

## El uso de datos biométricos para la protección de los menores

Los sistemas biométricos y el tratamiento de los datos que pueden obtenerse a partir de ellos están evolucionando muy rápidamente. Los nuevos sistemas aumentan el detalle de la información recogida e incluso permiten la posibilidad de recoger información sin la cooperación de la persona, que en ocasiones ni siquiera es consciente de ello. A ello se suma el desarrollo de la inteligencia artificial, que puede utilizarse para inferir información adicional sobre las personas.

En su reciente guía *Tratamientos de control de presencia mediante sistemas biométricos*, la Agencia Española de Protección de Datos (AEPD) fija los criterios para la **utilización de la biometría** para el control de acceso, tanto con fines laborales como no laborales, estableciendo las medidas que han de tenerse en cuenta para que un tratamiento de datos personales que utilice esa tecnología cumpla con el Reglamento General de Protección de Datos (RGPD), entre otras normativas.

La Agencia considera el tratamiento de datos biométricos, tanto para identificación como para autenticación, como un tratamiento de alto riesgo que incluye categorías especiales de datos. Tal y como establece el Reglamento General de Protección de Datos, para poder tratar esas categorías es necesario que exista una circunstancia que levante la prohibición de su tratamiento y, además, una condición que lo legitime.

De acuerdo con el apartado 1 del artículo 9 del Reglamento, referido al tratamiento de categorías especiales de datos personales, queda prohibido el tratamiento de datos biométricos dirigidos a identificar de manera unívoca a una persona física, si bien en el apartado 2 se recogen una serie de excepciones, cuando el tratamiento:

- Cuenta con el consentimiento explícito del interesado para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado.
- Sea 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;

- Sea necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento.
- Sea efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados;
- Se refiera a datos personales que el interesado ha hecho manifiestamente públicos.
- Sea necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial.
- Sea necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.
- Sea necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3 de este artículo.
- Sea necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional.
- Sea necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.

El apartado 4 señala que los Estados miembros podrán mantener o introducir condiciones adicionales, inclusive limitaciones, con respecto al tratamiento de esos datos biométricos.

La AEPD, por su parte, especifica que el consentimiento no es motivo suficiente para levantar la prohibición del tratamiento de estos datos o ser una base para determinar su licitud, al existir un desequilibrio entre la persona a la que se somete al tratamiento y quien lo está llevando a cabo.

En todo caso, la Guía precisa que, en caso de pretender captar datos biométricos, de forma previa al inicio del tratamiento, será obligatoria la realización de una Evaluación de Impacto para la Protección de Datos en la que, entre otros aspectos, se acredite la superación del triple análisis de idoneidad, necesidad y proporcionalidad del tratamiento (Véase el 35). Y añade un listado de medidas que deben llevarse a cabo si se superan todos los requisitos de cumplimiento de los principios del RGPD:

- Informar a las personas sobre el tratamiento biométrico y los riesgos elevados asociados al mismo.
- Implementar en el sistema biométrico la posibilidad de revocar el vínculo de identidad entre la plantilla biométrica y la persona física.
- Implementar medios técnicos para asegurarse la imposibilidad de utilizar las plantillas para cualquier otro propósito.
- Utilizar cifrado para proteger la confidencialidad, disponibilidad e integridad de la plantilla biométrica.
- Utilizar formatos de datos o tecnologías específicas que imposibiliten la interconexión de bases de datos biométricos y la divulgación de datos no comprobada.
- Suprimir los datos biométricos cuando no se vinculen a la finalidad que motivó su tratamiento.
- Implementar la protección de datos desde el diseño.

- Aplicar la minimización de los datos recogidos, con una evaluación objetiva de que no hay tratamiento de categorías especiales de datos.

*Para saber más:*

<https://www.aepd.es/documento/guia-control-presencia-biometrico-nov-2023.pdf>

<https://www.aepd.es/documento/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf>