

GARRIGUES

**Newsletter  
Economía del  
Dato, Privacidad  
y Ciberseguridad**

Abril 2025

## Índice

1. La Comisión Europea continúa desgranando el Reglamento de Inteligencia Artificial: definición de sistema de inteligencia artificial y código de buenas prácticas para IA de uso general
2. Resoluciones de las autoridades de protección de datos
3. Sentencias
4. Actualidad

## 1. La Comisión Europea continúa desgranando el Reglamento de Inteligencia Artificial: definición de sistema de inteligencia artificial y código de buenas prácticas para IA de uso general

El pasado 6 de febrero, la Comisión Europea publicó las directrices para ayudar a los diferentes operadores del entorno de inteligencia artificial a analizar si se encuentran ante un sistema de inteligencia artificial en los términos del Reglamento (UE) 2024/1689 de Inteligencia Artificial. Además, el 11 de marzo, publicó el tercer borrador del Código de Buenas Prácticas para IA de uso general. En el siguiente artículo, desgranamos las claves de ambos documentos.

### Alejandro Padín Vidal

El pasado 6 de febrero, en atención de las previsiones establecidas en el artículo 96.1. f) del Reglamento IA, la Comisión Europea publicó las [directrices sobre la definición de sistema de inteligencia artificial](#), un que se unen a las publicadas 2 días antes sobre las prácticas prohibidas de inteligencia artificial, sobre las que ya publicamos anteriormente [este post](#).

Estas nuevas directrices tienen por objetivo tratar de ayudar a los diferentes operadores a identificar si se encuentran ante un sistema de inteligencia artificial que se encuentre regulado por el Reglamento de IA.

Las directrices vienen a tratar de concretar la definición de “**sistema de inteligencia artificial**” contenida en el artículo 3 (1) del Reglamento IA. Como se desprende de este artículo, y se matiza en las directrices, a la hora de analizar si estamos ante un sistema de inteligencia artificial, debemos encontrarnos ante un sistema cumpla todos estos requisitos:

- i. **Basado en una máquina** (*hardware* y *software*).
- ii. Diseñado para **funcionar con diferentes niveles de autonomía**, es decir, que pueda actuar con cierto grado de independencia con respecto a la actuación humana y tenga ciertas capacidades para funcionar sin intervención humana.
- iii. Que pueda mostrar **capacidad de adaptación tras el despliegue**, un elemento que no es requisito indispensable para estar dentro del ámbito de aplicación del Reglamento IA. Es decir, un sistema de inteligencia artificial puede tener tal consideración a efectos del Reglamento IA incluso aunque no tengan capacidad de adaptación tras el despliegue.
- iv. Que tenga **objetivos explícitos o implícitos**, es decir, tanto objetivos establecidos claramente que se codifican directamente por el desarrollador del sistema (por ejemplo, optimización de

costes en una función) como objetivos que no se establecen explícitamente, pero se pueden deducir del comportamiento o asunciones subyacentes del sistema.

- v. **Que infiera** de la información de entrada que recibe **la manera de generar resultados de salida**, es decir, no se basa en reglas predefinidas por humanos para ejecutar automáticamente operaciones.

Las directrices citan algunos ejemplos que no cumplirían este elemento y, por tanto, no serían un sistema de inteligencia artificial a los efectos del Reglamento de IA: sistemas de gestión de bases de datos para filtrar o seleccionar según determinado criterio o sistemas de análisis meramente descriptivo como podría ser un *software* que utiliza técnicas de estadística sobre datos de encuestas.

- vi. Los resultados de salida generados puedan ser, entre otros, **predicciones, contenido, recomendaciones o decisiones**. El Reglamento IA utiliza la expresión “como”, lo que quiere decir que el resultado de salida puede ser otro.
- vii. Que el resultado de salida pueda **influir en entornos físicos o virtuales**. La propia redacción del reglamento determina que esta influencia no es esencial para la calificación de un sistema como IA.

Si bien estas directrices aún no están formalmente aprobadas y no tienen carácter vinculante, pueden ayudar a interpretar alguno de los múltiples términos indefinidos contenidos en el artículo 3 del Reglamento de IA. Esto puede ser de especial utilidad, teniendo en cuenta que la mayor parte del tejido empresarial se encuentra revisando y clasificando, contrarreloj, los sistemas de inteligencia artificial que utilizan, desarrollan o introducen en el mercado.

## IA de uso general

El otro documento publicado por la Comisión Europea al que nos referimos es el tercer borrador del [Código de Buenas Prácticas para la Inteligencia Artificial \(IA\) de Uso General](#), elaborado por expertos independientes. Este documento es fundamental para detallar las obligaciones establecidas en el **Reglamento de IA**, proporcionando a los proveedores directrices claras para garantizar el cumplimiento normativo y fomentar el desarrollo de modelos de IA seguros y fiables.

Este tercer borrador presenta una estructura más simplificada y precisa en comparación con versiones anteriores. Se centra en una serie de compromisos de alto nivel, acompañados de medidas detalladas para su implementación efectiva. Entre los aspectos más destacados, se incluyen:

- **Transparencia y derechos de autor:** todos los proveedores de modelos de IA de uso general deben cumplir con obligaciones específicas en materia de transparencia y respeto a los derechos de autor. Para facilitar este proceso, se ha incorporado un formulario de documentación estandarizado que permite recopilar y presentar la información requerida de manera coherente y accesible.
- **Evaluación y mitigación de riesgos sistémicos:** para los proveedores de modelos de IA que puedan representar riesgos sistémicos (definidos en el Reglamento de IA), el código establece medidas específicas. Estas incluyen la realización de evaluaciones exhaustivas de los modelos, la implementación de estrategias de mitigación de riesgos, la notificación obligatoria de incidentes graves y el cumplimiento de estrictas normas de ciberseguridad.

La creación de este código ha sido un esfuerzo colaborativo, coordinado por la **Oficina Europea de IA**, queha contado con la participación activa de cerca de 1.000 partes interesadas, incluyendo proveedores de modelos de IA, intermediarios, representantes de la industria, sociedad civil, académicos y expertos independientes. Esta diversidad asegura que el código refleje una amplia gama de perspectivas y conocimientos especializados.

Para los profesionales del derecho especializados en el mundo digital, este código representa una herramienta esencial. Ofrece un marco detallado sobre las responsabilidades y mejores prácticas para los proveedores de modelos de IA de uso general, facilitando la interpretación y aplicación del Reglamento de IA. Además, promueve la adopción de prácticas que equilibran la innovación tecnológica con la protección de los derechos fundamentales y la seguridad de los usuarios.

Se espera que el código definitivo esté listo en mayo de 2025, proporcionando a los proveedores una guía clara para demostrar el cumplimiento del Reglamento de IA antes de su plena aplicabilidad en agosto de 2025. La versión final incorporará las aportaciones recibidas durante esta última fase de consulta, asegurando que las directrices sean prácticas y adaptadas a las necesidades del sector.

### **Siguientes pasos**

La complejidad jurídica y técnica de esta nueva norma exige un esfuerzo de análisis y adaptación para todos los involucrados en las tareas de desarrollo de tecnología y en su cumplimiento regulatorio. Así lo demuestra el hecho de que la propia Comisión Europea esté publicando materiales de ayuda a la interpretación y aplicación de la norma.

## 2. Resoluciones de las autoridades de protección de datos

### La AEPD sanciona con 5 millones de euros a una compañía de seguros por la exfiltración de datos de millones de clientes

En septiembre de 2022 una compañía aseguradora sufrió un ataque de fuerza bruta contra el formulario de consulta de clientes a través del uso de credenciales de uno de sus corredores. Posteriormente, se produjo la exposición no autorizada a datos personales de más de 1,6 millones de clientes y exclientes, incluyendo nombre y apellidos, DNI, teléfono, dirección completa, estado civil, fecha y país de nacimiento, e incluso IBAN de las cuentas bancarias.

En su resolución [PS-00453-2023](#), la AEPD determinó que la entidad había infringido los artículos 5.1.f), 25, 32 y 35 del RGPD en tanto en cuanto (i) no garantizó una seguridad adecuada de los datos personales, incluyendo tanto el tratamiento no autorizado o ilícito derivado del ciberataque como la visualización y acceso a datos de exclientes por parte de los mediadores de seguros en el momento del incidente; (ii) con independencia de la brecha, las medidas de seguridad que había implantado eran insuficientes; (iii) en el momento del diseño de la aplicación o sistema en cuestión no tuvo en cuenta adecuadamente los principios de minimización y limitación de los datos; y (iv) tomando en consideración el volumen de datos tratados (incluyendo las categorías

especiales) y los riesgos de que terceros se apropien ilícitamente de los datos, debió haber realizado una evaluación de impacto sobre la protección de datos. Por todo ello, la aseguradora fue sancionada con 5 millones de euros.

