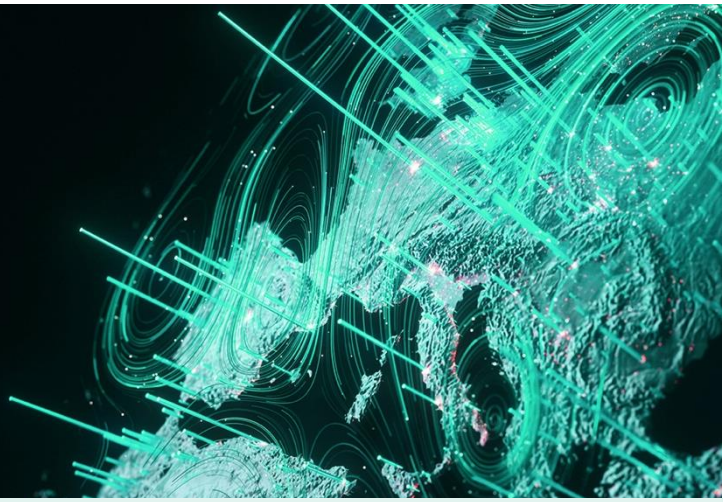
GARRIGUES

# Newsletter Economía del Dato, Privacidad y Ciberseguridad

Octubre 2024

# Índice

# 1. El laberinto regulatorio y de supervisión en la agenda digital europea: propuestas de racionalización



**La publicación del Reglamento europeo de Inteligencia Artificial establece un marco regulatorio complejo para supervisar el uso de IA, con autoridades de vigilancia y supervisión que se solapan y concurren con otras existentes en la economía digital o del dato. Buscando una gobernanza eficiente y coherente con otras normativas, como el RGPD, el Comité Europeo de Protección de Datos (CEPD) propone que las autoridades de protección de datos asuman funciones de supervisión para evitar la dispersión administrativa.**

**Alejandro Padín Vidal**

La reciente publicación del Reglamento europeo de Inteligencia Artificial supone uno de los principales hitos regulatorios en el ámbito de la economía digital, que también podemos denominar economía de la información o economía del dato. Desde el punto de vista estructural, es una norma extremadamente compleja, que pretende regular algo tan novedoso y cambiante como el uso de los sistemas de inteligencia artificial. Entre los contenidos regulados, esta norma incluye una estructura de gobernanza y supervisión en la que se establece la creación de diversas autoridades competentes tanto a nivel nacional en cada estado miembro como a nivel de la Unión.

El enfoque tiene todo el sentido, ya que una regulación que desarrolla tanto las obligaciones de las entidades afectadas debe ir acompañada de una adecuada verificación de su aplicación. Sin embargo, si tomamos perspectiva, podemos ver cómo las autoridades previstas en el Reglamento IA se unen a otro elenco de autoridades de supervisión, gobernanza, control y registro que se crean en varias de las normas europeas que se han venido dictando en el ámbito de la agenda digital europea en los últimos años. Solo por citar algunas, se han creado autoridades de supervisión y/o control y/o registro, en ocasiones con potestades sancionadoras, en el Reglamento General de Protección de Datos de 2016, en el Reglamento de Datos, en el Reglamento de Gobernanza de Datos, en la Directiva NIS 2 o en el Reglamento DORA**.**

Esta realidad, que, desde el mundo empresarial, se puede entender como un incremento desproporcionado de las cargas administrativas y burocráticas, podría verse mitigada si se aplicaran criterios de eficiencia y especialidad, de forma que las distintas funciones de supervisión de diferentes normas fueran asumidas por una misma autoridad con funciones similares o vinculadas.

En esta línea, el Comité Europeo de Protección de Datos (CEPD) ha publicado una declaración en la que, en relación con el Reglamento de Inteligencia Artificial, defiende la conveniencia de que las autoridades de supervisión en materia de protección de datos creadas por el RGPD asuman las

funciones de autoridad de vigilancia del mercado del Reglamento IA. Ello se basa en el reconocimiento de que dicho reglamento y las normas de privacidad europeas, tales como el RGPD o la Directiva de e-Privacy deben ser consideradas e interpretadas de forma coherente como instrumentos complementarios y que se refuerzan recíprocamente.

Esta recomendación del CEPD está relacionada, por una parte, con la afirmación de que el tratamiento de datos (tanto personales como no personales) en el ciclo de vida de un sistema de IA, especialmente los de alto riesgo, es claramente un elemento central de las diferentes tecnologías cubiertas bajo el paraguas de la definición de IA en el Reglamento IA. Y, por otra parte, tal como señalaba ya el CEPD en su informe conjunto con el Supervisor Europeo de Protección de Datos (SEPD), está relacionada con la experiencia ya adquirida por las autoridades de control en materia de IA, los beneficios de instaurar un punto único de contacto para los operadores de mercado, y su grado de independencia, soslayando, además, potenciales discrepancias entre las resoluciones de ambas autoridades supervisoras.

Dado que hay Estados Miembros que han iniciado procesos legislativos para la creación de dichas entidades supervisoras contempladas en el RIA de manera paralela a las Autoridades de control de protección de datos (como es el caso de España), el CEPD remarca la importancia de que las entidades colaboren y cooperen en los futuros procesos con base en el artículo 4(3) del Tratado de la Unión Europea.

En definitiva, el CEPD recomienda que las autoridades de supervisión de protección de datos sean designadas, en aquellos países donde aún no existan, como las autoridades de vigilancia del mercado para los sistemas de IA de alto riesgo mencionados en el Reglamento IA.

