamiento al RGPD y su adaptación mediante la realización de un análisis de riesgos, e hizo hincapié en la auditoría de 2020 que ya había advertido de la necesidad de realizar la DPIA.

La AEPD propuso una sanción total de 100.000 euros (50.000 por infracción). Tras el pago voluntario con reducción del 20%, la sanción definitiva quedó en 80.000 euros.

Imposición de sanción por tratamiento de datos biométricos sin base jurídica válida y conservación excesiva de datos personales

La [AEPD ha impuesto una sanción de 950.000 euros](#) a una empresa especializada en la verificación de identidad y edad en entornos digitales por tratar datos biométricos sin contar con base de legitimación del artículo 9.2 RGPD, recabar un consentimiento inválido y conservar datos por tiempo superior del necesario.

En el alta del servicio, el usuario realiza un proceso de verificación en el que se capta su imagen facial. A partir de esa captura se genera y almacena una plantilla biométrica que se utiliza para autenticar al usuario y confirmar su identidad en accesos o interacciones posteriores. La AEPD concluye que este proceso supone la identificación unívoca de una persona física, constituyendo un tratamiento de categorías especiales de datos conforme al artículo 9.1 RGPD. La empresa alegó que su sistema no “identificaba” al usuario. Sin embargo, al no reconocer el carácter especial de los datos tratados, no aplicó ninguna de las bases jurídicas del artículo 9.2 RGPD, por lo que el consentimiento recabado se consideró inválido.

Además, se sanciona la obtención del consentimiento para fines de investigación y mejora mediante casilla premarcada, incompatible con un consentimiento libre, específico, informado e inequívoco (artículo 7 RGPD). Por último, se aprecia infracción del principio de limitación del plazo de conservación al mantener datos personales durante un periodo superior al estrictamente necesario, sin criterios efectivos de supresión (artículo 5.1.e RGPD).

La AEPD sanciona a una empresa por el indebido tratamiento de datos personales a través de uno de sus comerciales

La AEPD ha emitido una [resolución](#) por la cual impone una sanción de 20.000 euros y otra de 200.000 euros por la infracción de los artículos

13 y 6 del RGPD, respectivamente, a una empresa del sector energético.

La controversia surge a raíz de la realización de una llamada telefónica a un interesado por parte de un comercial de la empresa reclamada, que fue seguida del envío de un correo electrónico al mismo interesado con datos personales suyos precargados. Como en numerosos otros casos similares, el reclamante alega no tener contacto o relación previa alguna con la entidad reclamada, cuyos productos y servicios estaban siendo promocionados por el comercial.

La entidad reclamada alegaba que, en el momento de enviar las comunicaciones, el comercial actuaba como responsable del tratamiento independiente, y que, por lo tanto, cualquier tratamiento de datos indebido por su parte debiera acarrear, en su caso, responsabilidades para el comercial y no para la entidad reclamada. No obstante, la AEPD hace un análisis detallado sobre los conceptos de responsable y encargado del tratamiento, concluyendo que, en atención a los detalles del caso, la entidad reclamada determinaba fines y medios del tratamiento, y, por lo tanto, era, en efecto, responsable del tratamiento. De ahí que se aprecie la infracción del deber de informar y de contar con una base de legitimación suficiente para la realización de tales comunicaciones por parte de la entidad reclamada, que no guardaba relación alguna con el reclamante.

Esa resolución da claves relevantes para tener en cuenta en la determinación de los roles, y es un aviso frente a las prácticas extendidas en determinados sectores, en los que la información de los interesados es comunicada con excesiva liberalidad entre empresas comerciales y suministradores de diferentes servicios.

Sanción derivada de incidente de seguridad

En esta [resolución](#) la AEPD aprecia un incumplimiento de los artículos 5.1.f), 32, 33 y 34 del RGPD a raíz de un incidente de seguridad sufrido por la reclamada, que había afectado hasta a un millón de registros, e impone una sanción total de 1.090.000 euros.