### Una plataforma de 'streaming' es sancionada con 4,75 millones de euros por no proporcionar información adecuada sobre el tratamiento

La investigación comenzó en 2019 a raíz de dos quejas presentadas por Noyb (ONG austriaca comprometida con la privacidad) en representación de dos interesados ante la Autoridad de Protección de Datos Austriaca (Datenschutzbehörde) y posteriormente fueron remitidas a la Autoridad Neerlandesa de Protección de Datos (Autoriteit Persoonsgegevens), quién confirmó la comisión de varias infracciones del RGPD por parte de la entidad denunciada.

Concretamente, [en la resolución del 18 de diciembre de 2024](#) se constató la infracción del artículo 12 apartado 1 en relación con el artículo 13 apartados 1 y 2 del RGPD entre el 25 de mayo de 2018 y el 30 de julio de 2020 por la falta de información sobre las finalidades y bases de legitimación del tratamiento, los destinatarios de los datos, los plazos de conservación y las garantías empleadas en caso de realizar de

transferencias internacionales de datos fuera del Espacio Económico Europeo en su política de privacidad. Asimismo, la compañía no atendió correctamente las solicitudes de acceso planteadas, infringiendo así el artículo 12 apartado 1 en relación con el artículo 15 apartados 1 y 2 del RGPD entre el 25 de octubre de 2018 y el 19 de noviembre de 2020 porque, entre otros, no proporcionó específica sobre los datos personales utilizados y los destinatarios de estos.

### **La autoridad supervisora de protección de datos polaca impone una multa de 928.498,06€ a una entidad bancaria por no informar a sus clientes de una brecha de datos personales**

Un empleado de la entidad bancaria envió por error documentos de clientes de la reclamada a otra entidad bancaria en los que se incluían datos personales (nombres y apellidos, nombre de los progenitores, cuentas bancarias, domicilios, ingresos, etc.). La autoridad supervisora instó a la entidad a informar a los clientes afectados por la brecha, pero la reclamada no lo hizo alegando que el tercero que había accedido a los datos era también una entidad bancaria, por lo que estaba sujeta también al secreto bancario, deviniendo así una *trusted entity*.

La autoridad supervisora dictamina en su [resolución](#) que no es el *status* del tercero el que determina si es de confianza, sino la existencia de una relación directa (y permanente) entre el emisor y el receptor. En este caso, no existe dicha relación entre las entidades bancarias, por lo que no se puede asegurar que el tercero fuera de confianza. En consecuencia, la brecha debió ser comunicada a los interesados. Por tal motivo, la autoridad supervisora impuso a la entidad una multa de 928.498,06€ por infracción del artículo 34 del RGPD.

### **La CNIL impone una multa de 40.000 euros a una compañía del sector inmobiliario por realizar una**

### **monitorización excesiva de sus empleados**

La compañía había instalado un *software* de vigilancia de la actividad de los empleados para los días en que teletrabajaban a fin de medir el tiempo de trabajo efectivo y la productividad de los trabajadores. Asimismo, había instalado cámaras de videovigilancia que captaban de forma continua imágenes y sonido de los trabajadores, tanto en zonas de trabajo como de descanso.

La CNIL considera en su [resolución](#) que la compañía no ha podido argumentar que exista un motivo suficiente para ejercer tal grado de vigilancia sobre los empleados, por lo que tilda estos tratamientos de excesivos. Además, en el marco de la investigación, la CNIL determina también que la compañía no ha informado debidamente a los empleados de estos tratamientos, así como que tampoco ha realizado una evaluación de impacto ni implantado medidas de seguridad adecuadas para dichos tratamientos. Por tanto, impone a la compañía una multa de 40.000 euros por la infracción de los artículos 6, 12, 13, 32 y 35 del RGPD.

### **Sancionada con dos multas una empresa de telecomunicaciones por infringir los artículos 5.1 f) y 32 del RGPD con motivo de una brecha de seguridad**

En fecha 26 de septiembre de 2022, la empresa de telecomunicaciones en cuestión notificó a la AEPD la concurrencia de una brecha de seguridad motivada por un acceso indebido por parte de un tercero no autorizado a datos personales tratados por la compañía en calidad de responsable, viéndose afectados más de un millón de clientes. Como consecuencia de esta notificación, se iniciaron unas investigaciones previas para determinar si había tenido lugar una vulneración de la normativa por parte de la entidad, ordenándose a la misma en último término que comunicase la brecha a los interesados afectados. Aunque en un principio la compañía se opuso a dicha orden, alegando

que los afectados por el incidente no eran identificables, tras llevarse a cabo una serie de requerimientos de información la entidad procedió a realizar dicha comunicación.

Como consecuencia de ello, la AEPD decide acordar la incoación de un procedimiento sancionador a la compañía por la presunta infracción de los artículos 5.1.f) (referido a los principios de integridad y confidencialidad) y 32 (referido a las medidas de seguridad) del RGPD, según lo tipificado en los artículos 83.4 y 83.5 del RGPD respectivamente. Finalmente termina proponiendo una sanción total de 1.300.000 euros por la comisión de las infracciones citadas.

En [la resolución del procedimiento sancionador](#), la AEPD confirma la sanción propuesta destacando las siguientes cuestiones:

1. En relación con la **naturaleza de los datos afectados**, recuerda que, en la actualidad, el número de teléfono -ya sea fijo o móvil- encaja a la perfección en la definición de lo que es un dato de carácter personal según el artículo 4.1) del RGPD. Por una parte, permite, por sí solo, hacer identificable a la persona a la que pertenece, aun cuando no venga acompañado de ningún otro dato. Por otra, es posible llegar a identificar, a través del número de teléfono, a la persona a la que pertenece sin realizar esfuerzos desproporcionados.
2. Por otro lado, **la AEPD argumenta que la conducta de la compañía sancionada es perfectamente subsumible en las infracciones citadas**, toda vez que en el procedimiento queda probado que la entidad no contaba con medidas apropiadas que garantizaran un nivel de seguridad adecuado al riesgo, teniendo en cuenta la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas.
3. En cuanto a la **falta de diligencia** de la compañía, la AEPD considera que queda patente, toda vez que la entidad no tenía implantadas medidas adecuadas de control de accesos en el aplicativo para empleados que estaba publicado en internet, ni medidas tendentes a generar alertas y bloqueos ante situaciones totalmente anómalas, no generándose ninguna alerta o evento de seguridad con advertencia inmediata al CSIRT-TE (el Equipo de Respuesta ante Incidentes de Seguridad de la entidad).
4. Por último, tampoco cree la AEPD que se dé una **falta de culpabilidad**, ya que entiende que las medidas que debieran haber sido aplicadas en el momento del incidente eran conocidas según el estado de la técnica y de coste asequible.

### Sancionadas dos entidades por publicar en internet imágenes de menores sin su consentimiento

En el primer caso, [la entidad reclamada había publicado en su página web una imagen de la reclamante, menor de edad, obtenida de un tercero -Telegram-](#) como acompañamiento a una noticia relativa al padre de la menor, personaje público. En el segundo caso, [la entidad reclamada publicó en su canal de Telegram una imagen de la reclamante, menor de edad, tomada en un espacio público](#) e incluida en un chat en el que se vertieron diferentes descalificaciones sobre su persona.

Asimismo, añade que, en este caso, la información recabada por los atacantes (la dirección MAC -*Media Access Control*- y los detalles del fabricante del dispositivo, la configuración de los puertos de la conexión asociada al teléfono fijo, los nombres de la red wifi y su contraseña, etc.) también debe considerarse dato de carácter personal por tratarse de información concerniente a personas físicas identificadas o identificables, ya que, con los datos afectados por la quiebra, es posible la identificación de los titulares de los mismos sin un esfuerzo exagerado o desproporcionado.

En ambos casos, la AEPD concluye que el tratamiento llevado a cabo por las reclamadas resulta excesivo, debido a que la difusión de la imagen de las menores era innecesaria para la finalidad de información que podría entenderse perseguida. En consecuencia, considera que los hechos son constitutivos de una infracción por vulneración del artículo 5.1. c) del RGPD.

Igualmente, entiende procedente graduar las sanciones debido a (i) la naturaleza, gravedad y duración de las infracciones, ya que la publicación de las imágenes, en ambos casos, se hizo por canales que posibilitaban una difusión inmediata y de gran alcance del contenido publicado; (ii) la intencionalidad, ya que la publicación fue directamente realizada por las reclamadas; y (iii) la afectación a los derechos de los menores. Por todo ello, en ambos casos se fija una sanción de multa administrativa de 5.000 euros, así como la medida definitiva de retirada del contenido publicado en el canal correspondiente.

### **La autoridad de control finlandesa ha impuesto una multa de 2,4 millones de euros a una empresa de servicio postal por incumplimiento de los artículos 5 y 6.1 del RGPD**

En este caso, la entidad, principal servicio postal del país, había creado un buzón de correo electrónico automático para comunicarse con sus clientes sin su autorización y, muchas veces, sin su conocimiento, sustituyendo la correspondencia postal tradicional. Además, el buzón electrónico se había vinculado a un conjunto más amplio de servicios, sin que se permitiese al cliente elegir sobre el uso o no de dicho buzón electrónico, ya que los diferentes servicios estaban vinculados entre sí en un único contrato. Por tanto, no se podía prescindir del buzón electrónico sin que también cesaran los demás servicios.

La autoridad finlandesa considera que el servicio solicitado por el cliente podría haberse prestado sin la creación automática de un buzón electrónico. Además, estima que el responsable del tratamiento tampoco

informó debidamente a sus clientes sobre la activación de tal buzón, a lo que se añaden una serie de configuraciones técnicas en el servicio que no cumplían con los requisitos que impone la normativa de protección de datos aplicable (por ejemplo, se incluía una función de selección activada automáticamente, así como una casilla de verificación premarcada).

El procedimiento sancionador culmina con la imposición de una multa de 2,4 millones de euros al responsable, al mismo tiempo que se ordena a la entidad la adopción de una serie de medidas correctivas.

### **Según la AEPD, el uso de plantillas biométricas encriptadas para el control de presencia constituye un tratamiento de datos biométricos**

La [Agencia Española de Protección de Datos \(AEPD\) ha sancionado con 20.000 euros a un colegio profesional por el uso de un sistema de control de presencia mediante el uso de la huella dactilar](#), implementado con anterioridad a la publicación de la Guía sobre tratamientos de control de presencia mediante sistemas biométricos de la AEPD, al no superar el levantamiento de la prohibición del tratamiento de datos biométricos y por no disponer de una evaluación de impacto adecuada al tratamiento.

La Autoridad considera que las plantillas biométricas encriptadas también son categorías especiales de datos personales, cuyo tratamiento está prohibido, salvo que concorra alguna de las excepciones contempladas en el artículo 9.2 del RGPD. Para el levantamiento de la prohibición, el colegio alegó que el uso del sistema estaba amparado en las obligaciones legales del Estatuto de los Trabajadores para el control laboral. La AEPD contraargumenta que la normativa no exige el uso de biometría, debiendo interpretarse las excepciones de manera restrictiva.

Aunque el colegio presentó una Evaluación de Impacto de Protección de Datos (EIPD), la AEPD evaluó su contenido, concluyendo que

el sistema no era funcional, necesario ni proporcional, especialmente porque ya existían métodos alternativos implementados como códigos alfanuméricos.

## **La CNIL impone una sanción de 50 millones de euros a un operador telefónico por mostrar publicidad encubierta sin el debido consentimiento**

La [Autoridad Francesa de Protección de Datos \(CNIL\)](#) ha impuesto una sanción de 50 millones de euros a un operador de telefonía por la introducción de publicidad sin el consentimiento adecuado en las bandejas de entrada de los usuarios de cuentas de correo de dicho operador, lo que constituye una infracción del artículo 34.5 del Código francés de Comunicaciones Postales y Electrónicas (que tiene como equivalente en España al artículo 21 de la Ley de Servicios de la Sociedad de la Información).

La CNIL señaló que la empresa tenía control sobre los anuncios en cuestión, dado que gestionaba y comercializaba los espacios dedicados a los anunciantes dentro de las bandejas de entrada de los usuarios. La autoridad valoró también, sin embargo, que se tomaron medidas correctivas al cesar el uso de este tipo de publicidad en noviembre de 2023 tras implementar un nuevo sistema de anuncios que permite distinguir claramente entre los anuncios y los correos electrónicos legítimos.

Adicionalmente, la autoridad identificó una infracción del artículo 82 de la Ley de Protección de Datos francesa, relacionada con el uso de cookies, ya que se constató que, a pesar de la retirada del consentimiento otorgado por parte del interesado, se seguía recopilando información a través de ellas.

## **Doble sanción en materia de videovigilancia por instalar un sistema que capta imágenes en vía pública sin contar con autorización administrativa y sin incluir la información preceptiva**

Se presentó un escrito de reclamación por la instalación de un sistema de videovigilancia, existiendo indicios de un posible incumplimiento de lo dispuesto en la normativa de protección de datos de carácter personal. La reclamación se fundamenta en que la parte reclamada ha instalado una cámara de videovigilancia que es susceptible de captar imágenes de la vía pública, sin que conste que cuente con autorización administrativa previa para ello.

La resolución [PS-00399-2023](#) de la AEPD sanciona a la parte reclamada, ya que, efectivamente, existía una cámara de videovigilancia susceptible de captar imágenes de la vía pública. Además, a pesar de que la cámara se encontraba señalizada mediante un cartel de zona videovigilada, en dicho cartel no se hacía referencia a la normativa vigente de protección de datos personales, no se incluía la información preceptiva sobre el responsable del tratamiento, ni tampoco a qué dirección debían dirigirse los interesados para el ejercicio de derechos.

Según la AEPD, los hechos son constitutivos de una doble infracción, imputable a la parte reclamada, por vulneración de los artículos 5.1.c) (minimización de datos) y 13 (información a facilitar al interesado) del RGPD, fijando una multa de 500 euros por cada una de ellas.

## **Sancionado con 10.000 euros un medio de comunicación por la publicación del nombre de una persona física**

En su resolución [PS-00335-2023](#), la AEPD impone una sanción a un conocido medio de comunicación por publicar en su página web una noticia sobre la divulgación en redes sociales de un vídeo, en la que se incluía tanto el nombre como la imagen de la parte reclamante, además de enlaces que conducían al vídeo objeto de la reclamación.

A juicio de la AEPD, la inclusión en publicaciones periódicas de la imagen de una persona o de un vídeo que contenga su

imagen y su voz de tal forma que se identifique a dicha persona o que la haga identificable - en este caso, además, junto con su nombre- supone un tratamiento de datos personales, debiendo conciliarse el derecho a la información y el derecho a la protección de datos. En el presente caso, la AEPD considera que el medio de comunicación ha tratado datos que resultaban excesivos al no ser necesarios para la finalidad perseguida.

Así, se impone a la entidad una sanción por importe de 10.000 euros por infracción del artículo 5.1.c) del RGPD, tipificada en el Artículo 83.5 del mismo reglamento y calificada como muy grave a efectos de prescripción.

### La Autoridad Italiana de Protección de Datos (IDPA) multa a OpenAI con 15 millones de euros por recopilar datos personales para entrenar a ChatGPT

En marzo de 2023, Italia se convirtió en el primer país occidental en bloquear temporalmente ChatGPT por motivos de privacidad, después de que la Autoridad Italiana de Protección de Datos (IDPA) anunciara una investigación sobre presuntas infracciones de las normas de protección de datos.

Como resultado de esas investigaciones, la autoridad identificó posibles infracciones por la falta de transparencia de OpenAI sobre el origen de los datos con los que han entrenado a ChatGPT -más concretamente de los datos personales correspondientes a ciudadanos italianos-, así como por un fallo de seguridad que habría ocurrido en marzo de 2023 y sobre el que la compañía no habría informado a las autoridades. Todo ello ha conllevado la imposición de una multa de 15 millones de euros a OpenAI, y de la obligación de explicar al público [cómo funciona ChatGPT](#), sobre todo en lo relativo a la recolección de datos para el entrenamiento del modelo.

El organismo de control recoge [en su resolución](#) que OpenAI también "procesó los datos personales de los usuarios" para entrenar el chatbot sin identificar primero una

"base legal adecuada" para la acción, violando el "principio de transparencia y las obligaciones de información relacionadas con los usuarios." Además, según dicho organismo, OpenAI no ha proporcionado mecanismos para la verificación de la edad, lo que conlleva el riesgo de exponer a menores de 13 años a respuestas inadecuadas para su nivel de desarrollo y autoconocimiento.

Finalmente, teniendo en cuenta que, en el transcurso de la investigación, la empresa estableció su sede europea en Irlanda, la autoridad italiana transmitió los documentos del procedimiento a la Autoridad Irlandesa de Protección de Datos (DPC), que se ha convertido en la principal autoridad de control de conformidad con el RGPD, para que pueda retomar la investigación en relación con posibles violaciones de carácter continuado.

### Se confirma la multa de 200.000€ a una empresa de telecomunicaciones por realizar un duplicado de tarjetas SIM a petición de un tercero distinto al titular de la línea

La AEPD [ha confirmado la multa de 200.000€ a una empresa de telecomunicaciones](#) por realizar un duplicado de una tarjeta SIM correspondiente a la línea de teléfono de la parte reclamante. La empresa indicó que el duplicado SIM fue solicitado por un tercero que conocía datos personales de la reclamante, y, aunque se siguieron protocolos de seguridad, un error puntual permitió la gestión fraudulenta. Además, bloqueó la SIM al día siguiente y reembolsó las cantidades afectadas.

La compañía alegó que había tomado medidas técnicas y organizativas adecuadas para identificar a los clientes y evitar fraudes en la duplicación de tarjetas SIM; que la duplicación de una tarjeta SIM no permite acceder directamente a información bancaria, contraseñas u otros datos confidenciales; y que implementó medidas de seguridad diligentes.

Sin embargo, la AEPD contestó que no se evalúa la idoneidad de las medidas, sino su incumplimiento en este caso específico, lo que

vulnera el art 6.1 del RGPD; que el duplicado SIM no otorga acceso directo a información bancaria, pero es un elemento necesario para realizar fraudes; que la negligencia de Vodafone se evidencia en la falta de control y supervisión de sus agentes; y que la empresa no puede eludir su responsabilidad alegando factores externos

### **Sancionado un propietario de una vivienda vacacional por recoger indebidamente imágenes del DNI de los huéspedes**

El 18 de octubre de 2024, la AEPD inició un procedimiento sancionador contra el propietario de una vivienda vacacional, tras una reclamación por la recogida indebida de imágenes del DNI de los huéspedes como parte del proceso de *check-in* online. Este tratamiento excedía lo necesario, según la normativa de protección de datos, vulnerando el principio de minimización de datos del artículo 5.1.c) del RGPD.

El procedimiento finalizó tras el reconocimiento de responsabilidad del reclamado y el pago voluntario de 600 euros el 11 de noviembre de 2024. La AEPD también ordenó ajustar los procedimientos a la normativa y eliminar cualquier dato personal almacenado en exceso, otorgando un plazo de dos meses para su cumplimiento.

La Agencia Española de Protección de Datos se reafirma [con esta resolución](#) en la necesidad de que los responsables adopten prácticas proporcionales y adecuadas en el tratamiento de datos personales, especialmente en actividades relacionadas con hospedaje y servicios digitales.

### **Sancionada una empresa de cartonajes por dos infracciones al RGPD**

La Agencia Española de Protección de Datos (AEPD) [resolvió imponer sanciones a una empresa de cartonajes](#) tras identificar dos infracciones al Reglamento General de Protección de Datos (RGPD).

La primera infracción, relacionada con el artículo 35, fue calificada como grave y sancionada con 200.000 euros debido a la falta de una Evaluación de Impacto en la Protección de Datos (EIPD). La entidad utilizaba un sistema de reconocimiento facial para el control horario de sus 99 empleados sin haber realizado la EIPD obligatoria, una medida esencial para evaluar riesgos inherentes a los datos biométricos, considerados de categoría especial por el RGPD. La empresa continuó usando el sistema durante años sin realizar las adaptaciones necesarias tras la entrada en vigor del RGPD en 2018, lo que agravó su responsabilidad.

La segunda infracción, sancionada con 20.000 euros, corresponde al incumplimiento del artículo 15 del RGPD, al no atender adecuadamente el derecho de acceso de un empleado. A pesar de las solicitudes del interesado, la denunciada no proporcionó la información completa ni dentro del plazo estipulado, incumpliendo así sus obligaciones legales. La AEPD también ordenó a la entidad la adopción de medidas correctivas, incluyendo garantizar el cumplimiento del derecho de acceso y ajustar sus procedimientos al RGPD para evitar futuras vulneraciones.

### **Un club deportivo es multado con 200.000 euros por infringir el artículo 5.1. c) del RGPD al instalar un sistema de reconocimiento facial para el acceso a su estadio**

Con fecha 22 de noviembre de 2022, la AEPD recibió una denuncia contra un club deportivo por la implementación de un sistema biométrico de reconocimiento facial para el acceso a su estadio. Este sistema, instaurado en abril de 2022, fue presentado por el club a los socios como ocasional y complementario a los métodos de acceso existentes (i.e. tarjeta física, digital en el móvil y código QR). La denuncia alegaba que el sistema restringía libertades y derechos fundamentales, y que su falta de proporcionalidad hacía que, incluso, el consentimiento de los interesados no fuera suficiente para legitimar el tratamiento de datos.

Con fecha 14 de diciembre de 2023, la AEPD acordó iniciar un procedimiento sancionador contra el club por la presunta infracción de los artículos 5.1.c) (minimización de datos) y 9 del RGPD (tratamiento de categorías especiales de datos personales), tipificados ambos en el artículo 83.5.a) del RGPD. Además, ordenó como medida provisional la suspensión temporal de todo tratamiento de datos personales relativos a la solución de reconocimiento facial para el acceso al estadio. Finalmente termina proponiendo una sanción de 200.000 euros por la comisión de cada una de las infracciones citadas.

En la [resolución del procedimiento sancionador](#), la AEPD confirma la sanción impuesta respecto de la infracción del artículo 5.1.c) del RGPD, y ordena tanto la prohibición definitiva del tratamiento de datos mediante reconocimiento facial como la supresión de cualquier registro donde tuviera almacenados los datos biométricos, destacando las siguientes cuestiones:

1. El tratamiento de los datos personales debe cumplir con los **principios establecidos en el artículo 5 del RGPD**, que incluyen la licitud, lealtad, transparencia, limitación de la finalidad, minimización de datos, exactitud, limitación del plazo de conservación, integridad y confidencialidad, y responsabilidad proactiva. Estos principios aseguran que los datos se traten de manera adecuada y respetando los derechos de los interesados. La AEPD destaca en su resolución que el tratamiento de datos biométricos por parte del club no cumple con estos principios, especialmente en lo que respecta a la minimización de los datos.
2. En cuanto a la **necesidad y proporcionalidad del tratamiento**, la AEPD concluye que el tratamiento de datos biométricos mediante el sistema de reconocimiento facial no superaba el referido juicio de necesidad y proporcionalidad. La evaluación de la necesidad implica determinar si el tratamiento es esencial para alcanzar la finalidad perseguida y si no existen otros

medios menos intrusivos para lograr el mismo objetivo. En este caso, la AEPD determina que existían métodos menos intrusivos, como el uso de tarjetas físicas o digitales que podían alcanzar los mismos objetivos sin la necesidad de tratar datos biométricos.

3. Por otro lado, la AEPD subraya en su resolución que el tratamiento de datos biométricos por parte del club no cumplía con las condiciones necesarias para levantar la prohibición del tratamiento de **categorías especiales de datos**, ya que no se demostró que el consentimiento explícito de los abonados fuera suficiente para justificar el tratamiento en términos de necesidad y proporcionalidad.

No obstante, la AEPD no entra a valorar el incumplimiento del artículo 9 del RGPD, ya que considera que, siendo un tratamiento que no ha superado el juicio de necesidad y proporcionalidad, no debe valorar la legitimación de la base jurídica del mismo.

### Se insta a una entidad de intermediación en operaciones con valores a que atienda el derecho de acceso solicitado por la parte reclamante

La parte reclamante interpuso una reclamación frente a una entidad de intermediación en operaciones con valores porque, tras ejercer el derecho de acceso a sus datos personales frente a dicha entidad, esta le contestó que tenía consideración de sujeto obligado de conformidad con lo dispuesto en el artículo 2.1.i) de la Ley 10/2010, de 28 de abril, de prevención de blanqueo de capitales y financiación del terrorismo (LPBCFT) y que, de acuerdo con el artículo 32.2 de la citada ley, estos sujetos no tenían obligación de atender los derechos establecidos en los artículos 15 a 22 del RGPD.

A este respecto, [en su resolución](#) la AEPD alega que la parte reclamada únicamente transcribe el artículo 32 de la LPBCFT en su contestación, pero no acredita haber remitido la información necesaria respecto a los datos no sujetos a la limitación, es decir, la confirmación de si se

tratan sus datos o no, el acceso efectivo a los mismos, y acceso a la información sobre el tratamiento de acuerdo con el artículo 13 del RGPD. Es decir, la excepción del artículo 32 de la LPBCFT no permite que pueda obviarse la solicitud como si no se hubiera planteado, dejándola sin respuesta, por lo que condena a la entidad a facilitar la referida información.

## **La autoridad de protección de datos de Cataluña ha sancionado con una multa de 30.000 euros a una entidad de servicios de atención sanitaria por acceder a una historia clínica**

La Autoridad de Protección de Datos de Cataluña ha sancionado con 30.000 euros a una entidad de servicios de atención sanitaria de gestión pública por acceder hasta en nueve ocasiones al historial clínico de una persona sin su consentimiento. No obstante, la multa ha quedado reducida a 24.000 euros al haber reconocido su responsabilidad, lo que ha supuesto una reducción del 20%.

Los hechos ocurrieron entre mayo y julio de 2023, cuando una profesional de la entidad accedió en nueve ocasiones a la historia clínica de una mujer de forma indebida. Los accesos no estaban relacionados con ninguna actuación asistencial o de diagnóstico, porque la afectada nunca había sido atendida por esta facultativa ni había sido paciente de ese centro, por lo que no había ningún tipo de relación entre ellas. La reclamante detectó lo ocurrido cuando solicitó un informe detallado de accesos a su historial.

Por todo ello, la Autoridad de Protección de Datos de Cataluña considera que la organización pública ha infringido el artículo 5.1.f) del RGPD (principio de integridad y confidencialidad).



### 3. Sentencias

#### **El Tribunal General de la UE reafirma la capacidad de la EDPB para exigir investigaciones adicionales cuando las decisiones preliminares de una autoridad de control principal no abordan adecuadamente los aspectos relevantes de un caso**

El caso surge de una disputa entre la Comisión de Protección de Datos de Irlanda (DPC) y el Comité Europeo de Protección de Datos (EDPB). La Autoridad Irlandesa, actuando como la autoridad de control principal, había emitido decisiones preliminares sobre el tratamiento de datos por parte de Facebook, Instagram y WhatsApp. Sin embargo, otras autoridades de control no estaban de acuerdo con estas decisiones y presentaron objeciones relevantes y fundamentadas, por lo que la Autoridad Irlandesa remitió el asunto a la EDPB para resolver las disputas en el marco del mecanismo de coherencia del RGPD.

