Resolución sancionadora de la AEPD por uso de datos biométricos para registro de jornada laboral

Nota informativa

La Agencia Española de Protección de Datos (AEPD) ha dictado una nueva resolución, imponiendo una multa de **365.000 euros** por el uso de datos biométricos con fines de registro de jornada laboral, por infracción de los artículos 13 (*incumplimiento del deber de información*), 32 (*falta de adopción de medidas de seguridad adecuadas*) y 35 (*Evaluación de Impacto en materia de protección de datos insuficiente*) del RGPD.

Se trata de la primera resolución que sale a la luz tras la publicación de la controvertida "*Guía sobre tratamientos de control de presencia mediante sistemas biométricos*" publicada por la AEPD en noviembre de 2023 siendo, por tanto, una resolución muy esperada.

Entre los principales criterios interpretativos, por no decir el único, que la AEPD ratifica respecto a la Guía es que los sistemas de autenticación/identificación constituyen un tratamiento de categorías especiales de datos personales – *criterio que, por otra parte, ya se entendía superado tras las Directrices 05/2022, del Comité Europeo de Protección de Datos (CEPD), sobre Tecnologías de Reconocimiento facial*-.

Al margen de lo anterior, lo cierto es que lejos de confirmar los criterios interpretativos manifestados en la Guía, en la resolución, la AEPD ni siquiera entra a analizar si la base de legitimación sería adecuada a la finalidad pretendida y tampoco clarifica si el tratamiento sería viable en los términos propuestos por la entidad.

En definitiva, es muy reseñable el hecho de que la AEPD huya de analizar una de las principales cuestiones suscitadas tras la publicación de la Guía, esto es, la legitimidad del tratamiento de datos biométricos, y opte por sancionar por otras cuestiones relativas al deber de información, la aplicación de medidas de seguridad y la validez de la evaluación de impacto realizada.

(I) Supuesto de hecho

La resolución tiene su origen en la reclamación interpuesta ante la AEPD en febrero de 2022 por un particular contra su entidad empleadora por la solicitud de datos biométricos, en concreto, la huella dactilar, para ser utilizada tras la implantación de un sistema de fichaje basado en ese dato.

El reclamante expuso que, en el momento de recabar los datos biométricos, la entidad reclamada no comunicó que la información respecto al tratamiento de dichos datos se encontraba en el portal del empleado, no siendo fácilmente accesible para todos los empleados el acceso a la misma.

(II) Análisis de las infracciones e interpretación de la AEPD

a. Infracción del artículo 13 del RGPD (incumplimiento del deber de información)

La AEPD considera acreditado que la entidad no informó correctamente sobre el tratamiento de los datos biométricos, limitándose a incluir la siguiente referencia en la cláusula informativa: "*está instalado un lector de huella dactilar para acceso a oficinas*".

Adicionalmente, en la resolución se interpreta que la propia actualización de la cláusula, tras el requerimiento de información por parte de la AEPD, corrobora en si misma esa falta de información.

b. Infracción del artículo 32 del RGPD (medidas de seguridad inadecuadas)

En relación con la infracción del artículo 32 del RGPD y, pese a que la entidad informó a la AEPD sobre las medidas de seguridad habitualmente aplicadas en este tipo de sistemas, a juicio de la AEPD se consideran insuficientes, ya que:

i) en la información facilitada por la entidad se constata el acceso de algunos usuarios que no constan en el listado de usuarios autorizados;
ii) no queda acreditado el borrado de la huella tras su captura; y
iii) el hash de la huella y los datos identificativos de los empleados se encuentran en "tablas" diferenciadas, si bien, no se han constado las medidas implantadas para separar el acceso a ambas "tablas".

En relación con la primera de las medidas, resulta curioso, que la AEPD informa de una "*rebaja*" en la sanción impuesta por infracción del artículo 32 del RGPD al no poder determinarse con total certeza el acceso por usuarios no autorizados, si bien, con respecto a las otras dos medidas la entidad no aportó información o alegaciones al respecto.

c. Infracción del artículo 35 del RGPD (evaluación de impacto insuficiente)

La AEPD entiende que la evaluación de impacto aportada adolecía de los requisitos establecidos, en concreto, dicho documento se realizaba sobre un tratamiento en el que no existía un tratamiento de datos de categoría especial - *la entidad reclamada alegaba el uso de un sistema de autenticación y no de identificación*-, no detallaba las finalidades del tratamiento y no realizaba un verdadero juicio de proporcionalidad y necesidad respecto al tratamiento de datos biométricos, sin proponer, como viene siendo habitual, cuál debería ser el método correcto, según su criterio.

Además de las anteriores infracciones, la AEPD prevé un plazo de seis (6) meses para que la entidad adopte las medidas de subsanación necesarias. No obstante, si de conformidad con la interpretación realizada por la AEPD en su Guía, la legitimidad del tratamiento podría ser cuestionable y, además, el tratamiento no superase el juicio de necesidad – *tal y como indica la AEPD en la propia resolución*-, la efectividad de dichas medidas de subsanación podrían devenir en absolutamente innecesarias.

Por el contrario, también podría interpretarse que si la entidad cumple todas las medidas el tratamiento sería legítimo y proporcionado a ojos de la AEPD. Sin duda, una cuestión que queda en el aire.

Conclusión

La resolución analizada pone de manifiesto los riesgos asociados del uso de sistemas que utilicen datos biométricos en el entorno laboral, incluyendo la importancia de informar adecuadamente a los empleados, acreditar la adopción de medidas de seguridad adecuadas, así como, la obligación de llevar a cabo una Evaluación de Impacto en cumplimiento del artículo 35 del RGPD al tratarse de un tratamiento de alto riesgo para los derechos y libertades de los interesados.

No obstante, también se pone en tela de juicio el criterio interpretativo de la AEPD al no entrar a valorar uno de los principales caballos de batalla, esto es, la legitimidad del tratamiento de datos, así como, fijar criterios claros y homogéneos que permitan generar seguridad jurídica.

Por lo expuesto, y en caso de optar por el uso de sistemas de control de presencia y control de acceso mediante el uso de datos biométricos, se deberán analizar los riesgos para los derechos y libertades de los interesados y, en consecuencia, adoptar todas las medidas a fin de minimizar los riesgos asociados al tratamiento teniendo en cuenta los distintos criterios interpretativos que puedan ser manifestados por la AEPD o los Tribunales.