GARRIGUES

Newsletter Economía del Dato, Privacidad y Ciberseguridad

Junio de 2025

Índice

1. La Comisión Europea propone modificar el RGPD: lectura crítica y propuestas prácticas

La Comisión Europea ha presentado una propuesta de modificación del RGPD con el objetivo de reducir cargas burocráticas para pymes, ampliando las excepciones a la obligación de mantener un Registro de Actividades del Tratamiento (RAT) como medida principal. Aunque la intención es positiva, el enfoque elegido ha sido criticado por desatender la esencia del cumplimiento normativo. Analizamos lo que esto implica (no necesariamente una mejora para las pymes) y proponemos algunas mejoras alternativas para facilitar el cumplimiento del RGPD.

Alejandro Padín Vidal

La Comisión Europea ha publicado recientemente una propuesta de reglamento destinado a simplificar determinadas obligaciones que afectan a microempresas, pequeñas y medianas empresas. Entre las medidas que se desgranan en ese documento, se incluye una propuesta de modificación del Reglamento General de Protección de Datos (RGPD). El espíritu que subyace a esta propuesta es, principalmente, flexibilizar algunas de las obligaciones de cumplimiento que contiene el RGPD, con el pretendido objetivo de ayudar a las empresas pequeñas y medianas a cumplirlo sin una excesiva carga burocrática, persiguiendo un ahorro de costes y un incremento de la eficiencia de los negocios.

Aunque el propósito y la intención son muy loables, el contenido de las propuestas podría errar el tiro al focalizar su objeto en algunos puntos que están lejos de ser el problema de las pymes para cumplir el RGPD.

En este artículo lo explicamos con ejemplos concretos y proponemos, a continuación, algunas modificaciones que serían útiles para mejorar la situación de cumplimiento y adaptarlo a la realidad de las empresas medianas y pequeñas.

1. Obligación de tener un Registro de Actividades del Tratamiento y sus excepciones

La principal medida que incluye la propuesta de la Comisión se refiere a la obligación de disponer de un Registro de Actividades del Tratamiento (RAT) establecida en el artículo 30 del RGPD. En concreto, la propuesta pretende ampliar el umbral de excepciones aplicables a esa obligación, de forma que un mayor número de empresas puedan decidir no confeccionar este registro.

La redacción actual del artículo 30 del RGPD incluye un punto 5 que contiene las siguientes excepciones:

"Las obligaciones indicadas en los apartados 1 y 2 no se aplicarán a ninguna empresa ni organización que emplee a menos de 250 personas, a menos que el tratamiento que realice pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos personales indicadas en el artículo 9, apartado 1, o datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10".

Como es de apreciar, el texto obliga a cualquier empresa de más de 250 empleados y también a las que tengan menos de ese número si se da alguna de estas tres circunstancias: (i) que el tratamiento entrañe riesgo, (ii) que no sea ocasional o (iii) que incluya categorías especiales de datos o antecedentes penales.

El texto por el que se quiere sustituir el citado artículo 30.5 es el siguiente:

"Las obligaciones mencionadas en los párrafos 1 y 2 no se aplicarán a ninguna empresa ni organización que emplee a menos de 750 personas, a menos que el tratamiento que realice pueda entrañar un alto riesgo para los derechos y libertades de los interesados, en el sentido del Artículo 35".

Como se puede observar, además del aumento en el umbral numérico de empleados, se eliminan dos de las tres circunstancias bajo las cuales las empresas pequeñas también tendrían que disponer de un RAT, como son que el tratamiento no sea ocasional o que incluya categorías especiales de datos personales.

Reflexionando sobre esta propuesta de modificación nos surgen las siguientes preguntas: no disponer de un RAT, ¿es realmente un alivio de carga burocrática? ¿Supone una mayor facilidad de cumplimiento para las pequeñas empresas? ¿Mejorará el nivel de cumplimiento?

2. Comentario a la propuesta de modificación

En nuestra opinión, esta propuesta de reforma plantea dudas por dos motivos: en primer lugar, porque no tiene en cuenta la génesis del actual artículo 30.5 y los motivos por los que se incluyó un criterio numérico en su texto. En segundo lugar, porque no tiene en consideración la esencia de lo que significa el RAT en un programa de cumplimento del RGPD e induce a equivocación en los sujetos obligados sobre cuál es el objetivo del RGPD en su finalidad más esencial.

a. Aumento del número de empleados

En cuanto al primero de los motivos, es necesario remontarnos a la evolución del texto del RGPD durante los cuatro años que duró su tramitación en las instituciones de la UE hasta su aprobación final y publicación en el Diario Oficial de la Unión Europea (DOUE) como norma de carácter obligatorio.

En este sentido, es necesario recordar que, en alguna de sus versiones iniciales, el proyecto de RGPD contenía diversos casos en los que determinadas obligaciones se vinculaban a criterios numéricos de una u otra índole (por ejemplo, la obligación de designar Delegado de Protección de Datos -DPD- o representante en la Unión Europea se vinculaba en la versión inicial de la propuesta de RGPD a que la entidad responsable empleara a más de 250 personas; versiones posteriores lo vincularon a la existencia de tratamientos que afectaran a más de 5.000 interesados; finalmente decayeron estas barreras objetivas). En esa línea de objetivar obligaciones, el artículo 30 establecía la obligación de disponer de un RAT a empresas que tuvieran más de 250 trabajadores. En este caso, a diferencia de los otros en los que las referencias numéricas fueron eliminadas, el criterio numérico se mantuvo.

Durante su periplo en las instituciones europeas, la tramitación del RGPD basculó entre el enfoque jurídico primordialmente basado en los ordenamientos napoleónicos de codificación, de corte administrativista (derecho continental europeo) y el enfoque anglosajón (*Common Law*, con un componente de "*accountability*").

"*Accountability*" es un concepto jurídico que no tiene traducción directa al español. La versión española del RGPD lo traduce como "responsabilidad proactiva", mientras que el Reglamento de Inteligencia Artificial lo traduce como "rendición de cuentas". El contenido completo del "*accountability*" incluye: (i) la obligación de cumplir una obligación determinada, (ii) de ser capaz de demostrar el cumplimiento en todo momento y (iii) la rendición de cuentas o responsabilidad en caso de incumplimiento de cualquiera de las dos obligaciones anteriores.

El resultado final de ese recorrido fue una norma híbrida, que incluye artículos representativos de ambos esquemas jurídicos. Así, por ejemplo, podemos ver en los artículos 13 y 14 (obligación de informar), en el artículo 28 (contenido del acuerdo de encargado del tratamiento) y en el artículo 30 (RAT) una representación clara de la tradición más administrativista y, por el contrario, en los artículos 5.2 (principio de responsabilidad proactiva), artículo 25 (privacidad desde el diseño y privacidad por defecto) o artículo 32 (seguridad del tratamiento) como claras representaciones del *Common Law*.

La revisión final y el consenso que fue necesario alcanzar para poder publicar una norma aceptada por todos no fue nada sencilla. A todas luces el acuerdo político alcanzado pasaba por la eliminación de las referencias objetivas de cumplimiento y su sustitución por la flexibilización y adaptación al caso concreto, aplicando criterios de análisis de riesgo. De este modo, se eliminaron las menciones ya señaladas (número de empleados o de tratamientos para DPD, número de empleados o de interesados afectados para representante en la UE...) y se sustituyeron por obligaciones concretas o por conceptos jurídicos indeterminados, porque se entendía que el cumplimiento de la norma no debía fijarse en función de umbrales, sino que el criterio más importante era el de riesgo para los derechos y libertades de los interesados cuyos datos se tratan. Como resulta obvio, el riesgo de un tratamiento para las personas no depende ni del número de empleados de la entidad que trata los datos ni de ningún otro criterio objetivo. Puede haber una empresa con 1.000 empleados cuyos tratamientos de datos sean de menor riesgo que los que realiza otra empresa de 25 empleados.

Pues bien, en esa tarea final de eliminación de listones numéricos, el que figura en el artículo 30.5 del RGPD no puede calificarse sino como un olvido de última hora, puesto que la conveniencia de disponer de un RAT no tiene nada que ver con el número de empleados de la entidad. En todo caso, incluso aunque esa redacción no fuera fruto de un olvido, el propio texto incluye suficientes "excepciones a la excepción" que, en la práctica, vienen a suponer que el RAT sea una obligación en una gran mayoría de casos, teniendo en cuenta el alto nivel actual de uso de la tecnología.

Por tanto, el incremento del umbral de empleados para la obligación del RAT no resulta entendible.

b. Dudas sobre la flexibilización general

El segundo comentario que se puede hacer al enfoque de la propuesta de modificación con respecto a la obligación de tener un RAT tiene que ver con la propia esencia de lo que es un RAT y el lugar que ocupa en un esquema de cumplimiento del RGPD. No hay que perder de vista que la propuesta se plantea siete años después de la obligatoria aplicación de la norma, cuando ya tenemos suficiente experiencia y criterios prácticos y jurídicos para entender de verdad lo que es un RAT, su importancia y lo que significa.

Como hemos visto, además del criterio numérico referido a los empleados, la propuesta elimina la obligación de disponer de un RAT cuando existan tratamientos que supongan un riesgo para los

derechos y libertades de los interesados (se sustituye por "un alto riesgo"), cuando se trate de tratamientos no ocasionales y cuando se traten datos de categorías especiales.

Es necesario recordar aquí que el RAT puede calificarse como la columna vertebral de un programa de cumplimiento del RGPD. Y ello es así porque, más allá de una mera obligación formal de redacción de un documento, el RAT constituye el inventario detallado de tratamientos de datos que realiza el responsable del tratamiento. Esto, a su vez, resulta imprescindible para dar cumplimiento a muchas otras obligaciones del RGPD. La más inmediata, la obligación de informar (artículo 13), que exige al responsable del tratamiento trasladar al interesado todos los elementos importantes que afectan al tratamiento. Esos elementos se encuentran ordenados y detallados en el RAT y, por ese motivo, la redacción de una política de privacidad sin un RAT se convierte en una labor farragosa y abstracta. La misma importancia tiene el RAT en relación con la verificación de las obligaciones de conservación de datos, las medidas de seguridad, las transferencias internacionales, el control y seguimiento de encargados del tratamiento o las cesiones de datos. Todo ello se encuentra reflejado en el RAT y sirve como guía de cumplimiento del RGPD.

Cualquiera que haya realizado de forma rigurosa un proyecto de cumplimiento del RGPD sabe que sin el RAT la tarea se complica enormemente. Y, por ello, sorprende que se considere una "medida de flexibilización" el aumentar el número de casos en que no es necesario tener un RAT. La consecuencia, lejos de una flexibilización y mejora o una reducción de la burocracia, solo podría ser el empeoramiento en el nivel de cumplimiento del RGPD por parte de las pequeñas y medianas empresas, y la mayor dificultad en conseguir un buen programa de cumplimiento coherente y ordenado. Se podría generar una falsa sensación de cumplimiento en las empresas que se acojan a estas excepciones, que tendrán mayor dificultad en cumplir el RGPD en su totalidad. Y podría aumentar el número de empresas que seguirán cayendo, con mayor intensidad, en las redes de asesores sin escrúpulos que venden papel fotocopiado sin contenido válido (al no ser necesario un RAT, un programa vacío de contenido puede pasar desapercibido con mayor facilidad para alguien sin conocimientos en la materia).

3. Propuestas de mejora del RGPD

El RAT no sería, por tanto, el punto donde es necesario flexibilizar el RGPD. Y ahora analizamos qué medidas serían útiles de verdad para ayudar a las pequeñas y medianas empresas a cumplir la norma y, en definitiva, a proteger mejor los derechos y libertades de los interesados (que es lo verdaderamente importante).

Desde la experiencia de estos nueve años que han transcurrido desde la publicación y entrada en vigor del RGPD en 2016 y los 7 años de obligado cumplimiento desde aquel 25 de mayo de 2018, existen diversas mejoras que se podrían introducir, incluso sin necesidad de modificar ni una sola coma del RGPD. Algunos ejemplos:

- **Promover de forma más eficiente la publicación de códigos de conducta o esquemas de certificación.** La propuesta de modificación del RGPD que plantea la Comisión también incluye, como medidas segunda y tercera, la inclusión en el RGPD de una mención específica a medianas empresas (*mid-cap*) que se añade a la mención a pequeñas y medianas empresas que ya existía en los artículos en los que se recoge la posibilidad de aprobar códigos de conducta y esquemas de certificación. Lo que realmente hace falta, sin embargo, es incentivar que se lleven a cabo o promover su creación de forma activa, por ejemplo, publicando modelos de contenido para códigos de conducta que las asociaciones sectoriales puedan utilizar como referencia.

- **Desarrollar documentación que permita dar cumplimiento a las evaluaciones de impacto para las transferencias internacionales de datos (DTIA).** Actualmente resulta muy frustrante

ver cómo innumerables empresas se ven obligadas a repetir el mismo ejercicio de análisis ya realizado previamente cientos de veces por otras empresas, teniendo que gastar ingentes cantidades de dinero para obtener un informe que bien podría haber realizado alguna de las administraciones públicas competentes. Por ejemplo, aunque una DTIA requiere de diversos *inputs* -algunos de ellos específicos al caso concreto-, la realidad es que muchos otros se refieren al análisis del ordenamiento jurídico y la aplicación de la norma en el país destinatario de los datos. El hecho de que cada empresa que va a realizar una transferencia internacional basada en cláusulas contractuales tipo (la gran mayoría) a un país determinado tenga que encargar un informe legal sobre ese mismo país supone una carga burocrática y económica injusta y desproporcionada, que podría eliminarse por completo con un único informe realizado por una institución nacional o europea sobre cada país. Ni qué decir tiene que la eliminación del RAT no reduciría este problema, real y cotidiano.

- **Ayudar a la interpretación de la norma mediante la implementación de canales de consulta efectivos y útiles por parte de las autoridades de supervisión.** Enfocar la supervisión hacia un proceso de discusión constructivo entre la autoridad y el responsable del tratamiento, de forma que se pueda avanzar en el cumplimiento más allá de los procedimientos sancionadores y que las empresas no teman acercarse a las autoridades y tengan la percepción de que van a recibir ayuda y no silencio o evasivas.

- **Apoyar y ayudar a las empresas que sufren ataques cibernéticos a mejorar su situación en cuanto a la seguridad de la información** porque, en la mayoría de los casos, si no todos, a pesar de haber invertido en ciberseguridad, las empresas se encuentran impotentes cuando sufren un ciberataque y ello supone, además, una sanción por parte de las autoridades de supervisión. El régimen sancionador debería ser la “última ratio” en la aplicación del RGPD, reservado para aquellos casos claros de incumplimiento doloso o recalcitrante, y no para los casos en que las empresas sufren situaciones no deseadas aun cuando han intentado cumplir la norma.

En definitiva y como conclusión, las modificaciones del RGPD destinadas a flexibilizar y mejorar la eficiencia de las empresas sin debilitar la protección de los datos personales deben ser bienvenidas y alentadas pero, quizá, sería más sencillo reflexionar sobre de qué forma se pueden conseguir esos mismos objetivos sin necesidad de modificar la norma (que tanto costó aprobar y tanta fortaleza tiene), atacando los problemas prácticos de su aplicación y facilitando su cumplimiento real y efectivo por parte de las entidades obligadas.

2. Resoluciones de las autoridades de protección de datos

La AEPD impone una sanción en el marco de un caso de duplicado fraudulento de tarjeta SIM

La AEPD ha impuesto una multa total de 1.200.000 euros a una compañía de telecomunicaciones a raíz de dos infracciones por incumplimiento del artículo 6 del RGPD, relativo a bases legales (200.000 euros) y del artículo 25 del RGPD, sobre privacidad por diseño y por defecto (1.000.000 euros).

Esta sanción se dio en el contexto de un caso de *SIM Swapping*, en el que unos trabajadores de la entidad sancionada llevaron a cabo este fraude en el establecimiento en el que desempeñaban sus trabajos. En la resolución se hace constar que el responsable contaba con una serie de procedimientos internos relativos al tratamiento de datos personales por parte de su personal, que incluían las medidas de necesaria implementación. No obstante, considera la AEPD que esta documentación era de corte genérico, ya que, si bien hacía referencia a la existencia de riesgos, estos no estaban suficientemente detallados, ni se establecían actuaciones en concreto para el caso de que se materializaran.

Desestimando las diferentes alegaciones de la sancionada -que, entre otras, argumentaba que la AEPD estaba asumiendo un criterio de responsabilidad objetiva, fruto de un análisis de resultado-, la AEPD concluye que las medidas organizativas de la entidad no fueron suficientes, sobre todo teniendo en cuenta que en su sector este tipo de fraudes son relativamente comunes y pueden tener consecuencias de alta gravedad para los interesados.

Así, la AEPD acaba sancionando, además de por el tratamiento sin base legal del artículo 6 del RGPD, por el incumplimiento del artículo 25 del RGPD, todo ello en una resolución extensa y de gran interés, principalmente por las apreciaciones hechas en relación con el nivel de diligencia que los responsables han de adoptar en lo referente al cumplimiento con el principio de privacidad por diseño y por defecto.

La Liga, sancionada con un millón de euros por el tratamiento de datos biométricos

La AEPD ha impuesto una sanción de un millón de euros a la Liga Nacional de Fútbol Profesional (LNFP) por infracción del artículo 35 del RGPD y ha ordenado la limitación temporal o definitiva del tratamiento de datos biométricos de los aficionados en los clubes donde se realizan controles de acceso con esta tecnología, hasta que se realice y se supere una Evaluación de Impacto de Protección de Datos (EIPD) válida.

La sanción se debe a que la LNFP no realizó una EIPD en relación con el tratamiento de datos biométricos para el acceso a las gradas de animación en los estadios de fútbol de

primera y segunda división, incumpliendo el artículo 35 del RGPD. Según la AEPD, la LNFP era responsable de llevar a cabo esta evaluación debido a su papel en la instauración del sistema de control biométrico de acceso.

La AEPD ha señalado la falta de diligencia por parte de la LNFP, dado que, a pesar de la información disponible sobre los riesgos asociados con el tratamiento de datos biométricos, esta entidad impuso un régimen obligatorio para que los clubes y sociedades anónimas deportivas trataran datos biométricos para el acceso a las gradas de animación. Además, a través de una filial, la LNFP creó medios técnicos para la implementación del sistema biométrico, influyendo en los requisitos de acceso y condicionando a los clubes a adoptar una solución técnica específica, todo ello sin haber realizado dicha EIPD.

La AEPD sanciona con 600.000 euros a una mutua por una brecha de seguridad que afectó a casi 3.400 personas

La resolución de la AEPD en el expediente EXP202412881 se refiere a una brecha de seguridad cometida por una mutua colaboradora con la Seguridad Social que afectó a 3.395 personas cuyos datos personales, incluidos datos de salud, fueron enviados erróneamente a 354 entidades no autorizadas. Este incidente se produjo en el marco del uso de una plataforma online que permite a empresas y asesorías asociadas recibir semanalmente por correo electrónico ficheros Excel con información sobre las prestaciones económicas de sus trabajadores.

El fallo técnico que originó la brecha se debió a una modificación en el sistema de notificaciones automatizadas, por la que una línea de código esencial fue desactivada por error. Esta línea tenía la función de evitar que se acumularan archivos de destinatarios anteriores en los envíos posteriores. Al no ejecutarse, los correos enviados a las entidades contenían no solo los ficheros correspondientes, sino también otros que no les eran propios, lo que provocó la exposición masiva de datos personales.

La mutua detectó el error tras la alerta de una empresa usuaria y procedió a corregir el código, implementar controles técnicos y contactar con las entidades receptoras para solicitar la eliminación de los datos, así como a notificar la brecha a la AEPD. Además, propuso un rediseño del sistema con medidas reforzadas de seguridad, trazabilidad y caducidad automática de los documentos.

La AEPD consideró que la mutua vulneró el principio de integridad y confidencialidad del artículo 5.1.f) del RGPD, al no aplicar medidas técnicas y organizativas adecuadas para garantizar la seguridad de los datos personales. La infracción fue calificada como muy grave, conforme al artículo 83.5 del RGPD y al artículo 72.1.a) de la LOPDGDD. Inicialmente se propuso una sanción de 1.000.000 euros, que fue reducida a 600.000 euros tras el reconocimiento de responsabilidad y el pago voluntario por parte de la mutua, lo que supuso la terminación del procedimiento sancionador.

Desestimado el derecho al olvido sobre información de acceso público vinculada al empleo público

En el Expediente Nº EXP202404813, la Agencia Española de Protección de Datos resolvió el procedimiento de derechos iniciado por una reclamación contra una conocida empresa de motores de búsqueda online, en la que el reclamante solicitaba la eliminación de varios enlaces que aparecían en los resultados del buscador al introducir su nombre y apellidos. Alegaba que dichos enlaces contenían información personal obsoleta y sin relevancia pública, vinculada a su vida profesional, y que su mantenimiento vulneraba el artículo 93 de la LOPD-gdd sobre el derecho al olvido.

La entidad reclamada alegó que parte de las URLs ya habían sido objeto de resolución previa desestimatoria, que otras no aparecían en los resultados de búsqueda y que las

restantes remitían a información institucional sobre procesos selectivos y nombramientos como funcionario de carrera. Defendió que dicha información tenía relevancia pública y que su publicación respondía a obligaciones legales de transparencia y publicidad activa.

La AEPD concluyó que los datos personales publicados derivan de actos administrativos vinculados a procesos selectivos regidos por los principios de mérito, capacidad, igualdad y publicidad. Consideró que impedir a los motores de búsqueda redirigir a esta información supondría una merma del principio de publicidad que rige en el acceso al empleo público. Además, señaló que el tiempo transcurrido desde la publicación (2021 y 2022) no era suficiente para considerar la información obsoleta, especialmente cuando el reclamante aún ostenta la condición de funcionario de carrera.

Por tanto, la Agencia desestimó la reclamación al no concurrir circunstancias que justificaran la prevalencia del derecho del reclamante sobre el interés público en el mantenimiento de los enlaces.

Sancionada una empresa por usar el Whatsapp personal de los empleados con finalidad laboral

La Agencia Española de Protección de Datos resolvió el procedimiento sancionador iniciado contra una sociedad tras la reclamación de un trabajador que denunció el envío reiterado de datos personales de clientes a su número de WhatsApp personal, pese a haber manifestado expresamente su oposición al uso de su dispositivo personal para tal fin. La empresa alegó que el uso de WhatsApp era una práctica habitual y consentida entre todos los empleados y que el reclamante también había iniciado comunicaciones por esa vía.

La AEPD concluyó en su resolución que la empresa había vulnerado el artículo 6.1 del RGPD al tratar los datos personales del reclamante sin base jurídica, incluso una vez extinguida la relación laboral, y el artículo 32 del RGPD por no aplicar medidas de seguridad adecuadas al enviar datos de clientes a un dispositivo privado cuya configuración no podía controlar. La Agencia desestimó las alegaciones de la empresa, señalando que ni la costumbre ni la supuesta aceptación tácita justificaban el tratamiento, y que el reclamante había reiterado su negativa a usar su móvil personal como herramienta de trabajo.

Se impusieron dos sanciones económicas: una de 2.500 euros por la infracción del artículo 6.1 del RGPD y otra de 2.500 euros por la infracción del artículo 32 del RGPD. Además, se ordenó a la empresa acreditar en un plazo de tres meses la adopción de medidas para evitar el contacto con extrabajadores sin base legal y garantizar que los datos de clientes no se envíen a dispositivos personales sin cumplir con las exigencias del RGPD y la LOPD-gdd.

Doble sanción por un importe total de 3.500.000 euros a una entidad bancaria al no garantizar la seguridad de los datos personales de sus clientes

En la resolución PS 00477-2023 se presentó un escrito de reclamación por dos personas físicas frente a una entidad bancaria al constatarse que la madre de uno de los reclamantes tenía acceso no autorizado a información financiera de sus cuentas bancarias. En el supuesto abordado, la madre figuraba como autorizada en dos cuentas de titularidad exclusiva de uno de los reclamantes, pero la operativa de la banca online le permitía visualizar información de las cuentas compartidas y de todos los productos asociados como tarjetas de crédito, hipotecas y seguros, sin tener autorización para ello.

El reclamante presentó varias reclamaciones internas a la entidad bancaria y al Banco de España sin obtener una solución satisfactoria, reconociendo inicialmente la entidad que existía una "incidencia técnica" que permitía a la madre del reclamante acceder a información no autorizada.

La AEPD determinó que la empresa había vulnerado varios artículos del RGPD,

incluyendo la falta de consentimiento explícito y la ausencia de medidas adecuadas para garantizar la seguridad de los datos, existiendo una "negligencia en el tratamiento de los datos", ya que, pese a tener conocimiento de los hechos denunciados al ser informado por la reclamante, no se habían adoptado las medidas necesarias para evitar que continuara la infracción. Por ello, se considera que la parte reclamada incide todavía más en la culpabilidad y antijuridicidad de su conducta.

La resolución concluye con la imposición de una sanción económica a la empresa infractora, así como de la obligación de adoptar medidas correctivas para cumplir con la normativa de protección de datos, siendo los hechos constitutivos de una doble infracción, imputable a la parte reclamada, por vulnerar los artículos 5.1.f) ("principio de confidencialidad") y 25 del RGPD ("aplicación de medidas técnicas y organizativas adecuadas"). El balance de las circunstancias contempladas con respecto a las infracciones cometidas permite a la AEPD fijar una multa de 500.000 euros por el primer incumplimiento y otra de 3.000.000 euros por el segundo.

Se impone una multa de 500.000 euros por no informar al responsable del tratamiento de la identidad de las entidades que se pretendían subcontratar

Con fecha 1 de abril de 2009, la Consellería de Sanidad Universal y Salud Pública de la Generalitat Valenciana suscribió con una asociación dedicada a la prestación de servicios asistenciales sanitarios un contrato relacionado con la prestación del servicio de atención sanitaria en el Departamento de Salud de Denia. Dicho contrato incluía un acuerdo de encargo del tratamiento que recogía la obligación del encargado de informar al responsable de la identidad de las sociedades a las cuales pretenda subcontratar los servicios objeto del contrato. Ante el incumplimiento de dicha obligación, la Consellería presentó denuncia ante la AEPD.

En este caso, no consta que la parte reclamada hubiera informado a la Consellería con anterioridad a la formalización de los contratos suscritos con los subencargados para que, como responsable de los datos, hubiera tenido la oportunidad de oponerse. A la hora de decidir sobre la cuantía de la multa administrativa, la AEPD tiene en cuenta la naturaleza, gravedad y duración de la infracción por no informar de los tres contratos suscritos con los subencargados en 2018, vigentes a día de hoy, y el hecho de que los datos personales afectados por la infracción son datos de salud, que se consideran categorías especiales de datos. Por todo ello, la sanción impuesta asciende a 500.000 euros.

Condenada una entidad bancaria por no implementar las medidas apropiadas para garantizar la confidencialidad de los datos personales

En fecha 28 de octubre de 2022, la AEPD recibió una notificación de brecha de seguridad por parte de la sucursal española de una entidad bancaria francesa, según la cual uno de los subencargados que tenía contratados dicha entidad había sufrido un ciberataque de *ransomware*. En la resolución del procedimiento sancionador, la AEPD destaca las siguientes cuestiones:

1. Sobre la falta de legitimación pasiva de la sucursal española y la falta de competencia territorial de la AEPD, considera no solo la responsabilidad directa de la reclamada en los hechos, sino que la agencia tiene facultad suficiente para decidir sobre los tratamientos realizados en España.

2. En cuanto a la alegación de que la entidad bancaria es víctima de un delito, la AEPD señala que la culpabilidad de la reclamada no puede considerarse excluida ni atenuada por el hecho de que haya mediado la actuación fraudulenta de un tercero, pues su responsabilidad no deriva de la actuación de este sino de la suya propia.

3. Respecto de las obligaciones recogidas tanto el artículo 5.1.f) como el artículo 32 del RGPD, relativas a la necesidad de aplicar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo que incluya, entre otros, la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y la capacidad de restaurar el acceso a los datos personales de forma rápida , la AEPD declara la falta de diligencia y adecuación de las medidas adoptadas e implementadas por la entidad en este caso concreto, todo ello teniendo en cuenta los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas.

4. En particular, la AEPD constató que el acceso de un tercero no se habría producido si los datos personales hubieran estado cifrados, pseudonimizados o anonimizados, pues el atacante se hubiera llevado información ininteligible.

En relación con la responsabilidad del encargado del tratamiento, la AEPD apunta que la entidad bancaria es el responsable de los datos personales con independencia de la responsabilidad en que hayan podido incurrir terceros ajenos a ella. Por todo ello, la Agencia impone una sanción de 200.000 euros.

Multada con 2.000.000 euros una entidad financiera por exigir el consentimiento de un cliente para el tratamiento de sus datos como requisito para contratar una cuenta bancaria

La AEPD, en su resolución PS/00531/2023, impuso una multa de 2.000.000 euros a una entidad financiera que, para que sus clientes pudieran finalizar la contratación de un determinado tipo de cuenta bancaria, les exigía que otorgaran su consentimiento para que la entidad solicitara a la Tesorería General de la Seguridad Social información de su actividad económica con el fin de cumplir así con lo previsto en la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo.

Dicha ley determina la obligación de verificar las actividades profesionales y empresariales de los sujetos con los que se vaya a hacer negocio, pero no prevé que deba hacerse de una manera determinada. Si bien se puede optar por el consentimiento, la AEPD considera que la implementación no ha sido la adecuada, ya que no se puede considerar que el consentimiento sea una base legal válida si se sujeta la celebración del contrato al otorgamiento de este.

La autoridad supervisora de protección de datos irlandesa impone una multa de 530.000.000 euros a TikTok por la realización de transferencias internacionales irregulares

La autoridad supervisora irlandesa emitió el pasado 2 de mayo una nota de prensa en la que anunciaba la imposición a TikTok de una multa de 485.000.000 euros por la realización de transferencias internacionales a China sin una evaluación adecuada del impacto de estas transferencias, lo cual imposibilitaba la adopción de garantías adecuadas.

Asimismo, si bien los incumplimientos detectados en la política de privacidad dirigida a los interesados del Espacio Económico Europeo en el marco de la investigación fueron subsanados por TikTok en 2022, la autoridad supervisora le impuso una multa de 45.000.000 euros por el incumplimiento del deber de informar durante el periodo comprendido entre el 29 de julio de 2020 y el 1 de diciembre de 2022.

Las dos sanciones suman un total de 530.000.000 euros, a lo que se añade la obligación de regularizar las transferencias en los próximos seis meses o suspender su realización en caso contrario.

La AEPD sanciona al Ministerio para la Transición Ecológica y el Reto Demográfico (MTERD)

La Fundación Éticas Data Society denunció ante la AEPD que el "sistema de información BOSCO" utilizado por el MTERD para determinar la concesión del bono social eléctrico toma decisiones automatizadas sin intervención humana significativa, sin controles de calidad periódicos ni mecanismos adecuados para que los interesados puedan impugnar o expresar su punto de vista. Asimismo, se puso de manifiesto la falta de transparencia en relación con la información facilitada a los interesados sobre el tratamiento y la ausencia de una evaluación de impacto relativa a la protección de datos (EIPD).

A pesar de que el Ministerio defiende la existencia de participación humana en la gestión de las solicitudes y en la tramitación de reclamaciones, así como la implementación de códigos de observaciones para informar sobre las causas de denegación, la AEPD, en su resolución de 9 de mayo de 2025 PS-00324-2025, declara: (i) infringido el artículo 22 RGPD, ya que el sistema BOSCO adopta decisiones automatizadas sobre la concesión del bono social sin cumplir con los requisitos exigidos; (ii) la vulneración del artículo 35 RGPD, por no realizar una EIPD; y (iii) la infracción del artículo 13 RGPD, por no informar a los interesados sobre la existencia de decisiones automatizadas ni de sus derechos asociados. En consecuencia, la AEPD impone una serie de medidas correctoras, incluyendo la obligación de informar a los interesados sobre las decisiones automatizadas y realizar una EIPD en un plazo máximo de seis meses, así como garantizar el derecho a intervención humana en un plazo máximo de nueve meses.

La AEPD sanciona al Consejo General del Notariado (CGN) por exigir y almacenar copia del DNI de los registrantes en el Portal Notarial Ciudadano

El reclamante interpuso una reclamación ante la AEPD alegando que el Portal Notarial del Ciudadano requería una fotografía del DNI por ambas caras para registrarse, lo cual consideraba excesivo e innecesario, siendo la firma electrónica suficiente.

En su resolución de 6 de mayo de 2025 PS-00052-2024**,** la AEPD declara la ilicitud del tratamiento y la vulneración del artículo 6.1 RGPD, puesto que: (i) si bien el notario está obligado a verificar la documentación que acredite la identificación del interesado (como el DNI), su conservación únicamente es preceptiva en los supuestos establecidos en la Ley 10/2010 de prevención del blanqueo de capitales y de la financiación del terrorismo; y (ii) el consentimiento recabado no cumplía los requisitos del RGPD para considerarse válido. Adicionalmente, la AEPD señala que el CGN no cumplió con el deber de información del artículo 13 del RGPD, porque la política de privacidad no diferenciaba adecuadamente las bases jurídicas ni las finalidades del tratamiento (especialmente en lo relativo a la conservación de la copia del DNI). Finalmente, la AEPD declara que el Delegado de Protección de Datos (DPO) del CGN, que es la Agencia Notarial de Certificación (ANCERT), incumplió el deber de independencia exigido por el artículo 38.6 RGPD, ya que actuaba simultáneamente como encargado del tratamiento y DPO, lo que supone un conflicto de intereses. En consecuencia, la AEPD ordena la adopción de medidas correctoras para adecuar el tratamiento de datos a la normativa aplicable y su acreditación en el plazo de seis meses.

Sancionada una farmacia con 16.000 euros por tres infracciones del RGPD

La farmacia recopilaba y almacenaba datos personales y de salud de pacientes (nombre, apellidos, CIPA, CIP, medicación, médico prescriptor, centro de salud, etc.) en archivos excel para renovar la medicación sin la presencia del paciente ni de su tarjeta sanitaria. Este tratamiento se realizaba sin garantías de protección suficientes, ya que los archivos se almacenaban en los escritorios de los ordenadores de la farmacia, protegidos solo por una contraseña común a todos los empleados, y los ordenadores estaban en mostradores visibles para los clientes. Además, el tratamiento se realizaba sin el consentimiento informado del paciente, ya que no se proporcionaba información específica sobre el tratamiento de sus datos personales.

En su resolución de 5 de mayo de 2025 PS-00187-2025. la AEPD impuso una multa total de 16.000 euros por vulneración de los artículos 13, 9 y 32 del RGPD. Sobre el deber de información (art. 13 RGPD), la AEPD consideró que la farmacia no proporcionó información a los interesados sobre el tratamiento de sus datos personales, vulnerando el principio de transparencia, por lo que impuso una multa de 3.000 euros. En cuanto al tratamiento de datos de salud (art. 9 RGPD), la AEPD entendió que se trataron datos de salud sin base legal adecuada, sin consentimiento explícito ni concurrencia de ninguna de las excepciones del artículo 9.2 RGPD, por lo que impuso una multa de 10.000 euros. Respecto a la seguridad del tratamiento (art. 32 RGPD), la AEPD consideró que no se adoptaron medidas técnicas y organizativas apropiadas para garantizar la seguridad de los datos, existiendo acceso potencial no autorizado y falta de control sobre los archivos, por lo que impuso una multa de 3.000 euros.

Tras la notificación del acuerdo de inicio, la farmacia reconoció la responsabilidad y realizó el pago voluntario de la sanción.

Sancionado por cumplir indebidamente con la obligación del registro de viajeros

El reclamante reservó un apartamento turístico a través de una plataforma y fue obligado a utilizar una aplicación de *check-in* online que exigía fotografiar ambas caras del DNI y enviar una fotografía facial (*selfie*) para acceder al alojamiento. En su resolución de 8 de mayo de 2025 PS-00546-2024, la AEPD impone una sanción total de 2.500 euros, que se distribuye en 1.000 euros por infracción del artículo 5.1.c RGPD y 1.500 euros por infracción del artículo 9 RGPD.

Sobre el principio de minimización de datos (art. 5.1.c RGPD), la AEPD concluye que la normativa sectorial exige la recogida y comunicación de ciertos datos (nombre, apellidos, número de documento, nacionalidad, fecha de nacimiento, etc.), pero no la imagen completa del DNI ni la fotografía facial del huésped, por lo que no legitima el tratamiento de datos personales. En cuanto al tratamiento de datos biométricos (art. 9 RGPD), la AEPD considera que, dado que la verificación biométrica facial constituye un tratamiento de datos de categoría especial (prohibido a menos que concurra alguna de las excepciones del art. 9.2 RGPD) y no concurren ninguna de las excepciones del artículo 9.2 RGPD, se ha realizado un tratamiento de datos biométricos sin base legal. Además, la AEPD matiza que la obligación legal de registro de viajeros no ampara la recogida de datos excesivos ni el tratamiento de datos biométricos, pudiendo realizar la comprobación de la identidad por otros medios menos intrusivos.

La Autoridad Polaca de Protección de Datos sanciona con 132.000 euros porque el DPO de una compañía no ejercía plenamente su independencia y no incluyó la elaboración de perfiles en el RAT ni en la PIA

En su resolución de 18 de noviembre de 2024, la Autoridad de Supervisión polaca impuso

una multa de 132.000 euros a una entidad bancaria por la infracción de los artículos 30, 35 y 38 del RGPD. Tras la oportuna investigación, la Autoridad de Supervisión descubrió que, si bien el banco realizaba perfilados de numerosos datos de clientes con el fin de determinar la solvencia de estos y que posteriormente trataba el resultado de la puntuación crediticia obtenida, dichos tratamientos no constaban en su registro de actividades de tratamiento de datos. Además, el banco no llevó a cabo la correspondiente evaluación del impacto sobre la protección de datos, por lo que no evaluó las implicaciones de la elaboración de perfiles para la seguridad del tratamiento de datos personales. No obstante, el banco subsanó esta infracción antes de que se iniciara la investigación.

Asimismo, se puso de manifiesto la existencia de un conflicto de intereses en la figura del Delegado de Protección de Datos (DPO) designado por el banco. El DPO no ejercía plenamente la independencia exigida por el RGPD porque no dependía directamente de la más alta dirección del banco, es decir, del Consejo de Administración, y, además, trabajaba como auditor informático/especialista en seguridad en el departamento de Seguridad, dependiendo directamente del director de dicho departamento.

La AEPD impone una multa de 10.000 euros a una marca de cosméticos por infracción del artículo 22.2 de la LSSI

El procedimiento PS-531/2024 se inicia por denuncia de un reclamante sobre la instalación de *cookies* no técnicas sin consentimiento en la página web de la sancionada.

La entidad denunciada alega que el problema se debió a una omisión en los controles de implementación de *cookies* de terceros y que se han adoptado medidas correctoras para solucionarlo (bloqueo de vídeos embebidos, actualización de la política de *cookies*, integración de un CMP, refuerzo de auditorías, etc.). No obstante, la AEPD detectó varios problemas en el comportamiento de las *cookies* de la página web: (i) el panel de gestión de *cookies* presentaba las opciones premarcadas en "ON", lo que no es admisible; (ii) incluso tras rechazar las *cookies* no necesarias, la web seguía instalando *cookies* de segmentación y rendimiento; (iii) no existía un mecanismo accesible y permanente para modificar el consentimiento durante la navegación; y (iv) la información sobre la gestión de *cookies* se limitaba a instrucciones para el navegador, lo que no es suficiente como único mecanismo.

En conclusión, la AEPD estima la existencia de infracción del artículo 22.2 de la LSSI basándose en la instalación de *cookies* no técnicas o necesarias sin consentimiento previo, la instalación de *cookies* no técnicas incluso tras el rechazo expreso, y la ausencia de un mecanismo para modificar o retirar el consentimiento en cualquier momento. De esta forma, se impone una multa de 10.000 euros por infracción leve del artículo 22.2 de la LSSI, agravada por reincidencia, al haber sido ya la entidad sancionada por hechos similares en el año 2023.

El TJUE avala determinar las sanciones del RGPD según el concepto de 'empresa' del derecho de la competencia

El 13 de febrero el Tribunal de Justicia de la Unión Europea (TJUE) publicó la sentencia del asunto C-383/23, que resolvía una cuestión prejudicial planteada por el Tribunal de Apelación de la Región Oeste de Dinamarca ante el recurso presentado por una cadena danesa de tiendas de muebles contra la cuantía de la multa administrativa que se le imponía por la infracción del plazo de conservación de los datos personales.

Inicialmente, se impuso a dicha cadena una multa de 200.000 euros por infracción del artículo 5.1.e) del RGPD, que se calculó con base en el volumen de negocio del grupo empresarial al que pertenecía. Al analizar dicho volumen para llevar a cabo el cálculo de la multa, las autoridades danesas consideraron que era necesario aplicar el concepto de empresa utilizado en derecho de la competencia, por el cual se considera a una empresa como una “unidad económica”.

El TJUE responde basándose en el artículo 83 del RGPD, que indica que las multas deben ser proporcionales y disuasorias. Asimismo, distingue entre el cálculo del importe máximo de la multa y la proporcionalidad de esta. Sin perjuicio de lo anterior, el Tribunal indica que la consideración de “empresa” debe ir alineada con los artículos 101 y 102 del Tratado de Funcionamiento de la Unión Europea (TFUE), es decir, con la consideración de unidad económica según el derecho de la competencia.

El TJUE resuelve acerca del alcance del derecho de acceso del interesado y la lógica utilizada en la adopción de decisiones automatizadas

Una empresa de telecomunicaciones austriaca rechazó la prórroga de un contrato con una clienta basándose en una evaluación automatizada de su solvencia, que concluyó que la clienta no tenía una calificación crediticia suficiente para formalizar dicho contrato. La clienta acudió a la autoridad de protección de datos austriaca, que ordenó a la empresa proporcionar información significativa sobre la lógica aplicada en la decisión automatizada.

La empresa recurrió la orden, alegando que no estaba obligada a revelar más información debido a secretos comerciales, y el correspondiente tribunal austriaco determinó que la compañía había infringido el RGPD al no proporcionar suficiente información sobre la lógica del proceso automatizado. Sin embargo, la solicitud de ejecución forzosa de esta resolución fue desestimada

por la autoridad de ejecución en Viena, que consideró que la empresa había cumplido suficientemente su obligación de información.