En las decisiones vinculantes del EDPB de diciembre de 2022, el EDPB instruyó a la Autoridad irlandesa a ampliar su investigación y emitir nuevas decisiones preliminares. La DPC impugnó estas decisiones ante el Tribunal General, alegando que el EDPB había excedido su competencia. Sin embargo, en su [sentencia de 29 de enero de 2025, asuntos acumulados T-70/23 y T-84/23](#), el Tribunal General desestimó las acciones de la Autoridad Irlandesa y confirmó la competencia del EDPB para exigir una nueva investigación y la emisión de nuevas decisiones preliminares.

#### **La excepción a la obligación de informar al interesado se aplica a todos los datos personales que el responsable del tratamiento no haya obtenido directamente**

El Tribunal Supremo de Hungría plantea una petición de decisión prejudicial que tiene por objeto la interpretación de los artículos 14, apartados 1 y 5, letra c), 32 y 77, apartado 1, del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 106 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales.

En el contexto de la emisión de un certificado de vacunación contra el Covid-19, un interesado interpone una reclamación contra la administración húngara responsable de emitir dicho certificado, alegando que no cumplió con su deber de información.

La administración emisora del certificado indica que no está obligada a facilitar información sobre el tratamiento de datos personales, ya que, al amparo del artículo 14.5.c) RGPD, la obtención de los datos personales está prevista en la normativa nacional húngara y, en consecuencia, los datos (i) se obtuvieron mediante otro organismo de la administración, y (ii) fueron generados por la administración emisora en el ejercicio de sus funciones.

El tribunal húngaro competente indicó en su sentencia que la excepción del artículo 14.5 del RGPD no es aplicable en este caso, ya que en el contexto de los certificados de inmunidad se generan datos que el responsable no obtiene mediante otros organismos, sino que él mismo produce en el ejercicio de sus funciones (como, por ejemplo, el código QR incorporado a la tarjeta).

En el proceso de casación, el Tribunal Supremo de Hungría suspendió el procedimiento y consultó al TJUE si el artículo 14.5.c) del RGPD debe interpretarse en el sentido de que la excepción a la obligación del responsable del tratamiento de informar al interesado se aplica únicamente a los datos personales obtenidos de terceros, o si también se extiende a los datos personales generados por el propio responsable en el ejercicio de sus funciones.

En su sentencia de 28 de noviembre de 2024, [asunto C-169/2023](#), el TJUE responde que el artículo 14.5.c) RGPD debe interpretarse en el sentido de que la excepción a la obligación de información al interesado por parte del responsable del tratamiento afecta indistintamente a todos los datos personales que el responsable del tratamiento no haya obtenido directamente del interesado, hayan sido obtenidos por el responsable del tratamiento de una persona distinta del interesado, o generados por el propio responsable del tratamiento en el ejercicio de sus funciones.

## El Tribunal Supremo admite un recurso de casación sobre los deberes de transparencia de la Administración Pública en el uso de programas informáticos

En su [auto del 14188/2024](#), el Tribunal Supremo ha admitido a trámite el recurso de casación contra una sentencia de la Audiencia Nacional que avalaba la negativa del Ministerio de Transición Ecológica a proporcionar el código de BOSCO, la aplicación desarrollada para decidir sobre la concesión del bono social eléctrico. El motivo era que se consideraba que divulgar el código y la información podría suponer una vulneración de los derechos de autor, de la protección de los datos personales y de la seguridad de la aplicación.

Cuando se resuelva por el Tribunal Supremo, este caso podría sentar un precedente sobre la transparencia en el uso de programas y algoritmos por parte de las administraciones públicas y la posible limitación del acceso a la información bajo argumentos de propiedad intelectual, protección de datos o seguridad.

## Se confirma la sanción al CSIC por publicar en internet información incorrectamente anonimizada

En su [sentencia de 6091/2024](#), la Audiencia Nacional ha confirmado la sanción de apercibimiento impuesta por la AEPD al Centro Superior de Investigaciones Científicas (CSIC) por haber publicado un documento que revelaba la identidad de una persona que ejerció un derecho de acceso a información pública de dicho organismo. Aunque en el documento se colocaba un rectángulo en negro encima de los datos personales, el texto no era eliminado y se podía acceder a él utilizando un buscador de internet o un editor de PDF, no adoptando, por tanto, todas las medidas necesarias e infringiendo los artículos 5.1.f) y 32 RGPD.

Además, si bien el CSIC alega que la persona que ejerció el derecho de acceso a la información pública era una persona con un cargo público en el ámbito de la política, y que, por tanto, sería de interés público conocer la identidad de esa persona, la Audiencia Nacional confirma que la información solicitada no estaba vinculada con dicha condición de cargo público, realizándose en una esfera privada de actuación.

## Los Estados miembros pueden establecer normas más específicas para garantizar la protección de los derechos y libertades, pero sin eludir las obligaciones de otras disposiciones del RGPD

El asunto [C-65/23](#) deriva de una petición de decisión prejudicial planteada por el Bundesarbeitsgericht (Tribunal Supremo de lo Laboral de Alemania), mediante resolución de 22 de septiembre de 2022, recibida en el Tribunal de Justicia el 8 de febrero de 2023.

El caso surgió a raíz de la denuncia interpuesta por un trabajador de una compañía y, a su vez, presidente del comité de empresa a raíz de la transferencia de datos personales de los trabajadores de dicha compañía desde un programa informático a un servidor de la sociedad matriz del grupo situado en Estados Unidos. Dicha transferencia se enmarcaba en la implementación de un nuevo sistema de gestión de personal, extralimitándose con respecto a lo pactado en diferentes acuerdos del comité. En este contexto, el trabajador presentó demanda ante los tribunales territorialmente competentes en Alemania (el Arbeitsgericht o Tribunal de lo Laboral, con posterior recurso de apelación ante el Landesarbeitsgericht o Tribunal Regional de lo Laboral) con la pretensión de obtener el acceso a determinada información, la supresión de datos que le concernían y la concesión de una indemnización.

No habiendo obtenido todavía satisfacción en relación con este último punto, el interesado recurrió en casación ante el Tribunal Supremo de lo Laboral (Bundesarbeitsgericht), que es el órgano remitente de varias cuestiones prejudiciales ante el TJUE. Las consideraciones del tribunal tras el análisis de las diferentes cuestiones concluyen afirmando que, aun cuando los Estados miembros se basen en el artículo 88 del RGPD para introducir, en sus respectivos ordenamientos jurídicos internos, «normas más específicas» a través de disposiciones legislativas o de convenios colectivos, también deben cumplirse las exigencias derivadas de las demás disposiciones del RGPD. Por ello, la empresa debió haber valorado los requisitos del RGPD para el tratamiento de datos, incluyendo el criterio de necesidad que se discutía en el caso concreto. El TJUE establece entonces que, en un convenio colectivo, el artículo 88 del RGPD no otorga a las partes un “cheque en blanco” para legitimar tratamientos de datos personales, por lo que pueden establecer normas nacionales específicas para la protección de datos en el ámbito laboral, pero sin eludir las obligaciones establecidas en otras disposiciones del RGPD.

Asimismo, en su sentencia de 19 de diciembre de 2024, el TJUE concluye que, en un convenio colectivo aprobado al amparo de ese artículo, el margen de apreciación de que disponen las partes para determinar el carácter de necesario de un tratamiento no impide al juez nacional ejercer un control jurisdiccional completo.

## La recopilación de los datos sobre los términos de cortesía "señor" o "señora" no puede ampararse en la base legal de la ejecución de un contrato

En su [sentencia de 9 de enero de 2025, C-394/23](#), el Tribunal de Justicia de la Unión Europea ha establecido que la recopilación de datos sobre el término de cortesía (como "señor" o "señora") durante la compra de billetes de tren no es compatible con el Reglamento General de Protección de Datos cuando su único objetivo es personalizar la comunicación comercial.

La empresa ferroviaria francesa SNCF Connect obligaba a sus clientes a indicar un término de cortesía con que dirigirse a ellos (es decir, "señor" o "señora") en el momento de la compra en línea de títulos de transporte. Este hecho se impugnó ante la autoridad francesa de protección de datos porque se consideraba que tal obligación es contraria al RGPD, en concreto al principio de minimización de datos, puesto que no parece necesaria para ejecutar el contrato de compra de un título de transporte de ferrocarril.

El Tribunal de Justicia recuerda que, para que un tratamiento de datos personales pueda considerarse necesario para la ejecución de un contrato, debe ser objetivamente indispensable para permitir la correcta ejecución de ese contrato. En este caso, el TJUE concluyó que el tratamiento de datos basado en términos de cortesía vinculados a la identidad de género no es objetivamente indispensable para ejecutar un contrato de transporte. Por lo tanto, el TJUE considera que la práctica de SNCF Connect es desproporcionada y no justifica la recopilación de datos personales relativos al término de cortesía, al existir alternativas menos invasivas y acordes con el RGPD.