Si bien abundan resoluciones similares en las que, como en el presente caso, se debate sobre

el nivel de diligencia de la entidad en su implementación de medidas de seguridad y gestión del incidente, esta resolución es especialmente interesante en tanto que contiene referencias a cuestiones, aunque ya bien conocidas, no menos relevantes y de interés. Destacamos las siguientes:

- El cómputo del plazo de 72 horas para notificar a la AEPD del incidente de seguridad debe computarse en días naturales, y el hecho de que el plazo venza en día festivo no es motivo válido para la demora en la notificación.
- La AEPD sanciona conjuntamente por infracción de los dos artículos citados, el

5.1.f) y el 32 RGPD, como ha venido haciendo en reiteradas ocasiones. Si bien es cierto que recientemente se habían emitido resoluciones limitadas a uno de los dos artículos y no a ambos conjuntamente, la AEPD retoma este enfoque argumentando que la “doble” sanción no supone ninguna infracción de los principios de non bis in idem, y que son perfectamente compatibles.

Esta materia es objeto de recurrente discusión en las resoluciones que emita la AEPD y también en tribunales, por lo que será importante hacer seguimiento de la misma para estar al día de su evolución.



Sentencias

El TJUE se pronuncia al respecto de normativa nacional sobre tratamiento de datos biométricos

En esta [sentencia](#) el TJUE ha dado respuesta a varias cuestiones prejudiciales en relación con la aplicación de la normativa nacional francesa que transpone la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos.

El caso tiene su origen en Francia, donde una persona fue detenida durante una manifestación y se negó a someterse a la toma de huellas dactilares y fotografías. Aunque fue absuelta del delito principal investigado, fue condenada al pago de una multa de 300 euros por negarse a la toma de datos identificativos, en aplicación del artículo 55-1 del Código de Procedimiento Penal francés. Desde los tribunales franceses, tras los recursos concurrentes, se elevaron tres cuestiones prejudiciales al TJUE para determinar la compatibilidad de dicha normativa con la citada Directiva (UE) 2016/680.

La discusión versa, principalmente, sobre hasta qué punto una normativa nacional puede exigir la toma de datos especialmente sensibles como los biométricos. A este respecto el TJUE concluye que:

- Una normativa nacional que establezca la recogida sistemática de datos biométricos de toda persona sospechosa de haber cometido o intentado cometer un delito es

contraria al Derecho de la UE, a menos que se cumplan dos condiciones: (i) que el Derecho nacional defina de manera adecuada y suficientemente precisa los fines específicos y concretos de dicha recogida y (ii) que la autoridad competente esté obligada a evaluar, caso por caso, si la recogida es estrictamente necesaria para alcanzar dichos fines, de modo que la recogida no tenga carácter sistemático.

- La autoridad competente debe motivar adecuadamente, en cada caso concreto, por qué la recogida de datos biométricos resulta “estrictamente necesaria”. El Tribunal precisa que dicha motivación puede ser sucinta, pero debe ser lo suficientemente clara para que el afectado comprenda las razones de la medida y pueda ejercer su derecho a un recurso efectivo.
- En cuanto a la legalidad de la sanción por no cooperar con las autoridades, el TJUE concluye que el Derecho de la UE no se opone a que un Estado miembro sancione penalmente la negativa a someterse a la recogida de datos biométricos. No obstante, esta sanción solo será lícita si la recogida de datos cumplía el requisito de ser “estrictamente necesaria” y si la sanción impuesta respeta el principio de proporcionalidad.

Esta sentencia tiene un especial interés en el contexto de las actividades de las fuerzas y cuerpos de seguridad del Estado, ya que da importantes guías sobre sus facultades y los requisitos que han de cumplirse en las normativas nacionales para habilitar la recogida por estos cuerpos de determinados tipos de datos.

El recurso interpuesto por WhatsApp Ireland contra la decisión vinculante del Comité Europeo de Protección de Datos es admisible

El asunto sobre el que versa la presente resolución se remonta al procedimiento iniciado en diciembre de 2018 por la Autoridad de Protección de Datos de Irlanda (*Data Protection Commission* o DPC), como autoridad de control principal, frente a WhatsApp Ireland Ltd (WhatsApp) por un presunto incumplimiento de las obligaciones de transparencia e información establecidas en los artículos 12 a 14 del RGPD. En este sentido, tras una primera propuesta de resolución emitida por la DPC y presentada a las demás autoridades de control nacionales interesadas, ocho de estas formularon objeciones pertinentes y motivadas, lo que condujo a la remisión del conflicto al Comité Europeo de Protección de Datos (CEPD) conforme al artículo 65, apartado 1, letra a), del RGPD.

A este respecto, en julio de 2021 el CEPD adoptó la decisión vinculante 1/2021, en la que se dejaba constancia de que existía una infracción de las citadas disposiciones del RGPD, obligando a la DPC a modificar las medidas correctivas previstas y, en particular, la cuantía de las multas. Con base en lo anterior, la DPC adoptó una decisión definitiva en la que, entre otras medidas, impuso a WhatsApp una serie de multas por importe total de 225 millones de euros.

Ante dicha resolución, WhatsApp interpuso recurso de anulación frente a la decisión vinculante del CEPD ante el Tribunal General, si bien este declaró que el recurso era inadmisibile porque tal decisión no constituía un acto impugnabile, además de que no afectaba directamente a WhatsApp. En este sentido, el Tribunal General señaló que dicha decisión era una medida intermedia (no definitiva) y que únicamente la decisión definitiva podía ser objeto de impugnación ante un juez nacional. Frente a este auto, WhatsApp interpuso recurso de casación ante el TJUE, el cual se resuelve mediante la presente sentencia.

Así pues, las cuestiones jurídicas resueltas en la [sentencia](#) son fundamentalmente dos: (i) el carácter impugnabile de la decisión vinculante

del CEPD y (ii) el requisito de afectación directa del demandante.

En primer lugar, respecto al carácter de acto impugnabile conforme al artículo 263 del Tratado de Funcionamiento de la Unión Europea (TFUE), el TJUE recuerda que el recurso de anulación puede interponerse contra todos los actos adoptados por instituciones, órganos u organismos de la Unión destinados a producir efectos jurídicos vinculantes, debiendo atenderse a la esencia del acto y examinar sus efectos a la luz de criterios objetivos como su contenido, el contexto de adopción y las facultades del órgano autor, entre otros. A este respecto, el TJUE rechaza expresamente la calificación de "medida intermedia" que había efectuado el Tribunal General, precisando que la decisión del CEPD fija definitivamente la postura de dicho órgano sobre las cuestiones que debe resolver, agotando su ámbito de competencia.

Por otro lado, en cuanto al requisito de afectación directa previsto en el artículo 263 TFUE, párrafo cuarto, el Tribunal aplica su jurisprudencia consolidada que exige el cumplimiento de dos condiciones acumulativas: que el acto surta efectos directamente en la situación jurídica del demandante y que no deje margen de apreciación a los destinatarios encargados de su aplicación. En consecuencia, el TJUE concluye que la decisión del CEPD modifica sustancialmente la situación jurídica de WhatsApp, al declarar infracciones adicionales del RGPD (concretamente de los artículos 13.1.d) y 13.2.e)-, que obligan a la empresa a modificar su relación contractual con los usuarios del servicio de mensajería prestado, de lo cual se deduce que existe un vínculo directo entre la decisión y sus efectos en la situación de WhatsApp.

Con base en lo anterior, el TJUE ha declarado admisible el recurso de anulación interpuesto por WhatsApp, anulando el auto del Tribunal General y devolviendo el asunto al mismo para que se pronuncie en cuanto al fondo, incluyéndose la cuestión sobre si WhatsApp ha infringido las obligaciones de transparencia e información establecidas en los artículos 12 a 14 del RGPD.

Anuladas varias sanciones impuestas por la AEPD a una entidad aseguradora por remitir comunicaciones comerciales a correos electrónicos genéricos

La Sección Primera de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional ha [estimado](#) el recurso interpuesto por una conocida entidad aseguradora contra la resolución emitida por la AEPD en abril de 2022, que confirmaba la imposición de tres sanciones de 100.000 euros cada una por infracciones de los artículos 6, 28 y 17 RGPD.

El procedimiento sancionador tuvo su origen en la reclamación de un particular que, entre 2016 y 2020, solicitó reiteradamente la supresión de sus datos personales sin obtener respuesta, continuando la recepción de comunicaciones publicitarias en una dirección de correo electrónico de carácter genérico (info@.....), inscrita en la Lista Robinson.

