ECIJA

NOTA INFORMATIVA

Nuevo informe jurídico de la AEPD sobre el uso de biometría para el control de accesos

El pasado 18 de julio, la Agencia Española de Protección de Datos ("AEPD") emitió un informe jurídico (Ref. REGAGE25e00024730156) en respuesta a una consulta previa relativa al artículo 36 del Reglamento General de Protección de Datos ("RGPD"), que afecta a un tratamiento de datos personales que tiene por finalidad el control de accesos a las instalaciones de la Guardia Civil. Este nuevo informe podría suponer un punto de inflexión en el criterio mantenido hasta ahora por la AEPD, al admitir, en este caso, el uso de datos biométricos para dicha finalidad.

Lo que necesitas saber

- Hasta ahora, la AEPD consideraba el uso de biometría para el control de accesos como un tratamiento altamente intrusivo, difícil de justificar frente a métodos alternativos como tarjetas de acceso.

- Sin embargo, este nuevo informe jurídico de la AEPD marca un punto de inflexión: por primera vez, admite que, cumpliendo ciertos requisitos, el uso de estos sistemas puede ser conforme a la normativa de protección de datos, especialmente en determinados contextos y siempre que se apliquen garantías técnicas y organizativas sólidas.

- Lo más destacado:

  Este informe marca un giro relevante en el enfoque de la AEPD y ofrece algunas directrices para los responsables del tratamiento que quieran implementar biometría con garantías.

  Admite el consentimiento como base de legitimación para el control de accesos por medio de autenticación biométrica.

  Reitera la distinción entre identificación y autenticación, manteniendo que esta última resulta menos intrusiva.

  Propone medidas técnicas y organizativas para reducir el impacto sobre los derechos y libertades de los afectados, lo que sirve de refuerzo para la legitimidad del tratamiento.

¿Control de acceso biométrico? La AEPD asume que es viable.

Hasta la fecha, la AEPD se había mostrado reticente a aceptar el uso de biometría para el control de accesos, bajo la premisa de que al existir métodos menos intrusivos esta modalidad no superaba el triple test de idoneidad, necesidad y proporcionalidad. El mensaje era claro: **Biometría para el control de accesos: tratamiento altamente intrusivo + existencia de medios menos intrusivos = posible infracción.**

Sin embargo, el pasado 18 de julio de 2025, la AEPD publicó un informe jurídico relativo a un sistema de control de accesos a instalaciones de la Guardia Civil basado en autenticación biométrica, con el que, **además de una clara llamada al legislador, arroja luz sobre posibles contextos en los que el uso de esta tecnología puede estar justificada. Haciendo referencia expresa a medidas técnicas y organizativas cuya adopción contribuye de forma significativa a minimizar el impacto sobre los derechos y libertades de las personas afectadas, reduciendo, por tanto, el grado de intrusismo asociado al tratamiento.**

Si bien no podemos olvidar que este informe se refiere a un supuesto concreto y con un contexto normativo específico, tampoco podemos obviar el giro relevante en el enfoque de la AEPD, ya que abre la puerta a que, en determinados contextos y bajo condiciones concretas, la autenticación biométrica pueda considerarse una opción adecuada para el control de accesos.

I. ¿Consentimiento como base de legitimación válida?

Si bien en este supuesto el tratamiento de datos biométricos encuentra un apoyo normativo variado sobre la conveniencia de la adopción de medidas de seguridad suficientes, como por ejemplo la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, aplicable a este supuesto, así como la Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a la resiliencia de las entidades críticas y por la que se deroga la Directiva 2008/114/CE del Consejo, que se encuentra actualmente en transposición al ordenamiento a través de anteproyecto de Ley, **lo realmente llamativo es el giro que da la AEPD al contemplar, por primera vez con claridad, el consentimiento como base de legitimación válida para este tipo de tratamientos**. Este reconocimiento no es menor, pues hasta ahora se ponía en duda la suficiencia del consentimiento para levantar la prohibición al ser un tratamiento de alto riesgo que no superaba el requisito de necesidad.

Aunque ello no suponga un cambio de criterio generalizado, esta nueva interpretación podría tener implicaciones prácticas muy relevantes al abrir la puerta al uso de sistemas biométricos para el control de acceso en entornos no regulados, siempre que se cumplan con las garantías y medidas necesarias y se supere el test de proporcionalidad.

II. Determinación del contexto y cómo mitigar los riesgos asociados

Es igualmente relevante el hecho de que, en este informe, la AEPD reconoce reiteradamente que el control de accesos por medio de biometría es más eficaz que el uso de tarjetas, contraseñas o registros manuales, ya que permite verificar con mayor fiabilidad quién accede a los espacios protegidos, evitándose suplantaciones de identidad y permitiendo restringir accesos no autorizados.

En cualquier caso, todo responsable del tratamiento que deseé implementar este tipo de sistemas debe llevar a cabo una evaluación de impacto, así como analizar en detalle la idoneidad, necesidad y proporcionalidad del tratamiento.

Por ello, la AEPD establece que es preciso determinar en qué perímetro y qué tipo de sistema se va a implementar, puesto que no es equiparable la implementación de un sistema biométrico para el control de acceso a instalaciones de entidades críticas, que utilizarlo en entornos de menor sensibilidad, ya que el nivel de riesgo y las garantías exigibles varían significativamente.

Además del contexto en el que se implementa, el tipo de sistema utilizado también influye en el nivel del riesgo. La AEPD deja claro que la autenticación o verificación unívoca (1:1), que responde a la pregunta, ¿eres quién dices ser? presenta menos riesgos que la identificación (1:N), que responde a la pregunta ¿quién eres tú entre todos los posibles?, en tanto que la primera opción presenta un menor impacto sobre los derechos de los interesados, al implicar un tratamiento más limitado.

Así, las autoridades y tribunales europeos han sostenido que la implementación de este tipo de medidas debe limitarse a lo estrictamente necesario. Es decir, sólo deben aplicarse cuando los objetivos no puedan alcanzarse razonablemente con la misma eficacia mediante alternativas menos intrusivas.

En consecuencia, cuando existan varias opciones técnicamente eficaces, el responsable debe optar por la que resulte más adecuada al fin perseguido, siempre que respete el principio de proporcionalidad y reduzca al mínimo el impacto sobre los derechos y libertades de los afectados.

La pregunta que inevitablemente se plantea es: **¿cómo puede reducirse el impacto de estos tratamientos sobre los derechos de las personas?** En este sentido, la AEPD admite que, en el supuesto analizado, la adopción de medidas técnicas y organizativas adecuadas contribuye de manera significativa a mitigar el impacto y a reforzar las garantías en materia de protección de datos.

III. Deberes para el legislador y hoja de ruta para los responsables del tratamiento

Por medio del informe, la AEPD requiere también un papel activo al legislador, proponiendo la elaboración de una regulación específica que incorpore garantías adecuadas en el uso de tecnologías biométricas en el marco de la cuestión planteada, así como en distintos modelos normativos ya en desarrollo que contemplan la instalación de sistemas de reconocimiento biométrico, proponiendo un conjunto de recomendaciones concretas que podrían ser incorporadas en una futura regulación.

No obstante, las orientaciones dadas por la AEPD al legislador pueden ser tomadas como una hoja de ruta que permita a los responsables del tratamiento considerar las medidas técnicas y organizativas propuestas previo a la implementación de estos sistemas. Se destacan las siguientes:

- **Recabado asistido de datos:** los datos biométricos deben ser recabados con la intervención de personal cualificado.
- **Deber de información**: los interesados deben ser informados de forma clara y completa sobre el tratamiento, las alternativas disponibles y los riesgos del tratamiento.
- **Control exclusivo por el interesado:** los datos deben mantenerse bajo el control exclusivo del titular.

- Protección frente a terceros.
- **Prohibición de almacenamiento centralizado:** los identificadores biométricos no deben almacenarse en repositorios centralizados.
- **Generación local y en entornos aislados:** los datos deben generarse en sistemas locales, sin conexión a redes.
- **No interoperabilidad:** el sistema no debe ser interoperable con otros sistemas o bases de datos.
- **Identificadores renovables y con caducidad:** se deben usar identificadores que puedan regenerarse y que tengan una validez limitada.
- **Procedimientos de destrucción:** debe existir un protocolo definido la destrucción segura de los datos.
- **Conservación limitada de datos asociados:** los datos personales no biométricos vinculados al sistema se conservarán durante un máximo de 30 días antes de ser bloqueados.
- **Principio de minimización:** el sistema no debe de almacenar información más allá de los estrictamente necesario para cada autenticación.
- **Prohibición de transmisión:** no se habilitarán las transferencias de datos fuera del sistema.
- **Infraestructura controlada:** los dispositivos biométricos deben instalarse en ubicaciones físicamente seguras y controladas.
- **Evaluaciones de impacto:** las evaluaciones de impacto deben realizarse previo a la implementación del sistema y se deberán de actualizar cada cuatro años.
- **Cumplimento del ENS en nivel alto:** debe cumplirse con el nivel alto del Esquema Nacional de Seguridad, incluyendo auditorías periódicas.

Área de Protección de Datos de ECIJA

info@ecija.com

Telf: + 34 91.781.61.60