La interesada recurrió ante el tribunal remitente, que elevó cuestiones prejudiciales al TJUE. Dichas cuestiones se centraron en la interpretación del artículo 15.1 h) del RGPD, que establece que el interesado tiene derecho a obtener información significativa sobre la lógica aplicada en decisiones automatizadas, incluida la elaboración de perfiles.

En su resolución del caso C-203/22, el Tribunal de Justicia aclaró que, en caso de decisiones automatizadas, el responsable del tratamiento debe explicar de manera concisa, transparente, inteligible y de fácil acceso el procedimiento y los principios aplicados para explotar los datos personales del interesado. Además, si la información incluye datos de terceros protegidos o secretos comerciales, el responsable debe comunicar dicha información a la autoridad de control o al órgano jurisdiccional competente, que ponderará los derechos e intereses en cuestión para determinar el alcance del derecho de acceso del interesado.

El TJUE reconoce el derecho de rectificación sobre los datos relativos al sexo de la persona sin necesidad de demostrar el sometimiento a una cirugía de reasignación

Al hilo de una cuestión prejudicial presentada por un tribunal húngaro, se plantea el caso de una persona que solicitó que se corrigiera su nombre y sexo en el registro de asilo nacional de Hungría, aportando certificados médicos que acreditaban su identidad de género masculina. Sin embargo, la administración rechazó la solicitud al no haberse acreditado la cirugía de cambio de sexo.

En la resolución de este asunto (C-247/23), el TJUE ha dictaminado que, en virtud del artículo 16 del RGPD, una persona tiene derecho a rectificar los datos personales relativos a su sexo sin necesidad de demostrar que se ha sometido a una cirugía de reasignación, siendo suficientes los certificados médicos que prueben su identidad, de conformidad con el principio de exactitud de los datos. Añade que un Estado Miembro no puede condicionar el ejercicio del derecho de rectificación a la existencia de un procedimiento nacional de reconocimiento de género ni exigir una cirugía, ya que ello vulneraría los derechos a la integridad y a la vida privada reconocidos en la Carta de los Derechos Fundamentales de la UE.

El abogado general del TJUE emite un dictamen sobre el asunto C-654/23 relativo a la relación entre el RGPD y la Directiva ePrivacy

En el dictamen emitido en el marco del asunto C-654/23, Inteligo Media SA v Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Carácter Personal (ANSPDCP), en respuesta a la petición de decisión prejudicial planteada por el Tribunal Superior de Bucarest, el abogado general Szpunar, en sus conclusiones, sostiene que la provisión de un servicio aparentemente gratuito con fines publicitarios puede constituir una forma de mercadotecnia directa conforme al artículo 13 de la Directiva sobre privacidad y comunicaciones electrónicas (Directiva 2002/58/CE). En consecuencia, el envío de boletines informativos sin consentimiento previo sería lícito si se cumplen los requisitos del artículo 13.2 de dicha directiva, sin necesidad de acudir al artículo 6 del Reglamento General de Protección de Datos (RGPD) como base jurídica adicional.

El caso examinado se refiere a una web que ofrecía acceso limitado gratuito a contenidos, ampliable mediante registro con correo electrónico, mientras que el acceso completo requería pago. Tras el registro, el usuario -sin suscribirse al plan de pago- recibió un boletín con novedades del sitio.

El abogado general concluye que dicho boletín constituye mercadotecnia directa, ya que el modelo económico (*soft paywall*) persigue inducir al usuario a contratar un servicio de pago. Considera que proporcionar datos personales (como el correo) a cambio de contenido puede entenderse como contraprestación por un servicio, encajando en el concepto de "venta" del artículo 13.2. Este precepto sería exhaustivo, por lo que no se requeriría base adicional bajo el RGPD. Además, enfatiza que el RGPD y la Directiva ePrivacy responden a derechos fundamentales distintos, siendo compatibles y complementarios en su aplicación.

El TSJ de Extremadura confirma el despido procedente de una vigilante por divulgar datos personales en un grupo de WhatsApp

El Tribunal Superior de Justicia de Extremadura ha confirmado la procedencia del despido disciplinario de una vigilante de seguridad del Centro Penitenciario de Badajoz por, entre otros motivos, una grave vulneración de la normativa de protección de datos. La trabajadora fue despedida tras ausentarse durante nueve minutos de su puesto mientras el sistema de alarmas permanecía desactivado, incumpliendo el protocolo de relevos. La empresa le concedió 48 horas para presentar alegaciones, y la empleada respondió por escrito justificando su actuación por motivos de salud y acusando a su superior de acoso laboral.

Sin embargo, ese escrito de alegaciones -que incluía datos personales de compañeros, referencias a turnos, protocolos internos y detalles operativos del centro- fue posteriormente compartido por la propia trabajadora en un grupo de WhatsApp llamado "Grupo Extremadura VS" con casi 400 participantes ajenos a la empresa. El tribunal consideró que esta difusión no autorizada constituía una infracción muy grave de su deber de confidencialidad y una vulneración de la normativa sobre protección de datos personales.

La Sala de lo Social, en su sentencia 31/2025 de 21 Ene. 2025, Rec. 795/2024, desestima el recurso de la trabajadora por falta de base fáctica y jurídica suficiente, confirmando así la sentencia de instancia y declarando procedente el despido, sin derecho a indemnización ni salarios de tramitación.

La Audiencia Nacional confirma multa de 40.000 euros a una financiera por tratar datos de una víctima de suplantación sin base legal

La Audiencia Nacional ha confirmado la sanción de 40.000 euros impuesta por la Agencia Española de Protección de Datos (AEPD) a una empresa dedicada a la gestión del crédito y recobro por una infracción muy grave de la normativa de protección de datos. La empresa trató los datos personales de un afectado que había sido víctima de suplantación de identidad en la contratación fraudulenta de un préstamo sin contar con una base legítima para dicho tratamiento, vulnerando el artículo 6.1.b) del Reglamento General de Protección de Datos (RGPD).

A pesar de que el afectado comunicó la suplantación y solicitó la supresión de sus datos en marzo de 2021, la entidad no lo eliminó del fichero de morosidad ASNEF hasta casi dos meses después, manteniendo, entre tanto, el tratamiento de datos sin consentimiento ni causa que lo legitimara. La Sala de lo Contencioso-administrativo, Sección 1ª, en la sentencia de 13 Feb. 2025, Rec. 1005/2022, rechaza que se hubiera actuado con diligencia y descarta la aplicación de la exoneración prevista en el artículo 4.2.a) de la LOPD-gdd, ya que los datos no eran exactos ni procedían directamente del afectado.

El tribunal destaca que el consentimiento debe ser inequívoco y que la empresa era responsable del tratamiento incluso tras la cesión del crédito. Se desestima el recurso de la financiera y se le imponen las costas del proceso.

La Audiencia Nacional reconoce el derecho de acceso a datos personales bloqueados en ficheros de morosidad

La Sala de lo Contencioso-administrativo, Sección 1ª, de la Audiencia Nacional, en su sentencia de 13 Feb. 2025, Rec. 2255/2021, ha desestimado el recurso presentado por una entidad gestora de un fichero de morosidad contra la resolución de la AEPD que reconocía a un ciudadano su derecho de acceso a datos personales bloqueados en sus sistemas. Aunque los datos habían sido cancelados y se encontraban en estado de bloqueo desde marzo de 2019, en enero de 2021 el afectado solicitó acceder a información sobre su inclusión previa en el fichero, así como detalles sobre las entidades que consultaron sus datos y el motivo de la baja.

La entidad denegó parte de la información solicitada, alegando que los datos bloqueados no pueden visualizarse ni tratarse salvo por autoridades públicas en los supuestos previstos legalmente. Sin embargo, la Audiencia Nacional respalda el criterio de la AEPD al afirmar que facilitar al interesado el acceso a sus propios datos bloqueados -aquellos que fueron tratados mientras duró la relación contractual- no constituye una operación de tratamiento conforme al RGPD y la LOPD-gdd.

El tribunal destaca que el derecho de acceso persiste incluso tras el bloqueo de los datos, siempre que no hayan sido físicamente eliminados. Esta interpretación garantiza el control del afectado sobre su información y no vulnera el principio de limitación del plazo de conservación. Se imponen las costas procesales a la entidad recurrente.

Condenadas una entidad bancaria y una gestora de ficheros por intromisión ilegítima en el honor de un consumidor

En la sentencia 259/2024 de 20 diciembre de 2024, Rec. 367/2022, la Audiencia Provincial de Toledo confirma la condena a una entidad bancaria y a una entidad gestora de un fichero de morosidad por intromisión ilegítima en el derecho al honor de un consumidor, debido a su inclusión indebida en dicho fichero de morosos. El tribunal considera probado que no se cumplieron los requisitos legales exigidos por la normativa de protección de datos vigente en el momento de los hechos, como el requerimiento previo de pago y la adecuada notificación contractual sobre la inclusión en sistemas de información crediticia.

La entidad gestora del fichero, como responsable del mismo, alegó que su papel era meramente técnico y que actuaba conforme a las indicaciones del acreedor. Sin embargo, el tribunal, siguiendo la doctrina del Tribunal Supremo, sostiene que el titular del fichero debe comprobar la exactitud, pertinencia y licitud de los datos antes de mantenerlos, y no puede limitarse a una actuación pasiva. Esta falta de diligencia supuso un incumplimiento de la normativa y una vulneración del derecho fundamental a la protección de datos.

Ambas entidades fueron condenadas solidariamente al pago de 10.000 euros por daños morales, y adicionalmente la entidad gestora del fichero fue obligada a cancelar los datos del interesado. La sentencia incide en la responsabilidad activa del responsable del fichero y en la necesidad de proteger con rigor los datos personales frente a intromisiones indebidas.

Un juzgado de Murcia ordena limpiar los ficheros de morosidad tras conceder la exoneración del pasivo a un deudor

En el auto de 3 mayo 2024, Recurso 79/2024, el Juzgado de lo Mercantil nº 2 de Murcia concede a los deudores la exoneración del pasivo insatisfecho, y, como efecto directo de ello, activa el mecanismo de protección de datos previsto en el artículo 492 ter del Texto Refundido de la Ley Concursal (TRLC). Esta norma establece que la resolución judicial que acuerde la exoneración debe

incorporar un mandamiento dirigido a los acreedores afectados para que comuniquen dicha exoneración a los sistemas de información crediticia (ficheros de morosidad) en los que previamente se hubiera informado del impago o mora de las deudas exoneradas.

Esta obligación tiene como finalidad la actualización de los registros, garantizando que no se mantenga indebidamente la información negativa en perjuicio del deudor. De este modo, se protege su derecho a la exactitud y actualización de los datos personales, conforme al artículo 5.1.d) del RGPD. Asimismo, el deudor tiene la posibilidad de recabar testimonio de la resolución para requerir directamente la actualización de sus datos ante dichos sistemas, reforzando su derecho de acceso, rectificación y cancelación.

Este auto subraya la relevancia del principio de minimización del tratamiento y la necesidad de garantizar que los datos relativos a créditos ya exonerados no sean utilizados de forma ilegítima ni continúen afectando la solvencia del deudor, fomentando así la depuración efectiva de los ficheros de morosos.

El TJUE aclara que la publicidad de procedimientos de pago constituye oferta promocional protegida por la Directiva de Comercio Electrónico

El artículo 6 c) de la Directiva 2000/31/CE de Comercio Electrónico indica que las ofertas promocionales -como descuentos, premios y regalos-, cuando estén permitidas en el Estado miembro de establecimiento del prestador de servicios, deberán ser claramente identificables como tales, y las condiciones que deban cumplirse para acceder a ellas serán fácilmente accesibles y presentadas de manera clara e inequívoca.

El litigio (asunto C-100/24) enfrenta a una asociación de consumidores contra una empresa distribuidora de moda especializada en venta por catálogo, que publicó un mensaje publicitario en su página web relativo a un procedimiento de pago concreto. Concretamente, el anuncio incluía un mensaje que decía “cómoda compra a cuenta”. La asociación de defensa de los consumidores consideró que concurría una práctica comercial desleal, en particular una omisión engañosa, por no incluir en el mensaje publicitario que, para poder acceder a esta modalidad, era necesario someterse a una evaluación de solvencia.

Al llegar el asunto al Tribunal Superior Regional de lo Civil y Penal de Hamburgo, se planteó una cuestión prejudicial cuestionando si la publicidad de un procedimiento de pago (en este caso, “cómoda compra a cuenta”), que tiene un escaso valor monetario, pero sirve a la seguridad y al interés jurídico del consumidor, constituye una oferta promocional a efectos del artículo 6, letra c), de la Directiva 2000/31/CE de Comercio Electrónico.

El tribunal determinó que una oferta comercial debe entenderse en el sentido de toda comunicación mediante la cual un prestador de servicios pretende promocionar bienes o servicios proporcionando a su destinatario una ventaja objetiva y cierta que pueda influir en su comportamiento a la hora de elegir tales bienes o servicios. La forma que adopte esta ventaja, al igual que su relevancia, es indiferente, pudiendo tratarse, en particular, de una ventaja pecuniaria o jurídica o de una mera comodidad, como, por ejemplo, permitir a su destinatario ganar tiempo.

También recalcaba el TJUE la importancia de la interpretación teleológica de la norma, indicando que el objetivo de la directiva es asegurar un alto grado de protección para los consumidores.

Finalmente, el Tribunal concluyó que, efectivamente, un mensaje publicitario que mencione un procedimiento de pago concreto puede considerarse una oferta publicitaria en la medida que esta proporcione al destinatario de ese mensaje una ventaja objetiva y cierta que pueda influir en su comportamiento a la hora de elegir un bien o un servicio.

El Tribunal de Mercado de Bélgica confirma la sanción a IAB Europe y su corresponsabilidad en la gestión del 'Transparency & Consent Framework'

Tras la resolución por parte del TJUE de las cuestiones prejudiciales planteadas por el Tribunal de Mercado de Bélgica relativas a la validez del *Transparency & Consent Framework* (TCF) de IAB Europe, dicho tribunal ha dictado sentencia. Como cuestión más relevante, esta declara la corresponsabilidad de IAB Europe en la creación de las cadenas de consentimiento en las que se almacenan las preferencias de los usuarios en relación con el uso de sus datos en el ecosistema publicitario.

En febrero de 2022, la autoridad de protección de datos belga dictaminó que la citada asociación, que desarrolló el TCF como marco de autorregulación del mercado publicitario online, era corresponsable tanto de la creación de las cadenas de consentimiento como de los posteriores usos que se llevaran a cabo con ellas, imponiendo una sanción de 250.000 euros.

IAB Europe recurrió la decisión ante el Tribunal de Mercado de Bélgica, quien remitió al TJUE una serie de cuestiones prejudiciales que fueron resueltas en marzo de 2024, declarándose que las cadenas de consentimiento contienen datos personales, y que IAB Europe es corresponsable de su creación, pero no del uso posterior que otros agentes puedan darle a esos datos.

Aclaradas esas cuestiones, ahora el Tribunal de Mercado belga dictamina en ese mismo sentido, limitando la corresponsabilidad de IAB Europe a determinados aspectos del funcionamiento del TCF, confirmando la sanción de 250.000 euros inicialmente impuesta, y manteniendo la necesidad de implementar un plan de acción para garantizar el debido cumplimiento del RGPD.

La Audiencia Nacional se pronuncia sobre la sanción millonaria impuesta por la AEPD a una entidad bancaria en 2021

Esta resolución imponía sanciones por incumplimientos de los deberes de transparencia (2.000.000 euros), así como por ausencia de base legal suficiente para determinados tratamientos de datos personales por parte de la entidad financiera (4.000.000 euros).

Habiendo sido recurrida la resolución de la AEPD por parte de la sancionada, la Audiencia Nacional, en su sentencia al respecto, coincide con la AEPD en apreciar incumplimientos de la normativa aplicable, si bien difiere en el tratamiento jurídico de las conductas apreciadas, estimando parcialmente el recurso de la sancionada.

Lo más destacable de esta resolución es que la Audiencia Nacional aprecia un concurso medial por el cual los incumplimientos de los artículos 13 y 14 del RGPD, relacionados con la transparencia de la información facilitada a los interesados, se ven en cierto modo subsumidos en la sanción impuesta por el incumplimiento del artículo 6 RGPD sobre bases legales. En este sentido, se aprecia la comisión de una infracción del art. 6 RGPD en concurso medial con una infracción de los arts. 13 y 14 RGPD, y se impone una única sanción de 2 millones de euros.

Ello, a criterio de la Audiencia Nacional, a la vista de que, en caso de que la información de protección de datos facilitada por la entidad sancionada en sus políticas de privacidad hubiera sido completa y en pleno cumplimento de los citados artículos 13 y 14 del RGPD, el consentimiento de los interesados (que actuaba como base legal aplicable en este caso) podría haber sido válidamente recabado. Es decir, la Audiencia Nacional considera que el incumplimiento del deber de transparencia es un elemento esencial y consustancial a la violación del artículo 6 del RGPD. En este sentido, la sanción original se ve notablemente reducida.

Esta sentencia puede tener importantes implicaciones interpretativas de cara a futuro. Este mismo criterio podría ser trasladable a otras materias, como potenciales concursos mediales entre la falta de aplicación de medidas técnicas y organizativas de seguridad (art. 32 RGPD) y el deber de integridad y confidencialidad (art. 5 RGPD), infracciones que a menudo son sancionadas de manera independiente en casos de incidentes de seguridad. Por lo tanto, será de gran importancia hacer un seguimiento exhaustivo sobre posibles cambios de criterio de la AEPD en sus resoluciones venideras.

4. Actualidad

Las reformas en materia de protección de datos en Latam y sus efectos en las relaciones de trabajo

Autores: Ricardo Eckardt, Jairo Jaller, Franco Muschi, Mariana Ubidia, Miguel Ángel Rocha y José Alberto González Rebolledo

En un nuevo entorno caracterizado por la protección de los datospor encima de cualquier otra necesidad empresarial, las empresas se ven obligadas a revisar procesos y políticas internas, así como a adoptar medidas sólidas para garantizar el cumplimiento normativo y salvaguardar la información personal de sus trabajadores, candidatos y colaboradores. Desde procesos de selección hasta evaluaciones de desempeño y mecanismos de control laboral, el tratamiento de datos personales se ha vuelto un eje central en la gestión de personas. Sumado a ello, la utilización de herramientas de IA genera una exposición relevante de información personal –en muchos casos sensible– que, a menudo, requerirán de la adopción de políticas que garanticen la confidencialidad de la información que comenzarán a utilizar los departamentos de selección y reclutamiento.

Las regulaciones en la región latinoamericana han comenzado a responder a esta realidad. Perú, México y Chile ya han implementado reformas normativas relevantes en materia de protección de datos, mientras que en Colombia la regulación data de 2012, pero paulatinamente los empleadores y los trabajadores se han vuelto más conscientes de la importancia y la sensibilidad del manejo de datos personales. Este proceso de asimilación y de actualización de la normativa —que busca alinear las legislaciones locales con estándares internacionales— implica un mayor nivel de exigencia para los empleadores y una supervisión más rigurosa por parte de las autoridades.

A continuación, presentamos un panorama actualizado sobre los principales avances normativos y consideraciones prácticas en torno a la protección de datos personales en el entorno laboral en Perú, Colombia, México y Chile.

Perú

El 30 de noviembre de 2024 se publicó el Decreto Supremo N.º 016-2024-JUS, que aprueba el nuevo Reglamento de la Ley de Protección de Datos Personales (Ley N.º 29733), reemplazando íntegramente al reglamento anterior. Esta norma entró en vigencia el 30 de marzo de 2025 y marca un hito en la regulación peruana al incorporar estándares internacionales y establecer nuevas exigencias para el tratamiento de datos personales. En el ámbito laboral, introduce cambios sustanciales que requieren una revisión y adecuación integral de las prácticas empresariales vinculadas a la gestión de datos de trabajadores.

Como primer tema relevante, el nuevo reglamento refuerza obligaciones clave para los empleadores en el tratamiento de datos de trabajadores. De esta manera, se incorpora como infracción grave (sancionada con hasta USD 70,000.00 aproximadamente) el no informar de manera completa al trabajador sobre el tratamiento de sus datos personales, conforme al artículo 18 de la Ley. Esto exige revisar y adecuar todos los documentos informativos laborales (políticas, formatos, cláusulas, etc.).

Asimismo, se tipifica como infracción leve (hasta USD 7,000.00 aproximadamente) la atención fuera de plazo de los derechos ARCO (acceso, rectificación, cancelación y oposición), lo que obliga a revisar y fortalecer los procedimientos internos para el ejercicio de derechos por parte de los trabajadores.

Como novedad, se introduce la obligación de designar un oficial de datos personales cuando se cumplan ciertas condiciones. Recursos Humanos debe participar activamente en esta designación, ya que puede implicar cambios en funciones, acceso a información y condiciones laborales.

Finalmente, el reglamento detalla nuevas medidas de seguridad, como la exigencia de contar con un documento de seguridad actualizado y difundido internamente que incluya procedimientos de acceso, gestión de privilegios y uso de plataformas, entre otros. Su correcta implementación es esencial para minimizar riesgos legales, fortalecer la cultura de cumplimiento y promover la confianza de los trabajadores en la organización.

Colombia

La protección de los datos personales ha adquirido una relevancia creciente en el entorno empresarial, especialmente en el ámbito laboral. Desde la expedición de la Ley Estatutaria 1581 de 2012, que establece el régimen general de protección de datos personales, y sus decretos reglamentarios, las organizaciones están obligadas a implementar medidas que garanticen la privacidad, seguridad y tratamiento adecuado de la información personal de sus trabajadores.