La Sala fundamenta la estimación del recurso en varios motivos. En primer lugar, concluye que una dirección de correo electrónico genérica de tipo info@empresa.com no constituye un dato de carácter personal a efectos del artículo 4 RGPD, al no permitir la identificación directa ni indirecta de una persona física concreta. En segundo lugar, determina que el responsable del tratamiento no era la entidad aseguradora *per se*, sino los agentes de seguros que, de forma autónoma, recababan y gestionaban los datos en calidad de responsables independientes, sin que se acreditase la existencia de una base de datos compartida. Finalmente, el Tribunal constata que, una vez conocida la oposición del reclamante, se le informó de la inexistencia de datos en los sistemas de la aseguradora y se procedió a su baja en los listados de los agentes.

En consecuencia, la Audiencia Nacional anula las tres sanciones impuestas, con expresa imposición de costas a la Administración demandada.

La Audiencia Nacional avala la inadmisión de una reclamación por la pérdida de un informe médico al considerar prescritos los hechos

Tras la presentación de una reclamación ante la AEPD por la pérdida de un informe médico de 2015 relativo al padre de la reclamante, lo que, según esta, evidenciaba una brecha de seguridad, la AEPD inadmitió la reclamación por dos motivos: la prescripción de las acciones y la inaplicabilidad de la normativa de protección de datos a personas fallecidas, salvo lo previsto en el artículo 3 de la LOPD-gdd.

En vía de recurso, la Audiencia Nacional [confirma](#) la inadmisión de la AEPD, aunque matiza algunos aspectos. En primer lugar, coincide en que los hechos estaban efectivamente prescritos. No obstante, rechaza el argumento relativo al régimen aplicable a personas fallecidas, puesto que, en el momento de elaborarse el informe extraviado, el paciente aún estaba vivo. En segundo lugar, la Sala aclara que lo ocurrido no constituye una brecha de seguridad del sistema, sino un problema de gestión y registro documental: el facultativo consideró que el documento era un borrador y, por tanto, no lo incorporó al historial clínico.

La sentencia también se pronuncia sobre la legitimación de la reclamante. Reconoce que esta sí ostenta un interés legítimo para solicitar la investigación de hechos relacionados con el tratamiento de datos. Sin embargo, recuerda que este derecho no ampara la exigencia de iniciar procedimientos sancionadores ni la imposición de sanciones concretas.

En consecuencia, la Audiencia Nacional desestima el recurso y confirma la actuación de la AEPD, sin imposición de costas.

Anulada una sanción impuesta a un miembro de una junta de personal de un sindicato por reenviar correos corporativos a destinatarios ajenos a dicha junta

La Audiencia Nacional resuelve un recurso contencioso-administrativo interpuesto contra una resolución de la AEPD de 30 de agosto de 2022 por la que se impuso una multa de 2.000

euros por infracción del artículo 6.1) del RGPD, tipificada en el art. 83.5 del RGPD y 72.1 b) de la LOPD-gdd.

La AEPD consideró que un miembro de la junta de personal de un sindicato había reenviado de forma reiterada correos electrónicos que incluían datos de otro miembro de la junta (el reclamante), tales como el nombre y la dirección de correo laboral, a otras personas miembros y no miembros de la junta de personal y a correos corporativos de sindicatos y colectivos sin legitimación para ello, sin contar con el consentimiento del afectado y pese a la oposición expresa manifestada por este en varias ocasiones.

La AEPD estimó en su resolución que se trataba de un tratamiento ilícito de datos personales, considerando que el tratamiento de los datos personales del reclamante había sido excesivo, porque los correos electrónicos objeto de la reclamación se remitieron también a personas ajenas a la junta de personal.

Frente a esta resolución se interpuso un recurso contencioso-administrativo ante la Audiencia Nacional, alegando el recurrente que el uso del correo electrónico se realizó dentro del ámbito del derecho laboral y en el ejercicio de funciones sindicales, y que todos los destinatarios eran funcionarios o representantes sindicales, teniendo todos acceso a los datos objeto de reclamación por el denunciante a través del Portal del Empleado, tales como el correo corporativo, el nombre, la categoría profesional, el destino y el teléfono del reclamante.

