29/02/2024

Más de 16 millones de euros en multas por infracciones en privacidad en 2023

La sanción de mayor cuantía el pasado año es la impuesta a Endesa de seis millones por una brecha de seguridad. Los expertos prevén que en 2024 habrá menos multas, pero de mayor importe



La Agencia Española de Protección de Datos (AEPD) ha impuesto 357 sanciones en 2023 por un importe total que asciende a más de 16 millones de euros, según la información recogida por LA LEY a partir de lo publicado por la AEPD hasta el 24 de enero de 2024. Unas cifras que se espera que aumenten ligeramente cuando la agencia termine de publicar todas sus resoluciones del pasado año y lance su memoria anual de 2023, prevista para la próxima primavera.

La videovigilancia sigue siendo la materia con más sanciones, aunque sus multas no son ni de lejos las de mayor cuantía. El motivo, según Leandro Núñez, socio de Audens y experto en protección de datos, es que "las cámaras son cada vez más baratas y fáciles de instalar, lo que provoca que, en vez de contar con profesionales para su colocación, pymes y particulares las monten por su cuenta y riesgo".

El primer puesto en cuanto al importe de sus sanciones es para las quiebras de seguridad, con 43 resoluciones sancionadoras que suman más de 8 millones de euros. Este resultado se debe, en gran medida, a que la mayor multa, de 6.100.000 euros, es la impuesta el pasado mes de octubre a Endesa por una brecha en la seguridad de sus sistemas de protección de datos en las plataformas utilizadas por los clientes, lo que provocó el acceso de terceros a la información de más de seis millones de personas. En agosto de 2021, Endesa detectó que se estaban publicando en Facebook claves de acceso para acceder a su plataforma Sales Folder, pero en ese momento no tomó las medidas pertinentes ni avisó a las autoridades. Posteriormente, la empresa de energía rectificó: se puso en contacto con Facebook Spain para que retirase los anuncios e informó a la AEPD y a los usuarios afectados.

"La importancia de esta sanción radica en que se impuso por la falta de diligencia de la compañía al adoptar medidas demasiado tarde", remarca Paloma Bru, socia del departamento de TMT de Pinsent Masons en Madrid. La abogada añade que, a pesar de que se trata de una multa muy elevada, aún está lejos de las cuantías que imponen otros Estados de la Unión Europea por infracciones del Reglamento General de Protección de Datos (RGPD), como la sanción de 1.200 millones a Meta o la de 345 millones a TikTok, ambas en Irlanda.

Sanciones elevadas

La segunda multa de mayor cuantía, 2,5 millones de euros, recayó en Openbank, también en el mes de octubre. La entidad financiera no aplicó un enfoque de protección de datos en el diseño de su proceso para solicitar y recabar la documentación que necesitaba para cumplir con los protocolos contra el blanqueo de capitales.

La agencia concluyó que -Openbank no tuvo en cuenta la privacidad de sus clientes ni antes ni durante la realización del tratamiento de sus datos financieros al emplear este procedimiento. “Un usuario reclamó porque consideraba que el e-mail no es una vía apropiada para enviar según qué documentación, al ser una tecnología intrínsecamente insegura y fácil de interceptar por terceros”, comenta Leandro Núñez.

Otra de las sanciones millonarias de 2023 fue la impuesta a BBVA. En un primer momento, la multa fijada por la AEPD ascendió a 1,6 millones de euros. Sin embargo, tras la rectificación de errores en la contratación no autorizada de productos, la multa se redujo al millón de euros para sancionar la persistente falta de medidas de seguridad en sus procedimientos de comunicación, inclusión y mantenimiento en los sistemas de información crediticia de datos personales. Finalmente, gracias al uso de las reducciones previstas en la normativa, la sanción a la entidad financiera quedó en 800.000 euros.

“Las sanciones recibidas por estos dos grandes bancos españoles (Openbank y BBVA), son destacables no solo por su cuantía”, afirma Núñez, “sino también porque analizan el incumplimiento de una de las obligaciones más importantes, y menos conocidas por las empresas, del RGPD: la protección de datos desde el diseño”.

Además del financiero o del energético, otro sector muy sancionado por la agencia ha sido el de las telecomunicaciones. “Sigue habiendo una tendencia muy elevada de sanción a las empresas de telecomunicaciones por no prevenir acciones de fraude a sus clientes, como el duplicado de tarjetas SIM (SIM swapping)”, apunta Paula Garralón, abogada de privacidad y nuevas tecnologías en Bird & Bird. Por ejemplo, Vodafone y Digi han sido sancionadas, con multas de entre 40.000 y 140.000 euros por infracciones relacionadas con este motivo de manera reiterada en 2023.

Multas a particulares

Por otro lado, las multas de la AEPD a personas físicas cada vez son más habituales. Sus infracciones ya no solo se dan en materia de videovigilancia, es decir, por la instalación de sistemas de seguridad que no cuentan con las medidas de protección de datos previstas en la normativa, sino que también son numerosas en el ámbito de los servicios de internet, con la publicación de datos en redes sociales sin consentimiento, o por el incumplimiento de las políticas de privacidad.

Así, de las 121 resoluciones sancionadoras de la AEPD contra personas físicas en 2023, 91 son relativas a infracciones en materia de videovigilancia y diez del sector de los servicios de internet. La suma de todas las sanciones impuestas a personas físicas supera los 100.000 euros. De las seis que han alcanzado o superado los 10.000 euros, cinco se deben a la publicación en redes sociales de datos de carácter personal sin consentimiento, y la otra, a haber tirado al depósito de la basura doméstica, en repetidas ocasiones, documentación de índole sanitaria con datos personales de terceros.

A pesar de ello, Garralón insiste en que el grueso de las sanciones seguirá recayendo en las empresas, ya que el tratamiento de datos personales fuera del ámbito doméstico por particulares es muy residual.

Más concienciación

La cantidad de sanciones por infracciones del RGPD en España está directamente relacionada con una mayor concienciación de los ciudadanos, que cada vez denuncian más estas malas prácticas. “Hace cinco años muy poca gente había ejercitado alguno de sus derechos de protección de datos o conocía la existencia de la agencia”, destaca Garralón.

Esto también se traduce en un creciente interés de las empresas por cumplir en materia de protección de datos. “Desde la entrada en vigor de RGPD hemos notado un aumento de los recursos que las compañías dedican al cumplimiento de esta normativa, y creemos que esta tendencia seguirá incrementándose, también para evitar los daños reputacionales”, afirma Paloma Bru.

Para Leandro Núñez, la gran novedad de cara a 2024 es la creación de un nuevo procedimiento destinado a apercibir, en lugar de sancionar, cuando, ante ciertas infracciones, la AEPD entienda que no es necesario imponer una multa para garantizar el cumplimiento del RGPD. De hecho, Bru considera que la agencia ya ha comenzado a reducir el número de multas y a aumentar su importe, acercándose así a los criterios de otros países europeos.

SECTORES MÁS EXPUESTOS A INFRINGIR EL RGPD

Factores. El tipo de tratamiento, la tipología y el volumen de datos que manejen son los tres elementos que marcan el riesgo de las empresas para cometer una infracción del Reglamento General de Protección de Datos (RGPD).

Tecnología y servicios en línea. Las compañías que ofrecen servicios en línea y tecnología suelen recopilar y procesar una gran cantidad de datos para personalizar experiencias. “Las infracciones más comunes se deben a errores humanos y a deficiencias en las medidas de seguridad implementadas”, precisa Leandro Núñez, socio de Audens y experto en protección de datos.

Servicios financieros. Las instituciones financieras manejan información sensible, como datos bancarios y de tarjetas de crédito. En consecuencia, según indica Paloma Bru, socia del departamento de TMT de Pinsent Masons en Madrid, en este sector las infracciones más habituales son violaciones de seguridad, pérdida de datos y accesos no autorizado.

Salud y farmacéuticas. Las organizaciones en el ámbito de la salud procesan datos médicos confidenciales. Los incumplimientos en este caso suelen estar relacionados con la falta de medidas de seguridad robustas, la divulgación no autorizada de información médica y la retención de datos por más tiempo del necesario.

Recursos humanos. Cualquier empresa desde su departamento de RR HH gestiona datos de sus empleados y debe garantizar que el procesamiento de esa información cumpla con el RGPD. La falta de consentimiento para procesar esos datos, la retención inadecuada de información y la falta de seguridad en los datos del personal, son las infracciones más frecuentes.

Fuente

Link de la noticia