La gobernanza de la economía digital debería tender, en opinión del CEPD, a una agregación de funciones, con el fin de evitar una dispersión excesiva de órganos supervisores, inspectores y sancionadores que redundaría, en última instancia, en una barrera para la aparición y desarrollo de operadores en el mercado.

# 2. Resoluciones de las autoridades de protección de datos

## La AEPD impone una multa de 70.000 euros a una entidad bancaria por facilitar información fiscal al exmarido de la titular de los productos financieros

La parte reclamante manifiesta que la entidad bancaria, sin su consentimiento, había facilitado a su exmarido la información fiscal del año 2021 sobre todos los productos del banco de los que ella era titular. Por su parte, el banco alega que en sus sistemas constan tanto la reclamante como su exmarido como titulares solidarios del producto, motivo por el cual se accedió a toda la información fiscal de ambos titulares y se entregó al exmarido de la reclamante el Certificado Fiscal Único, incurriendo en lo que califica de "un error humano e involuntario".

En su resolución PS-00143-2023 del 11 de julio de 2024, la Agencia Española de Protección de Datos (AEPD) considera que ha tenido lugar una brecha de seguridad de datos personales (en concreto, de confidencialidad), al haber sido indebidamente difundidos estos a terceros. Asimismo, señala que el hecho de que el suceso se haya producido en actuación contraria a las normas internas por parte de un empleado, en una actuación individual y aislada, no exime al responsable del tratamiento del cumplimiento de la normativa de protección de datos.

La resolución incide en que no solo es necesario contar con un cuerpo normativo y un programa de formación continua y concienciación de los empleados, sino también adoptar otras medidas técnicas y organizativas que coadyuven a reducir los riesgos específicos que se derivan de las características concretas del tratamiento. De hecho, destaca que, si se han adoptado medidas adicionales a resultas de este procedimiento con el objetivo de evitar incidencias como la acontecida, es porque las medidas de seguridad implantadas eran insuficientes o no lo suficientemente robustas.

Otra cuestión que trata la resolución es la relativa a la vulneración del *non bis in idem*, llegando a la conclusión de que, en este caso, no existe tal vulneración, ya que los artículos 5.1 f) (principio de integridad y confidencialidad) y 32 (seguridad del tratamiento) del RGPD persiguen fines distintos, aunque pueden estar relacionados.

Concluye, pues, la AEPD que no se ha cumplido con el deber de diligencia exigible, ponderando especialmente la profesionalidad del sujeto infractor y la vinculación de su actividad a la realización de tratamientos de datos personales, e impone una multa de 50.000 euros por infracción del artículo 5.1 f) del RGPD y otra de 20.000 euros por infracción del artículo 32 del RGPD.

## La AEPD recuerda que los datos personales procedentes del Boletín Oficial de la Propiedad Industrial no pueden utilizarse para el envío de publicidad por terceros

La resolución PS-00206-2024 del 12 de julio de 2024 se refiere a un supuesto en el que la parte reclamante recibe publicidad postal de una entidad con la que no ha mantenido relación comercial ni ha contactado previamente. Los datos utilizados en la comunicación procedían del Boletín Oficial de la Propiedad Industrial (BOPI) y la comunicación tenía como objetivo captar como cliente al reclamante.

Para responder a la reclamación, la AEPD acude a un informe del gabinete jurídico elaborado como consecuencia de una solicitud del Colegio Oficial de Agentes de la Propiedad Industrial y alcanza las siguientes conclusiones:

- Los datos personales se publicaron en el citado boletín como consecuencia de un mandato legal. Es decir, la publicación de los datos personales de la reclamante en el boletín se habría producido por exigirlo así la ley, no porque el reclamante haya decidido de forma voluntaria hacer públicos dichos datos.

- Los datos personales se utilizaron apartándose de la finalidad legalmente prevista para su publicación en el BOPI, que consistiría en permitir que los demás interesados en el otorgamiento, concesión o denegación, etc. del derecho de propiedad industrial puedan oponerse, si así lo estiman conveniente. Sin embargo, la entidad reclamada realiza un tratamiento con la finalidad de enviar una carta postal informativa ofreciendo sus servicios.

- El tratamiento no era previsible para el reclamante.

- Debe considerarse que la carta postal informativa enviada por el reclamado está dirigida al reclamante como particular, y no como apoderado de empresas.

- En el caso analizado, no procedería invocar la excepción prevista en el artículo 9.2 e) del RGPD, al no tratarse de categorías especiales de datos personales.

Por tanto, se considera que el tratamiento de datos personales se habría efectuado sin una causa legitimadora de las contempladas en el artículo 6.1 del RGPD y se inicia el procedimiento sancionador, que finaliza por pago voluntario de la entidad reclamada.

## Ante un ejercicio de derechos deben conservarse todos los datos personales afectados

En su resolución PS 131/2023 la AEPD sanciona con 140.000 euros a un grupo de grandes almacenes por infracción de los artículos 15 y 18 del RGPD, relativos al derecho de acceso y limitación del tratamiento, respectivamente. La entidad sancionada no atendió correctamente la petición de la parte reclamante de conservar y poner a su disposición las grabaciones de las cámaras de seguridad del accidente que sufrió una menor en las instalaciones, para el caso de que fuese necesario presentarlas como documentación en una eventual reclamación por daños.

En su resolución, la AEPD establece que hay que conservar todos los datos personales que pueden ser útiles para el ejercicio de derechos, no correspondiendo al responsable determinar si son pertinentes o no, y debiendo en su caso solicitar la aclaración correspondiente de manera previa a la supresión.