Durante los últimos años, la Superintendencia de Industria y Comercio (SIC), como autoridad nacional en esta materia, ha fortalecido su rol de vigilancia y sanción, emitiendo nuevas instrucciones y decisiones que exigen a las empresas una revisión constante de sus políticas internas. Recientemente, se ha asimilado e interiorizado con mayor ahínco la regulación relacionada con la protección de datos y se han consolidado lineamientos más estrictos sobre el tratamiento de datos sensibles, la responsabilidad demostrada y la gestión de bases de datos, lo que ha llevado a un endurecimiento del régimen sancionatorio y a una mayor exigencia en la documentación de cumplimiento.

Dentro de la reciente emisión de reglamentos y directrices, se destacan las circulares externas expedidas por la Superintendencia de Industria y Comercio en materia de tratamiento de datos personales. Entre ellas, la Circular Externa No. 002 del 21 de agosto de 2024, que aborda el tratamiento de datos personales en sistemas de inteligencia artificial, y la Circular Externa No. 003 del 22 de agosto del mismo año, que imparte instrucciones a los administradores de compañías sobre el tratamiento de dicha información.

En el contexto laboral, estas disposiciones implican una transformación significativa en la forma en que las empresas gestionan la información de sus trabajadores. Desde la obtención del consentimiento informado durante el proceso de selección hasta la implementación de medidas de ciberseguridad, las organizaciones deben garantizar que sus prácticas respeten los derechos de los trabajadores y se alineen con los principios de legalidad, finalidad, libertad, veracidad, transparencia, acceso y circulación restringida.

La autoridad ha procurado emitir de manera constante lineamientos y guías dirigidas a orientar a las empresas y sus colaboradores en el tratamiento adecuado de datos personales. Estos instrumentos incluyen

cartillas y documentos técnicos sobre temas como la implementación del oficial de cumplimiento en protección de datos, así como sobre actividades relevantes para las organizaciones, como la videovigilancia y su adecuada gestión conforme a la normativa vigente.

Este marco normativo no solo busca proteger la intimidad de los trabajadores, sino también fomentar una cultura organizacional basada en la confianza, la transparencia y el cumplimiento normativo. Así, la protección de datos personales se ha venido convirtiendo en un eje fundamental de las relaciones laborales modernas en Colombia.

México

El 20 de marzo de 2025, se publicó en el Diario Oficial de la Federación una nueva Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Esta legislación, que reemplaza a la norma de 2010, introduce disposiciones más claras y robustas para garantizar el tratamiento legítimo y seguro de la información personal en el país. A continuación, exploramos las principales novedades y su impacto en el entorno empresarial latinoamericano.

Mayor claridad y obligaciones: a nueva ley refuerza los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición), ahora definidos con precisión y reconocidos explícitamente, superando la ambigüedad de la legislación anterior. Además, impone obligaciones más estrictas a las empresas y personas que manejen datos personales, ya sea en formato físico, electrónico o de cualquier tipo. Entre los requisitos destacan:

1. Avisos de privacidad más detallados: las empresas deben informar de manera clara y accesible sobre los propósitos del tratamiento de datos, especificando: (i) qué datos se recopilan, incluyendo los sensibles; (ii) cuáles requieren consentimiento expreso y, (iii) cómo ejercer los derechos ARCO.

2. Derecho a la oposición: los titulares de datos pueden oponerse a su tratamiento si existe una causa legítima, como un posible daño o perjuicio, o cuando el uso automatizado de datos afecte sus derechos, evalúe aspectos personales (desempeño laboral, situación económica o salud, entre otros) o genere efectos jurídicos no deseados.

3. Confidencialidad obligatoria: las organizaciones deben implementar controles para garantizar que cualquier persona involucrada en el manejo de datos mantenga estricta confidencialidad.

4. Cultura de protección de datos: las empresas deberán fomentar la protección de datos internamente, designando, si es necesario, un responsable o departamento para gestionar solicitudes relacionadas con los derechos ARCO.

Nuevo enfoque institucional: uno de los cambios más significativos es la desaparición del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) como órgano garante. En su lugar, la Secretaría Anticorrupción y Buen Gobierno asumirá la supervisión, verificación y sanción en materia de datos personales a nivel federal. Las resoluciones de esta Secretaría podrán impugnarse únicamente mediante un juicio de amparo en tribunales especializados, eliminando la vía del juicio de nulidad ante el Tribunal Federal de Justicia Administrativa.

Además, las sanciones y costos asociados al ejercicio de derechos ARCO se calcularán con base en la unidad de medida y actualización vigente, asegurando una base económica actualizada.

Impacto en el ámbito laboral: para las empresas en México y la región, esta reforma implica una revisión urgente de sus prácticas administrativas. Los empleadores deberán: (i) actualizar avisos de privacidad, contratos y reglamentos internos para cumplir con la nueva ley; (ii) implementar procesos que garanticen transparencia en el manejo de datos de empleados y(iii) capacitar a su personal en la protección de datos para evitar riesgos legales.

Estos cambios no solo fortalecerán la confianza de los trabajadores sino que también posicionan a las empresas como actores responsables en un entorno donde la privacidad es una prioridad global.

Chile

Tras siete años de debate legislativo, Chile cuenta con una nueva Ley de Protección y Tratamiento de Datos Personales (Ley 21.719), promulgada en diciembre de 2024 y que entrará en vigencia el último mes de 2026. Esta ley representa un hito al alinear la regulación nacional con los estándares internacionales, especialmente el Reglamento General de Protección de Datos (GDPR) de la Unión Europea, estableciendo un marco robusto y moderno para la gestión de datos personales en el país.

La nueva normativa es de aplicación general, abarcando a todas las personas naturales y jurídicas. Entre sus principales novedades, destaca la creación de la Agencia de Protección de Datos Personales, organismo autónomo encargado de dictar instrucciones, interpretar la ley, fiscalizar su cumplimiento y aplicar sanciones. Esta institucionalidad será clave para la correcta implementación y supervisión del nuevo régimen.

En el ámbito laboral, la ley reconoce a los trabajadores como titulares de datos personales frente a sus empleadores. Esto implica que ellos cuentan con los siguientes derechos sobre su información: acceso, rectificación, supresión, oposición, portabilidad y bloqueo de datos. Estos derechos son irrenunciables y deben ser respetados en toda relación laboral, reforzando la obligación ya existente en el artículo 154 ter del Código del Trabajo, que exige a los empleadores mantener la reserva de la información privada de sus trabajadores.

El tratamiento de datos personales en el contexto laboral podrá realizarse con el consentimiento expreso del trabajador, pero también será lícito cuando sea necesario para la ejecución del contrato de trabajo, el cumplimiento de obligaciones legales o la satisfacción de intereses legítimos del empleador, siempre que no se vulneren los derechos y libertades del trabajador. Especial atención merecen los datos sensibles, como los relativos a la salud, que solo podrán ser tratados bajo estrictas condiciones y con mayores resguardos.

Para las empresas, la entrada en vigencia de la ley implica la necesidad de revisar y adecuar sus políticas y procedimientos internos de tratamiento de datos. Será fundamental implementar medidas que aseguren el cumplimiento de los principios rectores de la ley: licitud, finalidad, proporcionalidad, calidad, responsabilidad, seguridad, transparencia y confidencialidad. Además, las empresas multinacionales deberán poner especial atención a los nuevos requisitos para la transferencia internacional de datos, asegurando que los países de destino cuenten con niveles adecuados de protección o que existan garantías contractuales suficientes.

En este periodo de transición hasta diciembre de 2026, las empresas deben anticipar la adecuación de sus sistemas, capacitar a sus equipos y estar atentas a la dictación de los reglamentos y directrices que la futura Agencia de Protección de Datos Personales emitirá, los cuales darán mayor claridad y sentido práctico a la ley.

Es de suma relevancia el adecuarse correctamente a la ley, dado que el incumplimiento de la normativa puede acarrear sanciones significativas, con multas que pueden alcanzar hasta 20.000 UTM (1.466.600 euros aprox.), suma que podría triplicarse en caso de reincidencia. Esto subraya la importancia de una gestión proactiva y responsable de los datos personales, tanto para evitar riesgos legales como para fortalecer la confianza de trabajadores y clientes en la organización.

En síntesis, la nueva ley marca un antes y un después en la protección de datos en Chile, exigiendo a las empresas un compromiso real con la privacidad y la seguridad de la información, especialmente en el ámbito laboral. La preparación y adaptación

temprana serán claves para enfrentar con éxito este nuevo escenario regulatorio.

Lorenzo Cotino Hueso y Francisco Pérez Bes toman posesión como presidente y adjunto, respectivamente, de la AEPD

El 3 de marzo de 2025, Lorenzo Cotino Hueso y Francisco Pérez Bes tomaron posesión como presidente y adjunto, respectivamente, de la Agencia Española de Protección de Datos (AEPD), en un acto celebrado en la sede de la Agencia y presidido por el ministro de la Presidencia, Justicia y Relaciones con las Cortes, Félix Bolaños.

Durante su intervención, Lorenzo Cotino subrayó los desafíos que plantea el "tsunami digital" para la privacidad, especialmente en ámbitos como los espacios digitales, la salud y la inteligencia artificial, y anunció la elaboración de un plan estratégico para afrontarlos. Por su parte, Francisco Pérez Bes destacó el compromiso de la AEPD con la cercanía al ciudadano, la transparencia, la agilidad y la innovación, así como con la colaboración institucional.

El ministro Bolaños remarcó la importancia del papel que asumen ambos cargos en un contexto de tensiones crecientes entre tecnología y privacidad, y anunció que la Ley para la protección de los menores en entornos digitales será aprobada próximamente en segunda vuelta en el Consejo de Ministros, iniciando así su tramitación parlamentaria.

El nombramiento de ambos responsables se formalizó mediante los Reales Decretos 142/2025 y 143/2025, respectivamente. El acto contó con la presencia de autoridades como Manuel Olmedo, Rafael Simancas y la exdirectora de la AEPD, Mar España, así como representantes del sector público y privado.

La AEPD participa en una acción europea para analizar la aplicación del derecho de supresión

El 5 de marzo de 2025, la Agencia Española de Protección de Datos (AEPD) anunció su participación en una acción europea coordinada centrada en el análisis del derecho de supresión (artículo 17 del RGPD), uno de los más ejercidos por los ciudadanos y también uno de los que más reclamaciones genera ante las autoridades de protección de datos. En concreto, se evaluará si los procesos utilizados son accesibles, comprensibles y eficaces para los ciudadanos.

Esta iniciativa se enmarca en el programa de acciones del Comité Europeo de Protección de Datos (CEPD) para 2025, y cuenta con la participación de 32 autoridades nacionales. La AEPD analizará cómo una muestra de responsables del tratamiento, tanto del sector público como privado, atienden las solicitudes de supresión, identificando buenas prácticas y posibles deficiencias.

