Alicia Maddio e Isabel Iglesias

Más allá de la huella: Desentrañando la Guía de Control de Presencia con Sistemas Biométricos de la AEPD

Sobre la Guía "Tratamientos de control de presencia mediante sistemas biométricos"

En la era de la digitalización y la innovación tecnológica, los métodos de control de presencia están evolucionando rápidamente. Una de las tecnologías emergentes más debatidas en este contexto es el uso de sistemas biométricos. En este contexto, la Agencia Española de Protección de Datos ("**AEPD**") publicó el pasado 23 de noviembre la Guía "Tratamientos de control de presencia mediante sistemas biométricos", un documento que aborda detalladamente los criterios para el tratamiento de control de presencia –dentro y fuera del contexto laboral– mediante sistemas biométricos, así como su conformidad con el Reglamento General de Protección de Datos ("**RGPD**").

En la presente nota desglosaremos los aspectos más importantes de la guía, proporcionando un análisis conciso de sus contenidos, para así facilitar a las organizaciones y sus responsables la comprensión y aplicación de estas directrices en sus sistemas de control de presencia.

¿Qué son los sistemas y datos biométricos?

Los sistemas de procesamiento de datos biométricos se basan en la recogida y procesamiento de datos personales relacionados con las características físicas, fisiológicas o conductuales de las personas físicas, que hacen posible su identificación, seguimiento o perfilado ("**tratamiento**"[1]).

Un dato biométrico[2] es aquel dato personal obtenido a partir de un tratamiento técnico específico, y que estando referido a las características físicas, fisiológicas o conductuales de una persona física **permiten o confirman** su identificación única. Este tipo de datos encuentran encaje en el art. 9.1 del RGPD, que contiene una regla general que prohíbe el tratamiento de datos personas que revelen, entre otros, datos biométricos destinados a identificar a una persona física de forma unívoca.

¿Cómo ha cambiado la posición de la AEPD al respecto?

En 2021, la AEPD publicó la guía "La Protección de Datos en las Relaciones Laborales[3]", en la que se abordaba en el apartado "Los datos biométricos" el empleo de biometría en la implementación de los tratamientos de registro de presencia. **Dicha guía señalaba que la autenticación biométrica[4] se encontraba fuera de las categorías especiales de datos**.

Sin embargo, esta interpretación se ha visto modificada por las Directrices 05/2022 del Comité Europeo de Protección de Datos ("**CEPD**"), sobre el uso de reconocimiento facial en el ámbito de las fuerzas de orden público[5], por lo que la interpretación que ofrece la AEPD en la guía aquí analizada busca adaptarse a este

1. Art. 4.2 del RGPD
2. Art. 4.14 RGPD
3. Disponible en: https://www.aepd.es/documento/la-proteccion-de-datos-en-las-relaciones-laborales.pdf
4. En particular, la AEPD estableció que los datos biométricos únicamente tienen la consideración de categoría especial de datos en los supuestos en que se sometan a tratamiento técnico dirigido a la identificación biométrica (uno-a-varios) y no en el caso de verificación/autenticación biométrica (uno-a-uno).
5. Disponible en: https://edpb.europa.eu/system/files/2023-05/edpb_guidelines_202304_frtlawenforcement_v2_en.pdf

contexto, y por ello, considera que la autenticación biométrica es un proceso que implica el tratamiento de categorías especiales de datos personales.

¿Cuáles son los aspectos más relevantes de la guía publicada?

- Señala que **la actual legislación española no contiene autorización suficientemente específica que justifique la necesidad de procesar datos biométricos con el objetivo de realizar un control horario de la jornada laboral (inicio/fin de la jornada y control de acceso con fines laborales)**.
- **El consentimiento del interesado**, en el caso del tratamiento de registro de jornada con técnicas biométricas, **no levanta la prohibición del tratamiento**, con carácter general, al existir una situación de desequilibrio con el responsable del tratamiento –tal y como ocurre en el ámbito de una relación laboral, o administrativa/funcionarial–, y por ello, no superaría la evaluación de necesidad requerida para tratamientos de alto riesgo. No obstante, **cuando existan opciones realmente equivalentes y disponibles** para todos los trabajadores, **se podría estudiar** si el consentimiento fuese válido.
- En relación con el control de acceso con fines no laborales, será necesario **demostrar la necesidad objetiva del tratamiento, así como las posibles alternativas**, es decir, para poder tratar datos biométricos no debe existir otra alternativa que satisfaga la necesidad identificada.
- No será posible utilizar el proceso de identificación o autenticación biométrica en aquellos casos de control de presencia con **decisiones automatizadas**, que no permitan la intervención humana con facultades para revertir las decisiones tomadas.
- Con carácter previo a cualquier decisión de implantación de un sistema de control de presencia a través de sistemas biométricos, es necesario realizar una gestión del riesgo[6] desde el diseño y por defecto[7], que aplique las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el RGPD. Al tratarse de tratamientos que entrañan un alto riesgo, se deberá superar favorablemente una Evaluación de Impacto para la Protección de Datos ("**EIPD**[8]").
- En cuanto a los sistemas biométricos que se implementan utilizando técnicas de inteligencia artificial, es esencial considerar su clasificación como "de alto riesgo"[9].

¿Qué medidas *mínimas* deben aplicarse al tratamiento de control de presencia?

La AEPD lista una serie de **medidas mínimas por defecto**[10] extensibles al tratamiento de control de presencia, que se indican a continuación:

1. Informar a los sujetos de los datos sobre el tratamiento biométrico y sus riesgos.
2. Implementar en el sistema biométrico la posibilidad de revocar el vínculo de identidad entre la plantilla biométrica y la persona física.
3. Implementar medios técnicos para asegurarse la imposibilidad de utilizar las plantillas para cualquier otro propósito.

6. Art. 24.1 RGPD

7. Art. 25 RGPD

8. La EIPD debe incluir y superar el triple juicio de idoneidad, necesidad y proporcionalidad del art. 35.7.b RGPD, también previsto por la doctrina del Tribunal Constitucional.

9. Tal y como señala el Anexo III de la Propuesta de Reglamento por el que se establecen normas armonizadas en materia de inteligencia artificial . Actualmente, la Propuesta de Reglamento está siendo debatida por el Parlamento y el Consejo en presencia de la Comisión Europea, en los llamados diálogos tripartitos ("*trilogue*"), siguiendo así el procedimiento legislativo ordinario de la Unión Europea.

10. Ya establecidas por la AEPD, en la guía "La Protección de Datos en las Relaciones Laborales", apartado "Los datos biométricos", disponible en: https://www.aepd.es/documento/la-proteccion-de-datos-en-las-relaciones-laborales.pdf (fecha último acceso: 24/11/2023).

4. Utilizar cifrado para proteger la confidencialidad, disponibilidad e integridad de la plantilla biométrica.
5. Utilizar formatos de datos o tecnologías específicas que imposibiliten la interconexión de bases de datos biométricos y la divulgación de datos no comprobada.
6. Suprimir los datos biométricos cuando no se vinculen a la finalidad que motivó su tratamiento.
7. Implementar la protección de datos desde el diseño.
8. Realizar una EIPD.

CONTACTOS

Raúl Rubio
Socio de Propiedad Intelectual, Industrial y Tecnología
rrubio@perezllorca.com
T. +34 91 353 45 59

Andy Ramos
Socio de Propiedad Intelectual, Industrial y Tecnología
aramos@perezllorca.com
T. +34 91 423 20 72

Yolanda Valdeolivas
Of Counsel de Laboral, compensación y beneficios
yvaldeolivas@perezllorca.com
T. +34 91 389 01 80