La AEPD también indica que, en esta ocasión, estaba plenamente justificado el que la entidad reclamada rebasara el plazo de conservación de las imágenes fijado por la propia entidad -15 días-, debiendo primar la atención a los derechos ejercitados por el reclamante.

Finalmente, la AEPD resuelve que, en este caso, el derecho de limitación no trae causa del derecho de acceso, por lo que corresponde imponer una multa diferenciada para cada una de las dos infracciones.

## Se prohíbe el fichaje de los trabajadores a través de sistemas de reconocimiento facial en instituciones públicas

Un demandante interpuso una reclamación ante la AEPD contra un ayuntamiento para que se analizase la legalidad de la imposición del fichaje mediante el reconocimiento facial como método de control de la jornada laboral para los empleados municipales de dicho ayuntamiento, y se revisase si se había efectuado una evaluación de impacto previa al tratamiento de los datos biométricos.

En su resolución de 21 de junio de 2024**,** la AEPD considera que no ha quedado suficientemente acreditado si resulta de aplicación alguna de las excepciones previstas en el artículo 9.2 del RGPD que permiten tratar datos biométricos como medio de control de la obligación legal de vigilar y controlar la jornada laboral de los empleados municipales.

Por ello, en este supuesto la AEPD ordena que se suspenda todo tratamiento de datos correspondiente a los sistemas de fichaje biométrico. Además, da un plazo de siete meses al ayuntamiento para que se realice una EIPD con el consecuente previo análisis de riesgos, así como la evaluación del triple juicio de idoneidad, necesidad y proporcionalidad de dichos sistemas de fichaje, determinando si concurre alguna de las excepciones del artículo 9.2.del RGPD, así como estableciendo las medidas de protección adecuadas y cumpliendo el resto de obligaciones requeridas por la normativa de protección de datos personales.

## La AEPD sanciona a una empresa por un error humano en el envío de las nóminas de los empleados

Tras solicitar su nómina al departamento de RRHH de su empresa, un trabajador recibió un correo electrónico con un documento en formato pdf que incluía tanto su nómina como la de otros 446 trabajadores más de la plantilla. Además de la información económica, aparecían datos como nombre, apellidos, DNI, número de afiliación a la Seguridad Social y número de la cuenta bancaria de los 447 trabajadores.

La empresa admitió los hechos reclamados, alegando que la brecha de datos personales se había producido como consecuencia de un error humano en el envío del archivo, sin que, además, el empleado de recursos humanos que remitió el archivo informara de ello a sus responsables o lo pusiera en conocimiento de la empresa. Por este motivo, según manifiesta la parte reclamada, la brecha no trascendió y no se pudo actuar de forma proactiva ante ella. Tras conocer los acontecimientos, la empresa implementó una herramienta de inteligencia de amenazas y se revisaron los protocolos internos de envío de nóminas.

A pesar de las medidas adoptadas, en su resolución la AEPD impone una multa de 300.000 euros por la supuesta infracción del artículo 5.1.f) del RGPD (relativo a la confidencialidad), y una multa de 150.000 euros por la supuesta infracción del artículo 32 del RGPD, al quedar acreditada la falta de medidas de seguridad suficientes, tipificada en el artículo 83.4.a) de dicha norma.

## Sanción millonaria de la autoridad holandesa a una empresa de VTC por la transferencia internacional de datos de conductores a EE. UU.

Más de 170 conductores franceses que trabajaban para una empresa holandesa de VTC presentaron una queja ante la asociación francesa de defensa de los derechos humanos *Ligue des Droits de l'Homme* (LDH). La autoridad de supervisión francesa remitió dichas quejas a la su homóloga holandesa.

Tras una investigación, se descubrió que la empresa de VTC recogía, entre otras cosas, información sensible de conductores de Europa y la almacenaba en servidores en EE. UU. Se trataba de datos de cuentas y licencias de taxi, pero también datos de ubicación, fotos, detalles de pago, documentos de identidad, e, incluso, en algunos casos, datos penales y médicos de los conductores.

Durante un período de más de dos años, entre la sentencia que invalidó el acuerdo *Privacy Shield* y la aprobación de su sucesor, la empresa de VTC transfirió todos esos datos a su sede en EE. UU., sin utilizar herramientas de transferencia. Por este motivo el 22 de julio de 2024 la autoridad holandesa impuso una multa de 290 millones de euros a la mencionada empresa**.**

## La dirección IP no constituye prueba suficiente por la alta vulnerabilidad a ataques informáticos de los 'routers' domésticos

La parte reclamante denunció que alguien había publicado un anuncio con su foto y su número de teléfono ofreciendo servicios sexuales, lo que generó que diversas personas contactaran con ella con ese propósito. La AEPD investigó los sitios web involucrados, pero los anuncios ya no estaban publicados. Por ello, solicitó información de los responsables, obteniendo una dirección IP vinculada a esos anuncios. Posteriormente, se requirió al titular de la IP que justificara la publicación, pero no hubo respuesta.

En el transcurso del procedimiento, la parte reclamada alegó que varios familiares usaban el mismo ordenador y la misma conexión, así como que la seguridad de los *routers* domésticos no es inviolable, apoyando su defensa en una sentencia del Tribunal Supremo de 3 de diciembre de 2021, rec. 2429/2011, que exculpaba a un acusado debido a la alta vulnerabilidad a ataques informáticos de su conexión de internet.

En su resolución PS 297/2023, la AEPD archivó el caso basándose en que (i) el reclamado vivía con otras personas que podían haber usado su conexión, (ii) hubo discrepancias en las fechas de publicación del anuncio, y (iii) el reclamado, de 75 años de edad y en una residencia en el momento de los hechos, difícilmente pudo realizar la publicación por sus propios medios. Por ello, no se pudo probar la responsabilidad del reclamado y el caso fue archivado.

## El canal de atención a consultas de trabajadores es un canal adecuado para recibir solicitudes de derecho de acceso

En su resolución PS 168/2023, la AEPD sanciona con una multa de 15.000 euros a una plataforma tecnológica de entregas a domicilio por no haber respondido adecuadamente a un derecho de acceso ejercitado por un trabajador.

La parte reclamada alegó que no cabía considerar responsabilidad, puesto que el trabajador ejerció su derecho de acceso a través del correo electrónico de soporte, y no a través del correo electrónico oficial para aspectos relacionados con la privacidad, que era el que se había indicado en la Política de Privacidad. También alega que se habían implementado mecanismos internos adecuados para que esta solicitud fuera reenviada al canal idóneo, y, con ello, ya se estaba dando cumplimiento al deber de realizar un esfuerzo razonable, al tratarse de una obligación de medios.

La Agencia consideró que el canal utilizado por el reclamante era un medio válido, y prueba de ello es que la reclamada ya preveía un protocolo para que tales solicitudes pudieran ser redirigidas de este canal al canal relacionado con cuestiones de protección de datos. Finalmente, matiza que pretender que un departamento de atención al cliente tramite una solicitud de este tipo no resulta desproporcionado, por lo que no puede considerarse que la reclamada haya realizado esfuerzos razonables.

## Condicionar la entrada a un establecimiento a que se otorgue consentimiento para el tratamiento de datos constituye una infracción de los artículos 4.11 y 7 del RGPD

La parte reclamante denunció a un parque temático porque éste condicionaba el acceso a sus instalaciones a la firma de un formulario en el que se autorizaba a la entidad a captar imágenes de los usuarios con fines publicitarios, viéndose obligada a otorgar su consentimiento para que su hijo menor de edad pudiera acceder. En ese sentido, al final del formulario solo figuraba una única casilla para marcar "*Aceptar*" sin que existiera la opción de rechazar.

En la resolución PS 104/2023, la AEPD hace referencia al artículo 4.11 del RGPD, que define el consentimiento como una manifestación libre, específica, informada y clara por la cual el interesado acepta el tratamiento de sus datos personales. El artículo 7 del RGPD añade que el responsable debe demostrar que el consentimiento fue otorgado, éste debe poder ser fácilmente retirado, y la finalidad para la que se solicita dicho consentimiento debe distinguirse claramente de otros temas en los formularios.

En el caso presentado, se considera que el parque vulneró el artículo 7 al condicionar el acceso al recinto a la firma de un consentimiento que no era libre ni específico. En consecuencia, la Agencia impone una sanción de 2.000 euros por infracción del artículo 7 del RGPD.

## Una entidad será responsable o encargada del tratamiento de datos según la situación concreta, sin que las partes puedan decidir su rol arbitrariamente

La AEPD ha hecho pública una resolución de procedimiento sancionador en la que se imponen dos multas de 2.500.000 euros cada una, por sendas infracciones de los artículos 5.1.a) (principio de lealtad y transparencia) y 5.2. (responsabilidad proactiva) del RGPD, y que resulta de gran interés al recoger de manera sistemática una variedad de conceptos y obligaciones que conciernen a la práctica totalidad de los sujetos obligados por la normativa de protección de datos en su día a día.

La resolución analiza el tratamiento de datos personales por parte de una comercializadora de energía que hacía uso de un tercero para la promoción telefónica de sus productos y servicios. El promotor realizaba llamadas telefónicas promocionales para captar clientes en nombre de esta comercializadora. Según indica la resolución, en estas llamadas se hacía uso de prácticas fraudulentas con objeto de incrementar las captaciones, usando datos e información engañosa, generando confusión entre los contactados e incumpliendo las obligaciones de transparencia impuestas por el RGPD.

La reclamada argumentaba que las llamadas las llevaba a cabo el promotor bajo su propia responsabilidad, pero, en su resolución, la AEDP, citando las conclusiones de las directrices 07/2020 sobre los conceptos de "responsable del tratamiento" y "encargado del tratamiento", establece que el rol de responsable corresponde a la reclamada, dado que existía un argumentario de ventas impuesto por esta, así como instrucciones claras y documentadas sobre cómo llevar a cabo la comercialización de sus servicios, actuando, pues, el promotor como encargado del tratamiento. La AEPD concluye que una entidad actuará como responsable o encargado del tratamiento dependiendo de la realidad de la situación concreta, sin que las partes puedan decidir su rol arbitrariamente según su conveniencia.

Por otro lado, la AEPD insiste en la necesidad de que los responsables del tratamiento realicen un control exhaustivo, constante y minucioso de la actividad de sus encargados del tratamiento, y en que lo hagan de manera documentada y acreditada de cara a poder demostrarlo.

Por último, y por destacar otro de los puntos de la extensa resolución, la AEPD señala que los incumplimientos de los principios de

lealtad y transparencia, y de responsabilidad proactiva recogidos en el artículo 5 del RGPD son sancionables de por sí, sin necesidad de encuadrarlos en otros tipos más concretos, y sin que ello suponga una violación del principio de tipicidad.