Los resultados se evaluarán de forma conjunta y podrían dar lugar a nuevas acciones de supervisión o aplicación en cada país. Además, se elaborará un informe agregado que ofrecerá una visión general del cumplimiento en el Espacio Económico Europeo, y los resultados se utilizarán para fomentar mejores prácticas y promover una aplicación coherente del derecho de supresión en el ámbito europeo.

Esta acción refleja la prioridad del CEPD de garantizar la protección efectiva de los derechos fundamentales en entornos digitales, especialmente en plataformas con un alto impacto sobre la privacidad de los usuarios. Es la cuarta acción del Marco de Aplicación Coordinada del CEPD, que busca reforzar la cooperación entre autoridades. Las acciones anteriores abordaron el derecho de acceso, el uso de servicios en la nube por el sector público y la figura del delegado de protección de datos.

Luz verde al anteproyecto de ley para regular la inteligencia artificial en España

El Gobierno ha aprobado el Anteproyecto de Ley de Gobernanza de la IA, que busca garantizar un uso ético, inclusivo y centrado en las personas. La norma adaptará el marco legal español al Reglamento Europeo de IA, en vigor desde 2024 y parcialmente aplicable ya, y se tramitará por la vía de urgencia. Próximamente deberá ser aprobada definitivamente por el Consejo de Ministros como proyecto de ley y se remitirá a las Cortes para su aprobación.

El texto establece, como cuestión destacada, qué autoridades supervisarán los sistemas prohibidos y los de alto riesgo según su ámbito de aplicación. Para los sistemas prohibidos, se asigna competencia a la AEPD (biometría y fronteras), el CGPJ (justicia), la Junta Electoral Central (procesos democráticos) y la AESIA (resto de usos). En cuanto a los sistemas de alto riesgo, se suman el Banco de España (solvencia crediticia), la CNMV (mercados financieros) y la Dirección General de Seguros (seguros).

Cataluña inicia una prueba piloto basada en IA para asistir en la redacción de sentencias judiciales

Cataluña ha iniciado un proyecto pionero en España con el uso de inteligencia artificial en tribunales a través de AI4JUSTICE, un asistente basado en IA diseñado para dar soporte a jueces en la redacción de sentencias.

El sistema permite búsquedas semánticas en jurisprudencia y fundamentos legales, con el objetivo de acelerar la resolución de casos repetitivos, optimizando el tiempo y permitiendo que los jueces se concentren en asuntos más complejos.

Desde septiembre de 2024, cuatro jueces mercantiles de la Audiencia de Barcelona han estado utilizando AI4JUSTICE en casos relacionados con cláusulas suelo y reclamaciones por incidencias en vuelos. Los primeros resultados muestran una reducción del tiempo de redacción de sentencias de dos horas a tan solo veinte minutos, y la previsión es un ahorro anual de 12.000 horas y 552.000 euros por cada veinte jueces.

El Gobierno aprueba el proyecto de Ley de Protección de los Menores en el entorno digital

Esta ley ha sido elaborada por los Ministerios de Juventud e Infancia, Justicia, Derechos Sociales y Transformación Digital. Al anteproyecto de la ley presentado en junio del año pasado se han incorporado aportaciones de numerosos organismos públicos y privados de España, así como de la Comisión Europea.

Entre otras medidas, el proyecto introduce el aumento de la edad mínima para redes sociales de 14 a 16 años para plataformas como Facebook, Instagram o TikTok (debiendo las empresas implementar sistemas fiables de verificación de edad), la obligación de los dispositivos móviles de incluir por defecto sistemas de control parental que se activarán durante la configuración inicial, y la tipificación como delito de la creación y difusión no autorizada de imágenes o audios manipulados mediante IA que resulten sexualmente explícitos o gravemente vejatorios.

También se han endurecido las penas de las sanciones contra adultos que engañan a menores en línea con fines sexuales, y se prohíbe el acceso de menores a mecanismos aleatorios de recompensa -conocidos como *"loot boxes"*-, un sistema que se incluye en muchos videojuegos.

La 'Information Commissioner's Office' (ICO) publica su guía sobre anonimización y seudonimización

La guía hace hincapié en la anonimización efectiva como proceso para hacer que los datos personales no sean identificables, recomendando evaluaciones de riesgo periódicas y la prueba del "*motivated intruder*" para garantizar que los datos permanezcan anónimos.

Para la ICO, que unos datos sean anónimos o seudónimos depende del contexto, adoptando

en este punto la doctrina subjetiva del TJUE que establece que hay que valorar la capacidad de la parte que trata los datos para concluir si son anónimos o seudónimos con base en si, en cada caso concreto, el responsable dispone de medios razonables para identificar a la persona. Lo que puede ser anónimo para uno puede no serlo para otro que sí tiene capacidad, en el contexto específico, de reidentificar a partir de un dato seudonimizado.

La guía también recomienda que las organizaciones adopten un enfoque global de la gobernanza a la hora de anonimizar o compartir datos anónimos, en concreto mediante la adopción de medidas como llevar a cabo evaluaciones de impacto sobre la protección de datos (EIPD) para documentar las decisiones de anonimización e identificar riesgos y mitigaciones, coordinarse con otras organizaciones que puedan tratar datos relacionados que afecten a la identificabilidad, y definir mecanismos y responsabilidades de supervisión.

La Comisión Europea publica un proyecto de reglamento sobre las Normas Técnicas de Reglamentación para la subcontratación en virtud del Reglamen-to DORA

La Comisión Europea publicó el pasado 24 de marzo un proyecto de reglamento en el que se detallan las Normas Técnicas de Reglamentación para la subcontratación en virtud del Reglamento DORA, que incluye normas para la subcontratación de servicios de TIC que apoyan funciones críticas o importantes.

Entre estas obligaciones, se incluyen normas sobre proporcionalidad, aplicación para grupos, diligencia debida, evaluación de riesgos, descripción y condiciones de la subcontratación, y cambios materiales en los acuerdos y derechos de rescisión de las entidades financieras. Además, se especifica que las entidades financieras deben ser informadas de los cambios materiales en los acuerdos de subcontratación y que tienen derecho a oponerse o rescindir los contratos si se superan las tolerancias de riesgo o se produce una subcontratación no autorizada.

La empresa 23andMe se declara en quiebra tras el incidente de seguridad sufrido en 2023

La empresa estadounidense 23andMe, especializada en análisis de ADN y pruebas genéticas directas al consumidor, se ha declarado en quiebra tras años de pérdidas económicas y tras el grave incidente de ciberseguridad que en 2023 comprometió los datos personales de millones de usuarios. 23andMe ha recopilado información genética de más de quince millones de personas.

Tras la declaración de bancarrota, 23andMe anunció que buscará una venta, lo que significa que la compañía, y con ella la información genética de sus quince millones de clientes, probablemente pronto estarán disponibles en el mercado. La empresa defiende que no cambiará la forma en que gestiona ni protege los datos de sus clientes, y declara que la privacidad de los datos será un factor importante en cualquier posible transacción que se produzca.

Sin embargo, el fiscal general de Nueva York ha emitido recomendaciones en relación con este asunto, dando instrucciones a los consumidores para que borren los datos genéticos facilitados a la citada compañía y destruyan las muestras de ADN suministradas.

El CEPD publica un informe en relación con los riesgos que conllevan los modelos de lenguaje de gran tamaño y su mitigación

El 10 de abril, el CEPD publicó un informe proporcionando guías y herramientas para la gestión de riesgos de privacidad en sistemas basados en modelos de lenguaje. La metodología ayuda a identificar, evaluar y mitigar riesgos de privacidad y protección de datos, apoyando un desarrollo responsable.

Las orientaciones respaldan los artículos 25 y 32 del RGPD, ofreciendo medidas de seguridad y protección de datos. No obstante, la adopción de dichas medidas no reemplaza por sí misma a la Evaluación de Impacto relativa a la Protección de Datos (EIPD) del artículo 35 del RGPD, sino que, en su caso, la complementa.

Publicadas las directrices europeas sobre el tratamiento de datos personales mediante tecnologías de 'blockchain'

El Comité Europeo de Protección de Datos ha publicado las Directrices 02/2025, de momento en fase de consulta pública. El CEPD destaca la complejidad e incertidumbre del *blockchain* en relación con el tratamiento de datos personales, lo que plantea desafíos específicos para cumplir con el RGPD. Es crucial evaluar los riesgos para los derechos y libertades de los interesados, mitigando algunos mediante medidas técnicas.

Las propiedades de *blockchain* pueden dificultar el cumplimiento de requisitos como el derecho de rectificación y el derecho al olvido. Las directrices proporcionan un marco para que las organizaciones evalúen cuidadosamente el uso de *blockchain* y las responsabilidades de los actores involucrados.

El SEPD publica un dictamen sobre la prórroga de la decisión de adecuación del Reino Unido

En junio de 2021, la Comisión Europea adoptó dos decisiones de adecuación para el Reino Unido, una bajo el RGPD y otra bajo la Directiva 2016/680 sobre protección de datos en el ámbito penal, permitiendo la transferencia de datos personales desde el Espacio Económico Europeo (EEE) al Reino Unido. Ambas decisiones incluían una cláusula de caducidad fijada para el 27 de junio de 2025, salvo renovación. En octubre de 2024, el gobierno del Reino Unido introdujo el proyecto de ley *Data (Use and Access) Bill*, que propone modificar ciertos aspectos de la legislación británica de protección de datos.

Dado que no estaba previsto que el proceso legislativo concluyera antes de la primavera de 2025, la Comisión propuso una prórroga técnica y limitada de seis meses, hasta el 27 de diciembre de 2025, para permitir la conclusión de dicho proceso legislativo y mantener mientras la protección adecuada de los datos. La Comisión requirió la opinión del Supervisor Europeo de Protección de Datos (SEPD), que consideró razonable la prórroga, subrayando su carácter excepcional y la necesidad de evaluar el marco legal definitivo una vez adoptado. El SEPD aclaró que esta prórroga no reabre ni modifica sus valoraciones previas sobre la adecuación del Reino Unido -que serán evaluadas tras la conclusión del proceso legislativo- ni prejuzga futuras decisiones, y que sus dictámenes emitidos en 2021 (dictámenes 14/2021 y 15/2021) siguen siendo válidos y deben ser tenidos en cuenta en futuras evaluaciones.

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

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

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

Marta Sabio
Asociada · Barcelona
marta.sabio@garrigues.com

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

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

Laia Llambric
Asociada · Bilbao
laia.llambrich@garrigues.com

Más información:

Economía del Dato, Privacidad y Ciberseguridad

GARRIGUES

Plaza de Colón, 2
28046 Madrid
T +34 91 514 52 00
info@garrigues.com

Síguenos en: