CIRCULAR INFORMATIVA Nº 16/2026

07/09/2026

Emisión de un borrador de "Guía sobre tratamientos en el control de acceso mediante sistemas biométricos", elaborado por la Agencia Española de Protección de Datos y remitido a CEOE con plazo para formular alegaciones sobre su contenido

Estimado amigo:

Desde CEOE se ha remitido a nuestra Federación un BORRADOR de **"Guía sobre tratamiento en el control de acceso mediante datos biométricos"**, elaborado por la Agencia Española de Protección de Datos (AEPD), en el que se concede la posibilidad de realizar alegaciones respecto de su contenido.

Sin ánimo de hacer un estudio exhaustivo de este documento, a continuación se tratan de resumir algunos de los aspectos más destacados o significativos del mismo:

ANTECEDENTES:

En el mes de noviembre del año 2023, la AEPD publicó en su web una Guía en la que fijaba unos criterios de actuación muy restrictivos en relación con el uso de la biometría, atribuyendo a tales criterios lo que podría considerarse como una cierta obligatoriedad de cumplimiento por parte de las empresas y particulares.

Esta guía fue objeto de muchas críticas, al considerar que excedía su función meramente orientativa, constituyéndose en la práctica como una especie de normativa de obligada aplicación elaborada sin seguir el procedimiento establecido para la aprobación de este tipo de normas. Recurrida por la Asociación Española de Empresas de Seguridad, esta guía fue anulada por la Audiencia Nacional mediante Sentencia número 367/2026, dictada el pasado día 30 de junio de 2026.

Como consecuencia de ello, la AEPD ha preparado este nuevo borrador en el que se deja claro su *"carácter informativo, orientador y de apoyo al cumplimiento"*, así como que esta guía *"no constituye una circular ni una disposición de carácter general, no introduce obligaciones nuevas ni modifica el contenido de las previstas en el RGPD, en la LOPDGDD o en otras normas aplicables"*. No obstante ello, no puede obviarse la relevancia que tiene la elaboración de una guía de esta naturaleza en la medida que la misma recogerá la interpretación de esta AEPD sobre este importante asunto del uso de la biometría en los controles de acceso.

ASPECTOS MÁS RELEVANTES DE LA GUÍA:

▶ APARTADO 2 – DEFINICIONES:

El objetivo principal de este apartado es definir la terminología técnica y operativa de los sistemas biométricos para determinar cómo se clasifica la información procesada y qué propiedades de seguridad debe cumplir. Establece el **marco conceptual** necesario para entender cómo deben tratarse los datos biométricos en sistemas de control de acceso. Se divide en cinco bloques: datos biométricos, tipos de identificadores, características de seguridad, registro y almacenamiento, e identificación/autenticación.

■ **Datos biométricos:** Son datos obtenidos mediante técnicas que permiten identificar a una persona (rostro, huella, voz…). Los sistemas biométricos captan estas características y generan datos para identificar o autenticar.

■ **Identificadores:**

- Referencias biométricas: huellas, fotos, plantillas o modelos que permiten identificar a alguien.
- Referencias de identidad: identificadores no biométricos (DNI, código de empleado).
Ambos pueden vincularse a permisos o autorizaciones.

■ **Propiedades o características de seguridad:**

Las referencias biométricas deben ser:
- Irreversibles (no reconstruyen la imagen original).
- No vinculables (no permiten relacionar usos distintos).
- Revocables/renovables (pueden invalidarse y sustituirse).

■ **Registro y almacenamiento:**

En el alta se confirma la identidad y se captan los datos biométricos. Las referencias pueden guardarse:
- En la **base de datos del responsable**,
- En un **dispositivo del individuo**,
- **distribuidas/cifradas** entre ambos.

■ **Diferencia entre Identificación y autenticación:**

- Autenticación (1:1): la persona declara quién es y se compara su biometría con la registrada.
- Identificación (1:N): la persona no declara identidad; el sistema compara su biometría con toda la base de datos.

▶ APARTADO 3 – ANÁLISIS LEGAL:

■ **Principio de proporcionalidad:**

El uso de biometría en control de acceso debe superar tres pruebas:
- Idoneidad: el sistema debe ser capaz de cumplir eficazmente la finalidad (control de acceso) y demostrarse con métricas objetivas.
- Necesidad: no debe existir otra alternativa menos intrusiva que logre la misma eficacia.
- Proporcionalidad: el beneficio debe superar la injerencia en los derechos; si el riesgo es alto y hay alternativas menos invasivas y con mayor riesgo, el tratamiento es desproporcionado.

■ **Categorías especiales de datos:**

Los datos biométricos usados para identificar o autenticar son **categoría especial** (art. 9 RGPD). Su tratamiento está **prohibido**, salvo que concurra una excepción del art. 9.2:
- **consentimiento explícito** que debe ser libre, específico, informado e inequívoco y prestado con todas las garantías;
- norma con rango legal que lo autorice, en la que debe declarar la finalidad de ese tratamiento y debe ser proporcionada con el objetivo perseguido.

La guía aclara que la intensidad de garantías depende del contexto: no es igual una identificación masiva sin conocimiento del afectado que una autenticación puntual y consentida.

■ **Licitud del tratamiento:**

Además de levantar la prohibición del art. 9, debe existir una **base jurídica del art. 6 RGPD** adecuada y suficientemente precisa según el riesgo del tratamiento.

■ **Decisiones automatizadas:**

Si el sistema biométrico toma decisiones automatizadas que afectan significativamente a la persona (p. ej., permitir o denegar acceso), deben cumplirse las obligaciones del art. 22 RGPD

▶ APARTADO 4 – GESTIÓN DEL RIESGO:

■ **Evaluación de impacto (EIPD):**

El uso de biometría en control de acceso **normalmente exige una EIPD**, porque implica categoría especial de datos y riesgos elevados. Debe analizarse la finalidad, necesidad, proporcionalidad y las medidas de mitigación.

■ **Alto riesgo:**

El tratamiento puede ser de **alto riesgo** cuando:
- Se usan bases de datos biométricas centralizadas.
- Hay identificación (1:N) en lugar de autenticación (1:1).
- El interesado pierde control sobre sus datos.
- Se emplea IA que pueda inferir información sensible.

Si el riesgo residual es alto, el tratamiento **no debe realizarse**.

■ **Superación del análisis de idoneidad, necesidad y proporcionalidad:**

Solo puede implantarse biometría si se demuestra objetivamente que:
- Es **idónea** para la finalidad.
- Es **necesaria** (no hay alternativa igual de eficaz y menos intrusiva).
- Es **proporcionada** (el beneficio supera la injerencia).

■ **Implementación y contexto:**

El riesgo depende del contexto: escala, tecnología, ubicación de los datos, control del interesado, frecuencia del tratamiento, posibilidad de captura accidental de terceros, etc.

■ **Garantías y medidas:**

Se exigen medidas **organizativas** (políticas internas, formación, control de accesos, minimización) y **técnicas** (cifrado, irreversibilidad, no vinculación, almacenamiento distribuido, seguridad del dispositivo del usuario).

■ **Brechas de datos personales:**

Las brechas con datos biométricos son especialmente graves porque los datos **no pueden cambiarse**. Deben notificarse conforme al RGPD y aplicarse medidas para evitar reutilización o suplantación.

▶ APARTADO 5 – ACCESO AL ENTORNO LABORAL. REGISTRO DE JORNADA:

■ **Excepción del artículo 9.2.b RGPD (norma legal):**

El uso de biometría para **control horario o acceso laboral** solo puede hacerse si existe una **ley** que lo autorice y cumpla los requisitos del art. 9.2.b RGPD. La guía aclara que **no basta** con obligaciones laborales generales: debe existir una **norma de rango legal** que permita específicamente tratar datos biométricos para esa finalidad.

■ **Licitud del tratamiento:**

Además de levantar la prohibición del art. 9, el responsable debe contar con una **base jurídica del art. 6 RGPD** adecuada (normalmente obligación legal o interés público). El tratamiento debe superar proporcionalidad, necesidad y minimización: si existen alternativas igual de eficaces y menos intrusivas, **no puede usarse biometría**.

■ **Subcontratación de trabajadores:**

Cuando hay trabajadores subcontratados o externos, el responsable debe garantizar que:
- El tratamiento biométrico se aplica solo cuando sea **estrictamente necesario**.
- Se respetan las obligaciones de información, garantías y medidas de seguridad.
- Se definen claramente las responsabilidades entre empresa principal y contratas.

▶ APARTADO 6 – CONCLUSIONES:

El apartado 6 sintetiza todo lo anterior y establece las siguientes ideas clave:

- La biometría es un tratamiento de alto impacto y solo puede usarse en control de acceso cuando se demuestre que es **idónea, necesaria y proporcionada**, y que no existe una alternativa menos intrusiva con igual eficacia.

- El tratamiento de datos biométricos para identificar o autenticar es **categoría especial**, por lo que **requiere una excepción del art. 9 RGPD** (consentimiento explícito o norma legal adecuada) **más una base jurídica del art. 6 RGPD**.

- La decisión de implantar biometría exige una **evaluación rigurosa del riesgo**, una **EIPD**, y la aplicación de **garantías técnicas y organizativas** que reduzcan el riesgo residual a un nivel aceptable; si esto no es posible, **el tratamiento no debe realizarse**.

- Registro de Jornada Laboral: Salvo habilitación específica por convenio colectivo con garantías del Art. 91 LOPDGDD, no se recomienda el control horario biométrico basándose en la obligación legal del Estatuto de los Trabajadores. Se aconseja utilizar métodos alternativos no biométricos (tarjetas RFID, códigos, etc.) o garantizar opciones alternativas neutras bajo consentimiento auténtico.

Sobre estas líneas generales se tendrá que realizar un estudio más pormenorizado sobre el impacto que las indicaciones y conclusiones de esta guía pueda tener de manera específica en nuestro sector y, especialmente, en el control de acceso a determinados establecimientos de juego de algunas Comunidades Autónomas que contemplan (permiten, exigen o autorizan) que estos controles se realicen utilizando datos biométricos.

En todo caso, el contenido de esta guía viene a reafirmar la importancia que tiene el que exista una **norma legal** que declare de interés público el uso de la biometría en los controles de acceso de los establecimientos de juego, así como que concurra un **consentimiento explícito** (libre, específico, informado e inequívoco y prestado con todas las garantías) por parte de los clientes.

En el caso de que se considere oportuno que desde FEMARA se formule algún tipo de alegación sobre el contenido de este borrador de guía, se tendrían que hacer llegar a la Federación los puntos sobre los que se quiera que se formulen alegaciones. Sin perjuicio de ello, al ser un tema que afecta más directamente a las empresas titulares de establecimientos de juego, se mantendrá contacto con ANESAR para analizar posibles alegaciones que se pudieran resultar conveniente formular o apoyar por parte de FEMARA.

Se adjuntan como **ANEXOS de esta circular** tanto el contenido íntegro del borrador de guía analizado, como un cuadro resumen elaborado por CEOE respecto de dicho borrador.

Esperando que este asunto resulte de tu interés, aprovecho para hacerte llegar un cordial saludo,

Fdo. Jesús Mª Molina del Villar
Secretario General Técnico