La Audiencia Nacional [reconoce](#) que el correo electrónico corporativo es un dato de carácter personal cuando hace referencia a un usuario concreto, en línea con la doctrina de la propia Agencia en su Informe 0437/2010. Sin embargo, concluye que no puede desconocerse que la difusión del correo electrónico se produjo exclusivamente dentro del ámbito de la Administración Pública y en un área organizativa concreta, siendo los receptores funcionarios u organizaciones sindicales que, en puridad, no pueden considerarse terceros ajenos a la información que la junta de personal enviaba.

Además, la Sala destaca que todos los destinatarios tenían habilitado el acceso al Portal del Empleado, por lo que los datos

difundidos eran datos ya publicados o respecto de los cuales existía consentimiento en su difusión, al menos en dicho contexto, perteneciendo al ámbito de lo público conforme al artículo 9.2.e) del RGPD. Por todo ello, la Audiencia considera que el tratamiento no puede calificarse de ilícito y, en consecuencia, estima el recurso y anula la resolución de la AEPD.

Una entidad cesionaria no vulnera el derecho al honor cuando acredita el requerimiento previo de pago antes de incluir datos en un fichero de morosidad

En esta [sentencia](#) del Tribunal Supremo, se analiza si la inclusión de los datos personales de un deudor en un fichero de solvencia patrimonial constituye una intromisión ilegítima en su derecho al honor cuando consta el envío del requerimiento previo de pago, pero no la prueba fehaciente de su recepción.

El litigio tiene su origen en la demanda interpuesta por un particular frente a una entidad dedicada a la gestión y adquisición de créditos, que había comunicado sus datos al fichero Asnef-Equifax por una deuda derivada de un contrato de telefonía. El demandante sostenía que dicha inclusión era ilegítima al no haberse acreditado la recepción efectiva del requerimiento previo de pago, solicitando la cancelación de los datos y una indemnización por daños morales. Tanto el Juzgado de Primera Instancia como la Audiencia Provincial estimaron la demanda, al considerar insuficiente la prueba aportada sobre la recepción del requerimiento.

El Tribunal Supremo estima el recurso interpuesto por la entidad demandada y revoca las resoluciones anteriores. La Sala recuerda su doctrina consolidada según la cual el requisito del requerimiento previo no exige la prueba fehaciente de su recepción, siendo suficiente una constancia razonable de que aquel se realizó correctamente. En el caso concreto, el requerimiento fue enviado por correo postal a la dirección facilitada por el propio deudor en el contrato, no constó su devolución y no se acreditó ningún indicio que permitiera dudar de su llegada al destinatario.

El Tribunal destaca, además, que la deuda era cierta, vencida y exigible, extremo no

controvertido en la demanda. En consecuencia, concluye que no existió intromisión ilegítima en el derecho al honor y acuerda la desestimación íntegra de la demanda, con imposición de costas al demandante en primera instancia.

Descartada la vulneración del derecho al honor por la inclusión en un fichero de solvencia de datos relativos a una deuda tributaria obtenidos de un boletín oficial

El Tribunal Supremo ha [estimado](#) el recurso de casación interpuesto por una empresa de servicios de información crediticia, revocando la sentencia de la Audiencia Provincial de Madrid que había declarado una intromisión ilegítima en el derecho al honor del demandante y condenado a la empresa al pago de 4.000 euros por daños morales.

El origen del litigio se sitúa en la inclusión de los datos del demandante en un fichero de solvencia patrimonial, a partir de la publicación en el Boletín Oficial del Estado de un anuncio de embargo por deuda tributaria con el Ayuntamiento de Madrid. La anotación permaneció vigente desde febrero de 2017 hasta mayo de 2021 y fue consultada por dos entidades bancarias, lo que motivó la denegación de un préstamo al afectado.

La cuestión casacional consistía en determinar si los requisitos del artículo 29, apartados 2 y 4, de la derogada Ley Orgánica 15/1999 - requerimiento previo de pago, advertencia de inclusión y notificación posterior- resultan exigibles a los ficheros del apartado 1 del mismo precepto, nutridos de datos procedentes de fuentes accesibles al público. El Tribunal Supremo, reiterando la doctrina de sus sentencias 434/2023 y 917/2025, concluye que tales requisitos no son aplicables a estos ficheros, que se rigen exclusivamente por las disposiciones generales de la ley y su reglamento.