### El TJUE limita la denegación de reclamaciones por exceso en solicitudes de acceso a datos

El caso (asunto C-416/23) se origina a partir de una reclamación presentada ante la agencia austríaca de protección de datos Datenschutzbehörde (DSB) por parte de un particular que denunció a una sociedad con la condición de responsable del tratamiento por no haber respondido en plazo a su solicitud de acceso a sus datos personales. Sin embargo, la DSB se negó a actuar respecto de dicha reclamación debido a su carácter excesivo, pues el interesado le había dirigido, en un intervalo de aproximadamente veinte meses, varias reclamaciones similares contra diferentes responsables del tratamiento.

Cabe recordar que, cuando una autoridad de control se enfrenta a solicitudes manifiestamente infundadas o excesivas (entendiéndose por excesivo, en opinión del CEPD, los casos de uso abusivo del artículo 15 del RGPD, en los que los interesados hacen un uso excesivo del derecho de acceso con la única intención de causar daños o perjuicios al responsable), existe la posibilidad de establecer una tasa razonable o de negarse a actuar. Sin embargo, [en su sentencia](#) el TJUE indica que permitir a las autoridades de control constatar el carácter excesivo de las reclamaciones por el único motivo de que su número es elevado podría comprometer un nivel de protección de datos personales adecuado. Si bien la multiplicación de las reclamaciones presentadas por una persona puede ser un indicio de la existencia de solicitudes excesivas cuando resulte que las referidas reclamaciones no están objetivamente justificadas por consideraciones relativas a la protección de los derechos que el RGPD confiere a esa persona, el número de sus reclamaciones no puede, por sí solo, justificar el ejercicio de la facultad prevista en el art. 57.4 RGPD.

## 4. Actualidad

### Se aprueba una nueva lista de publicidad no deseada validada por la AEPD: Lista Stop Publicidad

El pasado 31 de enero [la AEPD publicó en su sede electrónica](#) un nuevo fichero de exclusión publicitaria denominado **Lista Stop Publicidad** o LSP, como alternativa a la conocida Lista Robinson, que nació en 2009 y que, durante más de quince años, ha sido la única plataforma de exclusión publicitaria en España. El propósito de ambas consiste en que aquellos que no deseen recibir comunicaciones comerciales puedan limitar su envío, para lo cual bastará con que el interesado -persona física- inscriba sus datos gratuitamente a través de la página web de uno de estos sistemas, con la posibilidad de modificar sus datos o darse de baja en cualquier momento. No obstante, es importante tener en cuenta que, realizada la inscripción, las restricciones no entrarán en vigor hasta 30 días después.

Las diferencias fundamentales entre ambas listas radican en que la LSP (i) ofrece la posibilidad de inscribir en ella a personas fallecidas y (ii) bloquear no solo llamadas telefónicas, emails y mensajes SMS, sino también cuentas y perfiles en redes sociales y apps de mensajería.

Detrás de esta iniciativa de la creación de la LSP se encuentra la Asociación Española para la Privacidad Digital (Asociación EPD)

que, como se observa en la [resolución](#) de la AEPD, anteriormente presentó tres solicitudes que fueron denegadas.

### La Autoridad Italiana de Protección de Datos (GARANTE) ordena el bloqueo de DeepSeek en Italia

La Autoridad italiana de Protección de Datos (*Garante per la protezione dei dati personali*) [ha ordenado con efecto inmediato la limitación del tratamiento de datos de los usuarios italianos de las compañías chinas que proporcionan el servicio de chatbot de Deep Seek](#), como ya hizo con ChatGPT. Simultáneamente ha iniciado una investigación. Esta medida deriva de la respuesta a la petición de información del Garante a los gestores del sistema Hangzhou DeepSeek Artificial Intelligence y Beijing DeepSeek Artificial Intelligence, cuyo contenido fue considerado completamente insatisfactorio.

En dicho requerimiento, el Garante había solicitado que concretaran, en el plazo de 20 días, las siguientes cuestiones: (i) qué datos personales se recaban, (ii) de qué fuentes, (iii) con qué fines, (iv) cuál es la base jurídica de su tratamiento, (v) si se almacenan datos ubicados en China y (vi) si sus datos provienen del web scrapping. Por su parte, los operadores chinos han declarado que no operan en Italia y que, por ello, no se les puede aplicar la normativa europea.

En la misma línea que el Garante, otras autoridades de protección de datos europeas como la irlandesa o la francesa han comenzado a investigar y solicitar información a esta inteligencia artificial china.

## La Comisión Europea publica unas directrices sobre las prácticas prohibidas por el Reglamento de Inteligencia Artificial

La Comisión Europea ha publicado unas [directrices](#) que contienen el detalle y ejemplos prácticos para cada una de las prácticas de IA prohibidas por el artículo 5 del Reglamento de Inteligencia Artificial (p. ej. sistemas de IA que muestran texto o imágenes demasiado rápido para que la mente consciente lo registre, pero que sean capaces de influenciar actitudes y comportamientos, sistemas de IA que emiten sonido o imágenes de fondo que alteran el estado de ánimo del receptor, etc.).

En relación con los sistemas de IA para predecir el crimen, aun cuando los principales implementadores serían las fuerzas de seguridad, las directrices determinan que las actividades de entidades privadas también podrían estar cubiertas, por ejemplo, en supuestos en los que las fuerzas de seguridad encargan a entes privados tareas de prevención, investigación y persecución de delitos.

Aunque no sean vinculantes, estas directrices buscan asegurar una aplicación consistente, efectiva y uniforme del Reglamento de Inteligencia Artificial en los distintos Estados Miembros de la Unión Europea, sirviendo de guía para las autoridades competentes, los proveedores y los desarrolladores de sistemas de IA.

## La Autoridad Catalana de Protección de Datos (APDCAT) presenta un modelo pionero en Europa para desarrollar soluciones de IA respetuosas con los derechos fundamentales

La APDCAT ha presentado la primera [metodología](#) de Europa para la evaluación de impacto en los derechos fundamentales en materia de IA aplicada a cuatro casos concretos, la cual ha sido elaborada en el marco del grupo de trabajo de la red de delegados de protección de datos de entidades públicas y privadas de Cataluña (DPD en xarxa).

Los casos previstos pertenecen a ámbitos de actuación donde las soluciones de IA se utilizan cada vez más: (i) la educación (evaluación de los resultados del aprendizaje y predicción del abandono escolar), (ii) la gestión de personal (sistemas de apoyo a la toma de decisiones en la gestión de recursos humanos), (iii) el acceso a la asistencia sanitaria (tratamiento del cáncer basado en imágenes médicas) y (iv) los servicios de bienestar sociales (asistente de voz para personas mayores).

Esta metodología se desarrolla en tres fases: (i) planificación (descripción del sistema de IA y contexto de uso), (ii) análisis de riesgos (estimación del nivel de impacto sobre los derechos) y (iii) mitigación y gestión de riesgos.

## Chile adopta la nueva Ley de Datos Personales

La Ley Nº 21.719, publicada en el Diario Oficial el 13 de diciembre de 2024, establece un marco normativo actualizado para la protección y el tratamiento de datos personales en Chile. Esta ley modifica los estándares de seguridad de los datos de [la Ley 19.628 sobre Protección de la Vida Privada](#) e introduce nuevas bases de legitimación para su tratamiento, simplificando y ordenando de manera más efectiva la regulación en este ámbito.

Entre los principales cambios, destacan las nuevas disposiciones sobre los derechos de los titulares de los datos, las obligaciones de los responsables del tratamiento, la inclusión de nuevas categorías de datos, la transferencia internacional de datos y un régimen actualizado de sanciones.

Además, se crea la Agencia de Protección de Datos Personales como entidad de control, cuyo objetivo será velar por el cumplimiento de los derechos relacionados con la privacidad y protección de los datos personales, así como supervisar la ley y ejercer otras atribuciones clave en la materia.

Esta nueva normativa presenta importantes desafíos, especialmente en el ámbito tecnológico y a nivel de empresas. Estas deberán adoptar nuevos estándares de protección de los datos personales que gestionan, así como familiarizarse con estos, para cumplir de manera efectiva con la regulación.

La ley entrará en vigencia el 1 de diciembre de 2026.

## El Real Decreto 1154/2024, de 19 de noviembre, regula la expedición del pasaporte provisional y del salvoconducto

Este [decreto](#) establece las condiciones y procedimientos para la obtención de estos documentos, destinados a personas de nacionalidad española que se encuentren en el extranjero y no puedan obtener un pasaporte ordinario en un plazo razonable.

En lo referente a la protección de datos personales, el artículo 17 del decreto dispone que la expedición de pasaportes provisionales y salvoconductos se regirá por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de los mismos, así como por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

De forma más específica, se determina que los datos personales tratados a efectos del presente real decreto, incluida la imagen facial o fotografía del solicitante, se utilizarán únicamente para verificar su identidad y facilitar su viaje. El decreto también establece que las autoridades españolas garantizarán la

adecuada seguridad de los datos personales y que estos solo se conservarán mientras sea necesario.

En el caso de asistencia prestada a nacionales de otros Estados miembros de la Unión Europea o sus familiares, los datos personales no se conservarán más de 180 días tras su recogida; y, para personas españolas que hayan solicitado asistencia ante representaciones de otros Estados miembros, no más de dos años.

Al expirar el periodo de conservación, los datos personales serán suprimidos, y los documentos devueltos serán destruidos de forma segura.

## La AEPD respalda la conservación de datos en registros de hostelería, pero sugiere garantizar copias a los huéspedes

La AEPD ha emitido el [Informe del Gabinete Jurídico 2020-0099 \(4 diciembre 2024\)](#) que analiza el proyecto de orden que modifica la Orden IN/1922/2003, de 3 de julio, sobre libros-registro y partes de entrada de viajeros en establecimientos de hostelería y análogos.

Al respecto, la AEPD recuerda su Informe 103/2018 sobre el proyecto de real decreto por el que se establecían las obligaciones de registro documental e información de las personas físicas o jurídicas que ejercen actividades de hospedaje y alquiler de vehículos a motor, para destacar que la base jurídica de este tipo de tratamientos de datos es la del artículo 6.1 c) del RGPD, en cuanto que responden a una obligación legal impuesta a sus destinatarios. Sin embargo, la AEPD señala que la norma de la que se deriva esta obligación legal (artículo 25.1 de la Ley Orgánica 4/2015, de 30 de marzo) no contiene disposiciones específicas para adaptar la aplicación del RGPD a dicho tratamiento. Por tanto, según la AEPD aplicaría el criterio de que es el propio RGPD el que contiene las garantías mínimas, comunes o generales para el tratamiento de dichos datos, siempre que los tratamientos se refieran a datos

personales que no pertenezcan a categorías especiales de datos.

Por otro lado, aunque la AEPD se muestra conforme con el plazo de conservación de los libros registro de tres años que establece el proyecto de orden, advierte que no resulta ni de la modificación llevada a cabo por dicho proyecto ni de la regulación existente en la Orden INT/1922/2003 el que el interesado cuyos datos se recogen y tratan pueda tener copia del documento cuya firma se le exige. En consecuencia, sugiere que en el proyecto se haga mención bien a que dichas hojas de libro registro serán duplicadas de manera que el interesado pueda hacerse -si lo considera oportuno- con un duplicado de lo que firma, que incluirá la información efectos de la normativa de protección de datos; o bien disponer que el interesado podrá obtener una copia (fotocopia o similar) del documento firmado en papel o una copia del documento firmado digitalmente.

Al margen de lo anterior, la AEPD destaca que el hostelero (en tanto que responsable) deberá proporcionar al huésped/interesado toda la información a que se refieren los artículos 13.1 y 13.2 RGPD en el momento de la lectura y firma por el huésped del modelo de parte de entrada de viajeros que se adjunta a la orden como anexo, ya que es cuando se recogen los datos del interesado. También hace una breve mención a la posibilidad de facilitar dicha información por capas, conforme a lo dispuesto en el artículo 11 de la LOPDgdd.

Por último, llama la atención sobre el papel de las Fuerzas y Cuerpos de Seguridad del Estado en relación con los datos obtenidos en virtud de dichas fichas, para señalar que debería estar definido de manera más concreta, estableciéndose claramente los objetivos y la finalidad de dicho tratamiento.

**El CEPD aclara las normas para el intercambio de datos con las autoridades de terceros países y aprueba la certificación del sello de protección de datos de la UE**

Durante su última sesión plenaria, que tuvo lugar los días 2 y 3 de diciembre de 2024, el Comité Europeo de Protección de Datos (CEPD) publicó la [Directrices sobre el artículo 48 del RGPD](#) en relación con las transferencias de datos a las autoridades de terceros países, y aprobó un nuevo sello europeo de protección de datos.

Las citadas directrices, que han estado sujetas a [consulta pública](#) hasta el pasado 27 de enero de 2025, se centran en las solicitudes destinadas a la cooperación directa entre una autoridad pública de un tercer país y una entidad privada de la UE, a diferencia de otros supuestos en los que los datos personales se intercambian directamente entre autoridades públicas de la UE y de terceros países. Tales solicitudes pueden proceder de toda clase de autoridades públicas, incluyendo las autoridades supervisoras del sector privado (por ejemplo, del ámbito bancario, fiscal o asegurador), así como de las que se ocupan de la aplicación de la ley y la seguridad nacional.

En cuanto al ámbito de aplicación de estas directrices, se limita a aquellas solicitudes dirigidas a responsables o encargados sujetos al ámbito territorial establecido por el artículo 3.1 del RGPD. Por otro lado, aunque el artículo 48 no establece distinción alguna a este respecto, las directrices se centran en las solicitudes realizadas directamente a entidades privadas, por ser este el escenario más habitual, ya que las solicitudes a las autoridades públicas suelen enmarcarse en un marco de cooperación internacional establecido en acuerdos internacionales.

Por último, el CEPD destaca que, más allá de los requisitos del RGPD, la cooperación con las autoridades públicas de terceros países puede regirse por normas adicionales. Sin embargo, las directrices no entran a analizar cuáles serían dichos requisitos adicionales.

En lo referente a la aprobación del sello de protección de datos de la UE, el CEPD ha adoptado un dictamen por el que se aprueban los criterios de certificación de *brand compliance* relativos a las actividades de tratamiento por parte de los responsables o

encargados del tratamiento. Cabe destacar que, en septiembre de 2023, el CEPD ya adoptó un dictamen sobre la aprobación de unos criterios nacionales de certificación de *brand compliance* para Países Bajos. Sin embargo, los criterios establecidos por el nuevo dictamen serán aplicables en toda Europa y como sello europeo de protección de datos.

Sin duda, esta certificación permitirá a las organizaciones demostrar su cumplimiento con la normativa de protección de datos, coadyuvando a la transparencia y a la confianza de los interesados.

### El CEPD presenta una carta a la Comisión Europea sobre la revisión de sus once decisiones de adecuación adoptadas en virtud de la Directiva 95/46/CE (6 diciembre 2024)

En su [informe de 15 de enero de 2024](#), la Comisión Europea concluyó que los datos personales transferidos desde la Unión Europea a Andorra, Argentina, Canadá, Islas Feroe, Guernsey, Isla de Man, Israel, Jersey, Nueva Zelanda, Suiza y Uruguay pueden seguir llevándose a cabo bajo la cobertura de las once decisiones de adecuación vigentes, adoptadas sobre la base del artículo 25.6 de la Directiva 95/46/CE y que seguían en vigor en virtud del artículo 45.9 del RGPD.

Al hilo de lo anterior, el Comité Europeo de Protección de Datos (CEPD), sin cuestionar el contenido del informe, presenta a la Comisión Europea a través de [una carta](#) sus observaciones sobre la metodología a seguir en la evaluación de la adecuación, y señala determinados aspectos que podrían haberse descrito con más detalle en el informe del CEPD.

### El EDPS amonesta a la Comisión Europea por el uso de anuncios segmentados en la plataforma X

El [EDPS \(Supervisor Europeo de Protección de Datos\)](#) ha amonestado a la Comisión

[Europea](#), tras una denuncia interpuesta por el grupo NOYB - European Center for Digital Rights ("*None of your business*") por el uso de anuncios segmentados en la plataforma X durante una campaña desplegada en septiembre de 2023 con el objetivo de informar sobre una propuesta de reglamento para combatir el abuso sexual infantil. Los anuncios fueron mostrados 600.000 veces a perfiles de cierta ideología política y religión.

La Comisión justificó su actuación con base en el interés público, basándose en el RGPD y el Tratado de la UE, que establecen que la Comisión Europea deberá promover el interés general. Sin embargo, el EDPS argumentó que los ciudadanos no podrían prever este tratamiento de datos y que se estuvo realizando un tratamiento de categorías especiales de datos extraídos de cuentas privadas, sin que mediaran las excepciones previstas en el artículo 9 RGPD, como el otorgamiento del consentimiento por parte del interesado o la existencia de datos personales que este hubiera hecho manifiestamente públicos.

### El CEPD ha adoptado un dictamen sobre el uso de datos personales para el desarrollo y la implantación de modelos de IA

Este [dictamen](#) analiza 1) cuándo y cómo los modelos de IA pueden considerarse anónimos, 2) si el interés legítimo puede utilizarse como base jurídica para desarrollar o utilizar modelos de IA y, de ser así, cómo, y 3) qué ocurre si un modelo de IA se desarrolla utilizando datos personales que se han tratado de forma ilícita. También analiza el uso de datos propios y de terceros.

El dictamen fue solicitado por la Autoridad de Protección de Datos de Irlanda (APD) con vistas a buscar una armonización normativa a escala europea. El CEPD ofrece en su dictamen ejemplos de un agente de conversación para ayudar a los usuarios y el uso de la IA para mejorar la ciberseguridad.

El dictamen también incluye una serie de criterios para ayudar a las APD a evaluar si las

personas pueden esperar razonablemente ciertos usos de sus datos personales, entre ellos si los datos personales estaban o no a disposición del público, la naturaleza de la relación entre la persona y el responsable del tratamiento, la naturaleza del servicio, el contexto en el que se recopilaban los datos personales, la fuente de la que se recopilaban, y los posibles usos posteriores del modelo. Asimismo, se analiza qué ocurre cuando se desarrolla un modelo de IA con datos personales tratados ilegalmente, y si eso podría tener un impacto en la legalidad de su despliegue.

### Noyb Denuncia a TikTok, Shein y Xiaomi por transferencia ilegal de datos de europeos a China

La organización NOYB, conocida por enfrentarse a gigantes tecnológicos, ha denunciado a TikTok, Shein, Xiaomi, AliExpress, Temu y WeChat por transferir datos personales de usuarios europeos a China, violando así el Reglamento General de Protección de Datos (RGPD). Las denuncias, presentadas en cinco países europeos, buscan la suspensión de estas prácticas y reclaman sanciones que podrían alcanzar hasta el 4% de los ingresos globales de las citadas empresas.

Esta es la primera vez que NOYB centra su atención en compañías chinas, acusándolas de enviar datos a un país sin un nivel adecuado de protección, como exige la normativa europea. Según NOYB, TikTok, Shein y Xiaomi han reconocido estas transferencias, mientras que Temu y WeChat lo hacen a terceros países, además de a China. La organización argumenta que esto representa una grave vulneración de los derechos de los usuarios europeos.

Las compañías han defendido sus prácticas alegando cumplimiento normativo. TikTok destacó su Proyecto Clover para almacenar datos en Europa, mientras que Xiaomi afirmó su compromiso con la privacidad y la cooperación con las autoridades. Sin embargo, las denuncias subrayan la creciente presión de Europa y otros países occidentales

contra las empresas tecnológicas chinas por razones de privacidad, seguridad y competencia desleal.

### Una acción europea analiza la atención del ejercicio del derecho de acceso por parte de los responsables

El pasado 20 de enero el Comité Europeo de Protección de Datos (CEPD) adoptó un [informe sobre la aplicación del derecho de acceso por parte de los responsables del tratamiento](#). El informe resume el resultado de una serie de acciones nacionales coordinadas llevadas a cabo en 2024 con arreglo al Marco Coordinado de Cumplimiento (MCC), con la realización de una encuesta en la que han participado un total de 1.185 entidades del sector público y privado en el ámbito del Espacio Económico Europeo.

El documento enumera los problemas observados en algunos responsables, junto con una serie de recomendaciones para ayudarles a aplicar el derecho de acceso. Un elemento central del análisis es el conocimiento por parte de los responsables del tratamiento de las [Directrices 01/2022 del CEPD sobre los derechos de los interesados - Derecho de acceso](#) y si estas directrices se siguieron en la práctica.

Los resultados sugieren que es necesaria una mayor concienciación sobre las Directrices 01/2022, tanto a escala nacional como de la UE, ya que las directrices ayudan a los responsables del tratamiento a aplicar el derecho de acceso, explican cómo puede facilitarse el ejercicio de este derecho, y enumeran las excepciones y limitaciones del mismo.

Como resultado de la acción coordinada en 2024, se identificaron siete retos. Uno de ellos es abordar la falta de procedimientos internos documentados para tramitar las solicitudes de acceso. Además, también se observaron interpretaciones incoherentes y excesivas de los límites del derecho de acceso, como basarse excesivamente en determinadas excepciones para denegar automáticamente las solicitudes de acceso. Para cada reto

detectado, el informe ofrece una lista de recomendaciones no vinculantes que deben tener en cuenta los responsables del tratamiento y las autoridades de control.

La AEPD se ha hecho eco de esta noticia también, en la medida en que ha participado en esta iniciativa coordinada realizada en el marco del CEPD. La acción coordinada que se desarrollará a lo largo de 2025 se centrará en la implementación derecho de supresión.

### **El CEPD publica el Dictamen 01/2025 sobre el proyecto de decisión de la Autoridad de Supervisión francesa relativo a las normas corporativas vinculantes para los responsables del tratamiento del Grupo Coface**

En [este dictamen](#), el CEPD concluye que pueden adoptarse las normas corporativas vinculantes en la medida en que contienen las salvaguardas adecuadas para garantizar que el nivel de protección de las personas físicas garantizado por el RGPD no se vea socavado cuando los datos personales se transfieran y sean tratados por organizaciones del grupo con sede en terceros países.

En cualquier caso, el CEPD recuerda que la aprobación de las normas corporativas vinculantes no implica la aprobación de las transferencias específicas de datos personales que vayan a realizarse sobre la base de estas. Por consiguiente, esta aprobación no puede interpretarse como la aprobación de transferencias a terceros países para los que no pueda garantizarse un nivel de protección esencialmente equivalente al garantizado en la UE.

### **La Agencia Nacional de Ciberseguridad inicia su funcionamiento y se designa como director a Daniel Álvarez Valenzuela**

La Agencia Nacional de Ciberseguridad de Chile inició oficialmente sus operaciones el 1 de enero de 2025. Su principal objetivo es reforzar la seguridad digital en el país. La

formalización de su funcionamiento se realizó mediante la publicación en el Diario Oficial, el 24 de diciembre de 2024, del [Decreto con Fuerza de Ley \(DFL\) N° 1-21.663](#), que regula tanto su estructura organizativa como el personal directivo.

El proceso de creación de la agencia fue liderado por el Ministerio del Interior, y su primer director será Daniel Álvarez Valenzuela, quien desempeñará un papel clave en la gestión de la seguridad cibernética en Chile. Este nombramiento tiene lugar en un contexto de creciente preocupación por los riesgos cibernéticos y la urgente necesidad de una infraestructura sólida que resguarde la información crítica de las instituciones públicas y privadas del país.

La creación de la Agencia Nacional de Ciberseguridad es un paso crucial para fortalecer la protección digital en Chile. Su implementación, respaldada por un marco normativo adecuado, permitirá mejorar la capacidad de respuesta ante amenazas cibernéticas, garantizando la seguridad de la infraestructura crítica y la integridad de la información.

### **México: La nueva Ley Federal de Protección de Datos Personales en Posesión de los Particulares introduce conceptos como el aviso de privacidad y elimina el INAI**

El pasado 21 de marzo entró en vigor la nueva Ley Federal de Protección de Datos Personales en Posesión de los Particulares, que introduce nuevos conceptos como el aviso de privacidad, consentimiento y datos personales sensibles, además de regular el tratamiento y la transferencia de datos. También se incluyen medidas de autorregulación y se definen sanciones por incumplimiento.

La publicación completa se puede consultar [en este enlace](#).

**Alejandro Padín**

Socio · Madrid

[alejandro.padin@garrigues.com](mailto:alejandro.padin@garrigues.com)

**Miguel Ángel Rocha**

Counsel · Ciudad de México

[miguel.rocha@garrigues.com](mailto:miguel.rocha@garrigues.com)

**Alejandra Badillo**

Asociada sénior · Ciudad de México

[alejandra.badillo@sanchezdevanny.com](mailto:alejandra.badillo@sanchezdevanny.com)

**Antonio Durán**

Asociado · Málaga

[antonio.david.duran@garrigues.com](mailto:antonio.david.duran@garrigues.com)

**Laia Llambrich**

Asociada · Bilbao

[laia.llambrich@garrigues.com](mailto:laia.llambrich@garrigues.com)

**Carina Casadesús**

Júnior · Barcelona

[carina.casadesus@garrigues.com](mailto:carina.casadesus@garrigues.com)

**Rocío Álvarez**

Júnior · Sevilla

[rocio.alvarez@garrigues.com](mailto:rocio.alvarez@garrigues.com)

**Juan Luis Serrano**

Socio · Ciudad de México

[jserrano@sanchezdevanny.com](mailto:jserrano@sanchezdevanny.com)

**Sebastián Hassi**

Asociado principal · Santiago de Chile

[sebastian.hassi@garrigues.com](mailto:sebastian.hassi@garrigues.com)

**Adrián León**

Asociado · Alicante

[adrian.leon@garrigues.com](mailto:adrian.leon@garrigues.com)

**Garazi Tomás**

Asociada · Bilbao

[garazi.tomas@garrigues.com](mailto:garazi.tomas@garrigues.com)

**Marta Sabio**

Asociada · Barcelona

[marta.sabio@garrigues.com](mailto:marta.sabio@garrigues.com)

**Iciar Velasco**

Júnior · Madrid

[iciar.velasco@garrigues.com](mailto:iciar.velasco@garrigues.com)

**Oriol García**

Trainee · Barcelona

[oriol.garcia@garrigues.com](mailto:oriol.garcia@garrigues.com)

Más información:

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

## GARRIGUES

Hermosilla, 3

28001 Madrid

T +34 91 514 52 00

[info@garrigues.com](mailto:info@garrigues.com)

Síguenos en:



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.

[garrigues.com](http://garrigues.com)