## La AEPD cambia de opinión y considera que entregar un paquete a un tercero no debe ser objeto de sanción

La AEPD ha emitido una serie de resoluciones (EXP202314031, EXP202313840, EXP202313995 y EXP202314242) de las que puede deducirse un cambio de criterio en lo que respecta a la práctica de empresas de mensajería de entregar paquetes a terceros distintos a su destinatario original.

Recientemente, la AEPD llegó a imponer, por hechos similares, una sanción de 70.000 euros a una empresa de mensajería, mientras que, en esta nueva serie de resoluciones, la AEPD considera que entregar un paquete a un vecino, comercio aledaño al destinatario o portero de comunidad de propietarios no constituye una actividad que deba ser objeto de sanción.

La AEPD argumenta que, si bien es cierto que la entrega de los paquetes a estos terceros supone poner en su conocimiento información personal del destinatario sin su permiso, estos datos serían normalmente solo su nombre, apellidos y dirección, información ya conocida por el que recibe el paquete en nombre del destinatario. Es por ello que la AEPD considera esta práctica de menor relevancia y archiva los expedientes sin sanción.


## El tutor legal, encargado de proteger y gestionar los intereses de una persona bajo su cuidado, es responsable del tratamiento de datos, aunque forme parte del entorno personal de dicha persona

El Tribunal de Justicia de la Unión Europea (TJUE), en la sentencia de 11 de julio de 2024 (C-461/22), interpreta que la actividad de curador ejercida a título profesional por una persona física, aunque forme parte del entorno personal de la persona sujeta a su curatela, implica la condición de responsable del tratamiento de los datos personales en su posesión relativos a esa persona, y la consecuente obligación de cumplir con todas las previsiones del RGPD que sean de aplicación, incluida la atención al derecho de acceso del citado artículo 15 del RGPD.

Dicha sentencia tuvo lugar después de que un ciudadano alemán sujeto a curatela ejercitara el derecho de acceso con base en el artículo 15 del RGPD ante su antiguo curador, abogado nombrado en el marco de su actividad profesional. El órgano jurisdiccional remitente planteó la cuestión prejudicial de si el curador podía ser considerado un responsable del tratamiento desde la óptica de la normativa de protección de datos.

## Las asociaciones pueden reclamar en nombre del interesado el incumplimiento del derecho de información previa, entendiéndose una vulneración "como consecuencia de un tratamiento"

Una importante compañía tecnológica y la Federación de Organizaciones y Asociaciones de Consumidores de Alemania comenzaron un litigio relativo a la supuesta infracción por parte de la primera de la normativa alemana sobre protección de datos personales, que constituía, a la vez, una práctica comercial desleal, una violación de la legislación en materia de protección de los consumidores y un incumplimiento de la prohibición del uso de condiciones generales nulas. En este marco, el órgano jurisdiccional remitente cuestionó si, con base en el artículo 80.2 del RGPD, una asociación estaría legitimada para basar una demanda en el incumplimiento del derecho de información previa, al no tratarse estrictamente de un derecho vulnerado "como consecuencia de un tratamiento".

En este caso, en la sentencia del 11 de julio de 2024 C-757/22**,** el Tribunal de Justicia de la Unión Europea (TJUE ) resuelve que la obligación de información forma parte de los derechos que el artículo 80 tiene por objeto proteger, y que, de incumplirse, se estarían perjudicando los principios de transparencia y lealtad del tratamiento, además de que el consentimiento libre podría verse

perjudicado. Por todo esto, debe considerarse que la vulneración del derecho de información constituye una vulneración de los derechos del interesado "como consecuencia de un tratamiento". Además, el responsable del tratamiento debe comunicar al interesado afectado la información relativa a los fines de dicho tratamiento y a los destinatarios de los datos de forma concisa, transparente, inteligible y fácilmente accesible, con un lenguaje claro y sencillo, y, a más tardar, en el momento de su recogida.

## Anulan la multa de 250.000 euros impuesta por la AEPD en relación con la activación del micrófono y la geolocalización de los dispositivos móviles de los usuarios en una app

Mediante resolución de 10 de junio de 2019**,** la AEPD impuso a una organización profesional una multa de 250.000 euros por la infracción del principio de transparencia en el tratamiento de datos recogido en el artículo 5.1.a) Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 (RGPD), en relación con el uso de determinadas funcionalidades de su aplicación oficial. Concretamente, el hecho denunciado tenía relación con la activación del micrófono y la geolocalización de los dispositivos móviles de los usuarios, con la finalidad de detectar fraudes respecto a los contenidos audiovisuales de los partidos de fútbol.

El Tribunal Supremo, en su sentencia de 15 de julio de 2024, confirma que la información facilitada en la descarga de la app cumple con las exigencias previstas por el RGPD. No obstante, aclara la aplicación del principio de transparencia en supuestos en los que dicha app recopila datos personales, tanto en el momento de la instalación como de forma prolongada en el tiempo y sin previo aviso.

El Tribunal Supremo interpreta los límites del deber de transparencia y los conecta con el alcance sancionador de la AEPD, estableciendo que:

a. El deber de transparencia debe ajustarse a las circunstancias específicas del tratamiento de datos. En este supuesto, la obligación de transparencia se aplica tanto al instalar como al operar una aplicación móvil por cuanto que el uso prolongado puede conllevar que los usuarios olviden la información y se requieran mecanismos informativos adicionales.

b. La AEPD puede exigir la existencia un aviso específico en el móvil cada vez que se activa el micrófono, por considerarse una medida proporcionada.

c. No obstante, la exigencia de este aviso específico no está expresamente prevista en el RGPD ni se desprende de la Ley Orgánica 3/2018, de 5 de diciembre. La potestad sancionadora se rige por el principio de previsibilidad, por lo que la AEPD no puede extender el alcance de la exigencia de transparencia a límites que no son previsibles.

d. No era razonable dar por sentado que el principio de transparencia exigía un aviso de privacidad cada vez que la aplicación activase el micrófono del móvil. La AEPD no puede sancionar directamente el incumplimiento de garantías concretadas a posteriori y que no eran previsibles en el momento de realizar la conducta sancionada.

En conclusión, el Tribunal Supremo considera que se cumplió con el principio de transparencia en el tratamiento de datos personales obtenidos mediante la aplicación, ya que no era previsible la exigencia de incorporar un aviso informativo específico, y, en consecuencia, anula la sanción impuesta por la AEPD.

## La Corte Constitucional de Colombia aclara que la inteligencia artificial no puede sustituir al juez en la toma de decisiones

Al resolver una acción de tutela, la Corte Constitucional de Colombia efectúo consideraciones relevantes sobre el uso de la inteligencia artificial (IA) por parte de los jueces a la hora de resolver procesos judiciales.

En la sentencia T-323 de 2024, el tribunal concluyó que la IA no puede remplazar al juez en la toma de decisiones judiciales, sin importar la complejidad del asunto. Por lo tanto, será viable el uso de estos sistemas para gestiones administrativas o documentales, pero no para labores de creación de contenido ni interpretación de hechos o pruebas y, mucho menos, la solución de casos.

## La autoridad de control no está obligada a adoptar una medida correctora en todos los casos de infracción ni a imponer una multa

El Tribunal de Justicia de la Unión Europea (TJUE) ha dictaminado en el asunto C-768/21, originado en Alemania después de que una empleada de una Caja de Ahorros accediera sin autorización a datos personales de un cliente. La Caja de Ahorros no informó a dicho cliente, ya que su delegado de Protección de Datos consideró que no había un riesgo elevado para sus derechos. La empleada aseguró por escrito que no había copiado ni compartido los datos y que no lo haría en el futuro. Además, la Caja de Ahorros tomó medidas disciplinarias contra ella y notificó la infracción al comisionado de protección de datos del Land.

El cliente, al enterarse de la situación, presentó una reclamación ante la autoridad de control, quien decidió no adoptar medidas correctoras. Insatisfecho, el cliente recurrió a un tribunal alemán, solicitando que se ordenara a la autoridad de control actuar contra la Caja de Ahorros e imponer una multa.

En su sentencia, el TJUE ha dictaminado que las autoridades de protección de datos no están obligadas a adoptar medidas correctoras en todos los casos de infracción del Reglamento General de Protección de Datos (RGPD). En particular, no es necesario imponer una multa si el responsable del tratamiento ha tomado medidas adecuadas por iniciativa propia para subsanar la infracción y prevenir su repetición.

El TJUE concluye que las autoridades de control tienen un margen de apreciación para decidir cómo subsanar las deficiencias constatadas, siempre que se garantice un nivel coherente y elevado de protección de datos personales. Corresponde al tribunal alemán verificar si la autoridad de control respetó estos límites.

# 4. Actualidad

## Publicado el Reglamento Europeo de Inteligencia Artificial en el Diario Oficial de la Unión Europea

El 12 de julio se publicó en el Diario Oficial de la Unión Europea (DOUE) el Reglamento de Inteligencia Artificial (RIA); una norma que no será aplicable con carácter general hasta el 2 de agosto de 2026, es decir, 24 meses después de su entrada en vigor el pasado 2 de agosto de 2024.

Sin embargo, algunas previsiones de la norma son aplicables en plazos distintos. Por ejemplo, las prohibiciones de determinadas prácticas relacionadas con la IA serán ya aplicables a partir del 2 de febrero de 2025.

Además, las previsiones relativas a los organismos notificados, a los sistemas de IA generales pero que implican riesgos sistémicos, al sistema de gobernanza de la IA en Europa, y buena parte del régimen sancionador serán aplicables a partir del 2 de agosto de 2025, con lo que la base organizativa estará ya lista para cuando sea exigible el conjunto más sustancial de obligaciones.

Por último, a partir del 2 de agosto de 2027 será aplicable la regulación de ciertos sistemas de IA de alto riesgo, en concreto los que sean componentes de seguridad de ciertos productos o constituyan en sí mismos dichos productos, caracterizados por requerirse una evaluación de seguridad para su comercialización o puesta en servicio (por ejemplo, máquinas, juguetes, ascensores o productos sanitarios).

## La Agencia Española de Protección de Datos ha presentado un informe sobre la influencia de los patrones adictivos en Internet, y en especial sobre los menores de edad

Un informe de la Agencia Española de Protección de Datos (AEPD) pone de manifiesto cómo, en muchos casos, los proveedores de numerosas plataformas y aplicaciones implementan patrones de diseño engañosos y adictivos para prolongar el tiempo que los usuarios permanecen en sus servicios, o para incrementar su nivel de compromiso y la cantidad de datos personales que se recogen sobre ellos.

Además, este impacto adverso de las estrategias adictivas es considerablemente mayor cuando se utilizan para tratar datos personales de personas vulnerables, como es el caso de los niños y adolescentes.

La AEPD va a promover que el Comité Europeo de Protección de Datos incluya los patrones adictivos en las directrices que se están preparando sobre la interrelación entre el RGPD y la DSA, debido al elevado impacto que estas prácticas poseen sobre el derecho a la protección de datos en entornos digitales.

## El CEPD propone que se designen las autoridades de control de protección de datos como entidades supervisoras de la aplicación del RIA

Los motivos para esta declaración del Comité Europeo de Protección de Datos (CEPD) son principalmente la experiencia ya adquirida por las autoridades de control en materia de IA, los beneficios de instaurar un punto único de contacto para los operadores de mercado, y su grado de independencia, soslayando, además, potenciales discrepancias entre las resoluciones de ambas autoridades supervisoras.

Dado que hay Estados Miembros que han iniciado procesos legislativos para la creación de dichas entidades supervisoras contempladas en el RIA de manera paralela a las Autoridades de control de protección de datos, el CEPD remarca la importancia de que las entidades colaboren y cooperen en los futuros procesos con base en el artículo 4(3) del Tratado de la Unión Europea.

## El CEPD permite que las instituciones de la UE utilicen sistemas de IA generativa si respetan la normativa en materia de protección de datos

El Comité Europeo de Protección de Datos (CEPD) ha publicado las primeras orientaciones para garantizar el cumplimiento de la protección de datos para las instituciones de la Unión Europea (UE) al utilizar sistemas de inteligencia artificial generativa, cuyo contenido ofrece consejos prácticos e instrucciones sobre el tratamiento de datos personales en estos supuestos.

Con carácter general, se permite que las instituciones de la UE utilicen sistemas de inteligencia artificial generativa siempre que respeten la normativa aplicable, en particular, la normativa en materia de protección de datos.

Adicionalmente, las orientaciones tratan cuestiones relevantes como el desempeño del rol de los delegados de protección en la implementación de sistemas de IA generativa, la aplicación del principio de minimización de datos, o cómo informar a los interesados respecto al tratamiento de sus datos personales.

## La AEPD emite una guía sobre compra segura en internet junto con el INCIBE, AECOSAN y Policía Nacional

Atendiendo a la dimensión actual del comercio electrónico, la AEPD ha publicado una guía práctica sobre compra segura en internet cuyo contenido recoge los derechos que asisten a los usuarios en procesos de compra online, así como consejos y recomendaciones en el ámbito de la privacidad, la seguridad, el consumo y la persecución de prácticas fraudulentas.

La guía se estructura en varios apartados. En primer lugar, la AEPD ofrece recomendaciones de buenas prácticas previas al inicio de la compra online que ayudan a los usuarios a detectar fraudes y páginas de venta online falsas, así como a evitar ser víctima de phishing.

A continuación, la guía destaca los aspectos más relevantes en cuanto a la seguridad que ofrecen los medios de pago de uso común en el comercio online (transferencia bancaria, pago con tarjeta, etc.).

En el tercer apartado, la AEPD aglutina el conjunto de derechos y garantías que asisten a los usuarios en procesos de compra online (derecho de desistimiento, derechos sobre los datos personales, etc.).

Finalmente, en el apartado titulado “Cómo reclamar”, la guía establece las recomendaciones sobre los posibles canales que permiten a los usuarios interponer reclamaciones en supuestos en los que se haya incumplido alguna normativa.

## La OCDE publica un informe sobre los enfoques regulatorios de la inteligencia artificial en el sector financiero

El documento de políticas analiza, entre otras cosas, diferentes enfoques regulatorios para el uso de la IA en las finanzas en 49 jurisdicciones de la OCDE y no pertenecientes a la OCDE con base en la encuesta sobre enfoques regulatorios de la IA en las finanzas.

El informe destaca que la mayoría de las jurisdicciones cuentan con regulaciones adecuadas para la IA en finanzas, aunque reconocen posibles brechas como la falta de regulaciones específicas para la IA en este sector, que pocos reguladores han emitido.

## El Consejo de Europa firma el Convenio Marco sobre Inteligencia Artificial y los Derechos Humanos, la Democracia y el Estado de Derecho

Este convenio es el primer tratado internacional jurídicamente vinculante en este ámbito y tiene como objetivo "garantizar que las actividades que se desarrollan durante el ciclo de vida de los sistemas de IA son plenamente compatibles con los DDHH, la democracia y el Estado de derecho, a la vez que favorezcan el progreso tecnológico y la innovación".

Este convenio marco aplica tanto a autoridades públicas como a entidades privadas, y se establece un mecanismo de seguimiento para garantizar su cumplimiento, que incluye la cooperación internacional entre los Estados partes. Cada Estado tiene la flexibilidad de aplicar el convenio en su sistema legal, pero debe implementar medidas adaptadas a los riesgos de los sistemas de IA. Sin embargo, el convenio no regula la tecnología y es esencialmente neutral en materia tecnológica.

## La Comisión Europea publica un documento para ayudar a las empresas a conocer sus obligaciones sobre el 'Data Act'

El nuevo Reglamento de Datos de la Unión Europea o Data Act (Reglamento (UE) 2023/2854 del Parlamento Europeo y del Consejo sobre normas armonizadas para un acceso justo a los datos y su utilización) será plenamente aplicable desde el día 12 de septiembre de 2024, y, junto con el Data Governance Act (Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo relativo a la gobernanza europea de datos), tiene como objetivo incrementar la confianza en los mecanismos para compartir datos dentro de la Unión Europea.

En este sentido, la Comisión Europea ha publicado este compendio de preguntas y respuestas (FAQs) para ayudar a las entidades a comprender sus obligaciones de forma más detallada. Entre los temas tratados, cabe destacar a) la interacción de esta norma con otras normas europeas, b) cuestiones sobre *Internet-of-Things* (IOT), c) consideraciones sobre los usuarios, *data holders* y otros terceros involucrados, y d) establecimiento de condiciones justas, razonables y no discriminatorias, mecanismos de compensación y resolución de conflictos.

## La autoridad de control de Bélgica publica una guía sobre la utilización de modelos de inteligencia artificial y el Reglamento General de Protección de Datos

Este documento trata temas como a) la definición de los sistemas de IA, b) los requisitos para que estos cumplan con el RGPD, c) la garantía de los derechos de los interesados a través de la utilización de sistemas de IA, y d) los requisitos para cumplir con principios del RGPD, mantener los datos actualizados y asegurar la seguridad en los tratamientos.

Las orientaciones recogen de forma resumida los principales hitos que deben tenerse en cuenta a la hora de abordar esta tecnología desde la perspectiva de cumplimiento del RGPD.

## La AEPD publica unas orientaciones sobre obligaciones y responsabilidades por el uso de dispositivos móviles en los centros educativos

El uso de teléfonos móviles, tabletas y dispositivos inteligentes en las aulas de estudiantes ha crecido exponencialmente en los últimos años, lo que ha derivado en riesgos para la protección de los estudiantes. Por ello, la AEPD ha publicado un documento en el que se incluyen orientaciones para su utilización responsable y para el debido cumplimiento de la normativa de protección de datos personales.

Entre sus observaciones, resulta importante destacar que la AEPD desaconseja el uso en los centros educativos de estos dispositivos siempre que el fin pedagógico pretendido pueda conseguirse a través de otro recurso más idóneo. De acuerdo con el criterio de esta agencia, la utilización de dispositivos inteligentes en los centros educativos ha de superar positivamente el juicio de idoneidad, necesidad y proporcionalidad.

Asimismo, la AEPD recuerda que aquellos tratamientos de datos que se desvíen de la finalidad para la que estos son recabados deben considerarse ilícitos, pudiendo derivarse responsabilidades, no solo administrativas por infracciones de la normativa de protección de datos, sino también por daños y perjuicios, pudiendo considerarse, según el caso concreto, responsables solidarios los centros y las administraciones educativas.

## Chile: Avance legislativo e impactos de la nueva Ley de Datos Personales

El pasado 26 de agosto, el Congreso Nacional de Chile aprobó la nueva Ley de Protección de Datos Personales, que regula el tratamiento de los datos y fortalece los derechos de los titulares, alineándose con el Reglamento General de Protección de Datos de la Unión Europea. Una de las principales novedades es la creación de la Agencia de Protección de Datos Personales, encargada de supervisar el cumplimiento de la normativa y administrar el Registro Nacional de Sanciones y Cumplimiento, donde se llevará un registro de las sanciones impuestas a las empresas.

La Ley amplía los derechos de los titulares, incluyendo la portabilidad y supresión de datos. También impone a las empresas la obligación de realizar Evaluaciones de Impacto en Protección de Datos Personales cuando un tipo de tratamiento (por su naturaleza, alcance, contexto, tecnología utilizada o fines) pueda producir un alto riesgo para los derechos de las personas titulares de los datos.

Asimismo, destacan los deberes que recaen sobre los responsables del tratamiento, como el deber de secreto, información y transparencia, así como el establecimiento de políticas y medidas de seguridad adecuados para el tratamiento de datos. En esta misma línea, las sanciones por incumplimiento son más severas, con multas que pueden alcanzar las 20.000 UTM (US$1.418.000), y que pueden triplicarse en caso de reincidencia. La nueva Ley entrará en vigencia 24 meses después de su publicación en el Diario Oficial.

## Colombia: Los administradores de datos personales que usen sistemas de IA deberán ponderar la idoneidad y necesidad del tratamiento de dichos datos

Con el fin de asegurar el adecuado cumplimiento de la Ley 1581 de 2012, la Superintendencia de Industria y Comercio impartió lineamientos para los administradores de datos personales que utilicen sistemas de inteligencia artificial (IA).

Entre otras obligaciones, quienes utilicen estos sistemas deberán realizar una ponderación sobre la idoneidad, necesidad, razonabilidad y proporcionalidad del tratamiento de datos personales. Sumado a esto, previo al diseño y desarrollo del sistema de IA, es fundamental que se realicen estudios de impacto de privacidad y se implementen sistemas de administración de riesgos. La Circular Externa No. 002 de 2024 se puede consultar en este enlace.

**Alejandro Padín**
Socio · Madrid
alejandro.padin@garrigues.com

**Garazi Tomás**
Asociada · Bilbao
garazi.tomas@garrigues.com

**Antonio Durán**
Asociado · Málaga
antonio.david.duran@garrigues.com

**Adrián León**
Asociado · Alicante
adrian.leon@garrigues.com

**Ignacio Suárez**
Asociado · Madrid
ignacio.suarez@garrigues.com

**Javier Enebral**
Asociado · Madrid
javier.enebral@garrigues.com

**Sebastián Hassi**
Asociado principal · Chile
sebastian.hassi@garrigues.com

**Adolfo Gómez**
Asociado sénior · Colombia
adolfo.gomez@garrigues.com

Más información:

**Economía del Dato, Privacidad y Ciberseguridad**

GARRIGUES

Hermosilla, 3
28001 Madrid
**T** +34 91 514 52 00
info@garrigues.com

**Síguenos en:**