En consecuencia, la Sala estima el recurso, confirma la sentencia de primera instancia -que había desestimado la demanda al considerar los datos veraces y obtenidos de fuente pública- e impone al demandante las costas del recurso de apelación.

El Tribunal Supremo recuerda cuestiones clave en relación con la inclusión de datos en sistemas de información crediticia

Esta [sentencia](#) analiza la licitud del tratamiento de datos personales en sistemas de información crediticia y su impacto en el derecho al honor mediante la resolución de un recurso de casación interpuesto por una entidad contra una sentencia que declaró la vulneración del derecho al honor de la demandante por su inclusión indebida en dicho fichero.

El Tribunal aborda tres cuestiones clave en materia de protección de datos:

- Principio de calidad del dato: solo cabe inscribir en ficheros de solvencia deudas ciertas, vencidas y exigibles. Esta inclusión fue ilícita porque la deuda no quedó acreditada, al existir discrepancias entre el importe cedido y el certificado por la entidad cedente.
- Requerimiento previo de pago: el Tribunal admite el carácter funcional del requerimiento, pero establece que pierde relevancia cuando el deudor ya consta en ficheros de morosidad por inscripciones previas de otras entidades.
- Régimen indemnizatorio: se distingue entre la infracción del RGPD (que exige acreditar el daño, conforme al art. 82.1 RGPD y STJUE C-300/21) y la vulneración del derecho al honor, donde opera la presunción legal de perjuicio del art. 9.3 LO 1/1982.

El fallo estima parcialmente el recurso y rebaja la indemnización de 7.000 € a 3.000 €.

Anulada una multa por tratamiento ilícito de datos relacionada con una deuda por tarjeta de crédito, pero confirma la multa por vulneración del derecho de acceso

La [sentencia](#) estima parcialmente un recurso contencioso administrativo interpuesto por una entidad dedicada a la gestión de deuda

impagada contra una [resolución de la AEPD](#) que había impuesto dos sanciones por infracción del RGPD en el marco de una reclamación de deuda por tarjeta de crédito. La AN anula la multa de 30.000 euros por presunto tratamiento ilícito de datos (art 6.1 del RGPD) y confirma la multa de igual importe por falta de diligencia en la atención del derecho de acceso (art. 15 del RGPD).

El caso se origina por la reclamación de una consumidora a quien se exigía el pago de una deuda derivada de una tarjeta de crédito cuya contratación afirmaba desconocer. La AN apreció indicios suficientes de que el contrato se había celebrado telefónicamente en octubre de 2000 (pese a la ausencia de grabación de la llamada o de contrato firmado), valorando la constancia de datos personales de la interesada, el uso de la tarjeta hasta 2004, pagos posteriores referenciados al número de operación y la notificación de la cesión del crédito en 2008, sin oposición de la interesada. Con base en ello, la AN concluye que el tratamiento se fundamentaba en la ejecución del contrato (art. 6.1.b del RGPD) y que existió consentimiento inequívoco de la interesada, por lo que el tratamiento debe considerarse lícito.

No obstante, la AN confirma la sanción por infracción del artículo 15 del RGPD, puesto que la reclamante únicamente atendió la solicitud de acceso tras la reclamación interpuesta por la afectada ante la AEPD, sin acreditar gestiones previas adecuadas ni el cumplimiento del plazo legalmente previsto. La sentencia reitera la obligación de atender a los ejercicios de derechos y responder en el plazo de un mes con información clara, accesible y trazable, conforme a los artículos 12 y 15 del RGPD.

Confirmada la licitud del tratamiento de datos personales en el fichero de solvencia ASNEF

El Tribunal Supremo [desestima](#) el recurso de casación interpuesto por una particular contra una sentencia de la Audiencia Provincial de Madrid, confirmando la licitud de la inclusión de sus datos personales en el fichero ASNEF a instancia de una entidad prestamista de microcréditos.

Los hechos parten de un microcrédito de 200 euros formalizado electrónicamente en diciembre de 2017. Ante el impago, la

prestamista remitió 22 correos electrónicos de reclamación y una carta postal -devuelta con la mención "desconocido"- antes de inscribir los datos en ASNEF en marzo de 2018. La prestataria tampoco formuló oposición en el posterior procedimiento monitorio, que concluyó con despacho de ejecución.

Desde la perspectiva de protección de datos, el Tribunal examina, en primer lugar, el principio de calidad del dato, apreciando una deuda cierta, vencida y exigible, avalada por la documentación contractual y por la conducta procesal de la deudora. En segundo lugar, respecto del requerimiento previo de pago, reitera su doctrina sobre su carácter funcional: se trata de una garantía orientada a impedir la inclusión de personas que dejaron de pagar por simple descuido o error, sin que ese dato sea pertinente para enjuiciar su solvencia. En el caso, la Sala descarta cualquier efecto sorpresivo atendiendo a la naturaleza del contrato, a la existencia de anotaciones previas en ASNEF por deudas con otras dos entidades y a la pasividad de la afectada ante las reclamaciones, de modo que eventuales defectos formales en la acreditación del requerimiento no suponen, por sí solos, un tratamiento ilícito. Por último, rechaza que el principio de minimización del artículo 5.1.c) del RGPD impida la inclusión por deudas de escasa cuantía, pues una interpretación contraria dejaría al margen del sistema al deudor que reiteradamente incurre en impagos de obligaciones de escaso importe.

Se declara vulnerado el derecho a la protección de datos de una trabajadora al revelarse su nombre y salario en una carta de despido dirigida a su pareja

El Tribunal Superior de Justicia de Canarias declara vulnerado el derecho fundamental a la protección de datos de una trabajadora de una cadena de supermercados. La controversia surge a raíz de una carta de despido dirigida a la pareja de la trabajadora, también empleado de la misma cadena, en la que, para justificar que aquel percibía un complemento salarial indebido, la empresa incluyó el nombre y el salario de la empleada como término de comparación, al realizar ambos la misma jornada. La empresa fue condenada a indemnizarla con 7.500 euros.

El [tribunal](#) reconoce el interés legítimo empresarial en la potestad disciplinaria y en la motivación del despido, pero considera desproporcionada la revelación de datos personales sin consentimiento del interesado. Para lograr el mismo objetivo podía haberse realizado la comparación sin mencionar a una persona concreta, medida más moderada para la consecución de tal propósito con igual

eficacia, habiendo bastado con aludir a otro trabajador en idéntico puesto o con utilizar datos anonimizados. El análisis se efectúa a la luz de los artículos 5.1 y 6.1 del RGPD, destacando la exigencia de proporcionalidad en el tratamiento de datos en el ámbito laboral.

Contacta con nuestros profesionales

Alejandro Padín

Socio · Madrid

alejandro.padin@garrigues.com

Luisa Cyrne

Asociada principal · Lisboa

luisa.cyrne@garrigues.com

Álvaro Blanco

Asociado sénior · Madrid

alvaro.blanco@garrigues.com

Andrea Ugalde

Asociada · Bilbao

andrea.ugalde@garrigues.com

Garazi Tomás

Asociada · Bilbao

garazi.tomas@garrigues.com

Ignacio Suárez

Asociado · Madrid

ignacio.suarez@garrigues.com

Laia Llambrich

Asociada · Bilbao

laia.llambrich@garrigues.com

Franco Muschi

Socio · Lima

franco.muschi@garrigues.com

Adrián León

Asociado sénior · Alicante

adrian.leon@garrigues.com

Mariana Ubidia

Asociada sénior · Lima

mariana.ubidia@garrigues.com

Carina Casadesús

Asociada · Barcelona

carina.casadesus@garrigues.com

Iciar Velasco

Asociada · Madrid

iciar.velasco@garrigues.com

Javier Enebral

Asociado · Madrid

javier.enebral@garrigues.com

Marta Sabio

Asociada · Barcelona

marta.sabio@garrigues.com

Más información:

[Economía del Dato, Privacidad y Ciberseguridad](#)

GARRIGUES

Plaza de Colón, 2 - 28046 Madrid

T +34 91 514 52 00

Síguenos en:



info@garrigues.com

garrigues.com

Esta publicación contiene información de carácter general, sin que constituya opinión profesional ni asesoramiento jurídico

© J&A Garrigues, S.L.P., quedan reservados todos los derechos. Se prohíbe la explotación, reproducción, distribución, comunicación pública y transformación, total y parcial, de esta obra, sin autorización escrita de J&A Garrigues, S.L.P.