Necesidad de revisar la implantación de tecnologías de uso de datos biométricos para control de presencia o control de acceso

Con fecha 27 de noviembre de 2023 la AEPD ha publicado una guía sobre el tratamiento de los datos derivados del control de presencia mediante sistemas biométricos, que pone en riesgo la utilización de estas herramientas tecnológicas.

El RGPD recoge en el ordinal 14 del artículo 4, la definición de datos biométricos como *"datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos"*. De acuerdo con esta definición son datos biométricos todos aquellos que permitan la identificación o autenticación de una persona.

A modo de ejemplo, son datos biométricos, la huella dactilar, el reconocimiento facial, la firma personal, la lectura de retina e iris, etc.

Las empresas que utilicen este tipo de tecnologías para cumplir, por ejemplo, con el registro laboral de la jornada o para el control de acceso tanto con fines laborales como no laborales, deben revisar su utilización, toda vez que la AEPD ha modificado la interpretación sobre la tipología de datos que otorgaba a los datos biométricos en la que de acuerdo con la guía publicada por la AEPD sobre el tratamiento de datos personales en las relaciones laborales, de fecha 18 de mayo de 2021, consideraba que el tratamiento de datos biométricos en los supuestos de identificación uno a uno no son categorías especiales de datos, pudiendo en ese caso utilizarse para el cumplimiento de una obligación legal o para el cumplimiento de la ejecución de un contrato.

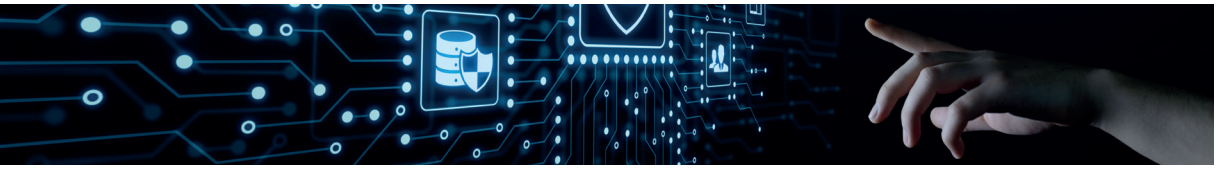
A partir de las Directrices publicadas por el Consejo Europeo de Protección de Datos de 26 de abril de 2023, la AEPD ha revisado su interpretación porque conforme a estas Directrices tanto la identificación biométrica como la autenticación biométrica son procesos que implican el tratamiento de categorías especiales de datos.

Esto supone que los criterios establecidos se refuerzan y las organizaciones deberán revisar la evaluación de impacto, en su día realizada, con objeto de acreditar que el uso de estas herramientas pasa el juicio de idoneidad, necesidad y proporcionalidad del tratamiento y las medidas técnicas, organizativas jurídicas hasta ahora implantadas deberán revisarse al objeto de ser reforzadas.

La AEPD califica la utilización de datos biométricos como un tratamiento de datos independiente de "Alto Riesgo" por considerar que se trata de categorías especiales de datos conforme establece el artículo 9.1 del RGPD, que como norma general prohíbe el tratamiento de categorías especiales de datos, salvo que estemos ante un supuesto de los previstos en el número 2 del precitado artículo 9.

En el caso del **registro de jornada y control de acceso con fines laborales**, para que se supere el levantamiento de la prohibición prevista en el artículo 9.1, podríamos considerar de aplicación lo dispuesto en la letra b), del número 2 del artículo 9 que dice expresamente:

"b) el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado"



Por lo que podría aplicarse el levantamiento de la prohibición sobre la base del cumplimiento de una obligación legal del responsable en el ámbito laboral y de la seguridad y de la protección social, en la medida que **así lo autorice una norma con rango legal**, ya sea dictada por la Unión Europea o por el Derecho de alguno de los Estados Miembros, o un convenio colectivo, siempre que se adopten medidas que respeten los derechos fundamentales y los intereses del interesado.

La normativa de aplicación sería el RDL 8/2019, de 8 de marzo, en cuyo artículo 10 regula la obligación del registro de la jornada como forma de combatir la precariedad laboral y establece la modificación del artículo 34 del estatuto de los Trabajadores, añadiendo un nuevo apartado 9 que dice:

"…La empresa garantizará el registro diario de jornada, que deberá incluir el horario concreto de inicio y finalización de la jornada de trabajo de cada persona trabajadora, sin perjuicio de la flexibilidad horaria que se establece en este artículo. Mediante negociación colectiva o acuerdo de empresa o, en su defecto, decisión del empresario previa consulta con los representantes legales de los trabajadores en la empresa, se organizará y documentará este registro de presencia. La empresa conservará los registros a que se refiere este precepto durante cuatro años y permanecerán a disposición de las personas trabajadoras, de sus representantes legales y de la Inspección de Trabajo y Seguridad Social.»

Para la AEPD esta obligación legal de implantar un registro de jornada laboral no legitima ni ampara el tratamiento de datos biométricos, toda vez que la norma no hace alusión a la utilización de datos biométricos para llevar el registro de jornada y tratándose de datos que pertenecen a categorías especiales de datos es necesario que se establezca en una norma legal.

En relación con el **control de acceso** con fines laborales es el artículo 20.3 del Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el Texto Refundido de la Ley del Estatuto de los Trabajadores, el que establece que:

"3. El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad y teniendo en cuenta, en su caso, la capacidad real de los trabajadores con discapacidad".

Pero como en el caso anterior tampoco en este artículo se habla de la utilización de datos biométricos para establecer el control de accesos.

Esta interpretación, igualmente se recoge en el Dictamen 1/2023 emitido por el Consejo de Transparencia y Protección de Datos relativo al tratamiento de datos biométricos mediante el uso de dispositivos de reconocimiento facial y/o huella dactilar para el control horario del personal de un Ayuntamiento, en el que señala que la legislación española no contiene autorización específica alguna para considerar necesario el tratamiento de datos biométricos con la finalidad de un control horario o control de acceso con fines laborales.

En base a esto, podemos concluir que las organizaciones deberán revisar los criterios en base a los cuales decidieron implantar este tipo de herramientas sobre la base de los siguientes puntos:

(i) Analizar los criterios de implementación con objeto de que pasen el juicio de idoneidad, necesidad y proporcionalidad de protección de datos.

(ii) Identificar que exista una circunstancia para levantar la prohibición de tratar las categorías especiales de datos y una condición que legitime el tratamiento, que no puede estar basada en el consentimiento.

(iii) Cualquier utilización de datos biométricos deberá tener su circunstancia propia de levantamiento de la prohibición del tratamiento.

(iv) Superado el Juicio de Protección de Datos, deben implementarse garantías organizativas, técnicas y jurídicas y realizar un análisis de riesgos.

Para más información, puede contactar con:

María Suárez
Socia | Privacidad y Propiedad Intelectual
maria.suarez@es.Andersen.com