Sistemas biométricos para control de presencia y control de acceso (según nueva guía AEPD – v. noviembre 2023)

Documento elaborado por:
Toni Ripoll, Consultor INGECAL
Marina Rejat, Consultora INGECAL

Más información y contacto:
www.ingecal.cat
ingecal@ingecal.cat
(+34) 93 237 83 90

Fecha de redacción:
04 de enero del 2024

INGECAL

La AEPD, en su guía[i] no establece la prohibición del uso de tratamiento biométricos para el control de presencia o control de acceso, sino que determina los criterios que deben aplicarse en la evaluación para su uso y que, por su naturaleza restrictiva, llevan a la conclusión de que en la gran mayoría de casos su uso no es adecuado a los requisitos del RGPD.

Fundamentos

- El RGPD define datos biométricos[ii] 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*".

> Las plantillas utilizadas en los sistemas biométricos que permiten distinguir claramente los individuos actúan como identificadores únicos de una persona ya que los singularizan inequívocamente.

- El uso de datos biométricos para control de presencia o control de acceso es un tratamiento de datos de categoría especial, tanto si se trata de autenticación (verificación 1 a 1) o identificación (1 entre muchos)[iii]
- Tanto si el sistema se utiliza para control de presencia, como para control de acceso, la finalidad de estos tratamientos no es tratar datos biométricos, por lo que en base al principio de minimización de datos[iv], estos datos biométricos solamente se deberían tratar si estas finalidades no pudieran lograrse razonablemente por otros medios.
- Asimismo, se deberá respetar la obligación de protección de datos desde el diseño y por defecto[v] según la cual se deberán aplicar las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento.
- El tratamiento de datos biométricos se considera un tratamiento de alto riesgo, ya que concurren los criterios de tratarse datos de categoría especial, el uso de datos biométricos para la identificación de personas y la utilización de nuevas tecnologías[vi], por lo que será necesario llevar a cabo una evaluación de impacto relativa a la protección de datos[vii].

- EL RGPD establece la prohibición de tratamiento de datos de categorías especiales[viii]. Esta prohibición únicamente puede levantarse si se dan alguna de las excepciones[ix]:

  - Se dispone del consentimiento explícito del interesado (que por su definición debe ser libre[x]) para el tratamiento adicional de datos biométricos.

    En particular, en el contexto de las relaciones laborales, únicamente podría considerarse la existencia de un consentimiento libre[xi], si el interesado dispone de una alternativa de libre elección para cumplir con dicha obligación[xii].

    Sin embargo, si existen alternativas que permitan que todos los trabajadores opten por otras alternativas, el procesamiento de datos biométricos podría dejar de cumplir el criterio de ser necesario para la implementación del tratamiento.

  - Es necesaria para el cumplimiento de una norma de rango legal en el ámbito del derecho laboral, en este caso, que establezca garantías adecuadas del respeto de los derechos fundamentales[xiii].

    Se ha tratado de justificar la licitud del tratamiento haciendo referencia a la obligación del registro de jornada establecida en el Real Decreto-ley 8/2019, de 8 de marzo, de medidas urgentes de protección social y de lucha contra la precariedad laboral en la jornada de trabajo, pero cabe remarcar que este solamente establece la necesidad de garantizar el registro de jornada, pero no a realizarla utilizando datos biométricos.

    Es decir, el Real Decreto-ley 8/2019 legitima el registro de jornada, no el sistema de reconocimiento.

- Igualmente se tiene que justificar la licitud del tratamiento de acuerdo con las condiciones (causas) establecidas en el artículo 6.1 del RGPD, tanto si se trata de un sistema para control de presencia, como si se utiliza para control de acceso.

  La condición de que el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al tratamiento, o la de que el interesado ha dado su consentimiento no son viables según lo explicado hasta el momento.

- Igualmente, para el resto de las condiciones del artículo 6.1 se deberá evidenciar el cumplimiento del requisito de necesidad, idoneidad y proporcionalidad.

- El criterio de necesidad implica[xiv]:

  a. El sistema deber ser esencial para satisfacer la necesidad, por lo que no basta la mera conveniencia o rentabilidad (ahorro de costes)[xv].

  b. En cuanto al uso para el control de acceso, el tratamiento de datos biométricos solo puede justificarse como un instrumento necesario para asegurar los bienes o las personas cuando se disponga de pruebas, sobre la base de las circunstancias objetivas y documentadas, de la existencia de un riesgo considerable[xvi].

- El criterio de idoneidad implica que debe existir un vínculo lógico y directo entre el tratamiento y el objetivo perseguido, además de determinar objetivamente la efectividad real del tratamiento para resolver la necesidad planteada.

- La evaluación de la proporcionalidad en sentido estricto implica que es una medida ponderada y que mantiene el equilibrio con otros derechos fundamentales, derivándose más beneficios o ventajas que perjuicios sobre otros valores en conflicto.

  Se debe ponderar si el grado de intrusismo y los riesgos de posible pérdida de intimidad derivada del tratamiento de datos biométricos justifican los beneficios en cuanto a comodidad o ahorro económico.

La superación de estos criterios de necesidad, idoneidad y proporcionalidad se deberá documentar en una EIPD.

Conclusiones

- Si estas evaluando implementar un sistema para el control de presencia o control de acceso, desaconsejamos el uso de mecanismos biométricos.
- En el caso de que ya esté implementado el sistema para control de acceso o de presencia:
    - Optar por otras alternativas que no impliquen el tratamiento de datos biométricos.
    - En casos puntuales en que la organización considere necesario el uso de sistemas biométricos, será necesario realizar y superar una EIPD.

---

[i] Guía sobre tratamientos de control de presencia mediante sistemas biométricos

[ii] RGPD Artículo 4.14

[iii] Directrices 05/2022 del CEPD/EDPB, Punto 12: *"While both functions – authentication and identification – are distinct, they both relate to the processing of biometric data related to an identified or identifiable natural person and therefore constitute a processing of personal data, and more specifically a processing of special categories of personal data."*

[iv] RGPD Articulo 5.1.c: "*Los datos personales serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»)".*

RGPD Considerando 39: *"… Los datos personales deben ser adecuados, pertinentes y limitados a lo necesario para los fines para los que sean tratados. …. Los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios."*

[v] RGPD Artículo 25.2

[vi] AEPD. Lista de tipos de Tratamientos de Datos que requieren Evaluación de Impacto relativa a Protección de Datos

[vii] RGPD Artículo 35

[viii] RGPD Artículo 9.1: *"Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física."*

[ix] RGPD Artículo 9.2

[x] RGPD Considerando 32: *"El consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen"*

[xi] Directrices 5/2020 del CEDB/EDPB, Punto 37: El responsable del tratamiento podría argumentar que su organización ofrece a los interesados una elección real si estos pudieran escoger entre un servicio que incluya el consentimiento para el uso de datos personales con fines adicionales, y un servicio equivalente ofrecido por el mismo responsable que no implicara prestar el consentimiento para el uso de datos con fines adicionales. … No obstante, ambos servicios deben ser realmente equivalentes

[xii] Directrices 5/2020 del CEDB/EDPB, Punto 37: El responsable del tratamiento podría argumentar que su organización ofrece a los interesados una elección real si estos pudieran escoger entre un servicio que incluya el consentimiento para el uso de datos personales con fines adicionales, y un servicio equivalente ofrecido por el mismo responsable que no implicara prestar el consentimiento para el uso de datos con fines adicionales. … No obstante, ambos servicios deben ser realmente equivalentes

[xiii] RGPD Artículo 9.1.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*"

[xiv] Directrices 05/2022 del CEPD/EDPB, punto 73: "*Processing can only be regarded as "strictly necessary" if the interference to the protection of personal data and its restrictions is limited to what is absolutely necessary. The addition of the term "strictly" means that the legislator intended the processing of special categories of data to only take place under conditions even stricter than the conditions for necessity. This requirement should be interpreted as being indispensable. It restricts the margin of appreciation permitted to the law enforcement authority in the necessity test to an absolute minimum. In accordance with the settled case-law of the CJEU, the condition of "strict necessity" is also closely linked to the requirement of objective criteria in order to define the circumstances and conditions under which processing can be undertaken, thus excluding any processing of a general or systematic nature."*

[xv] Dictamen 3/2012 del Grupo de Trabajo del Artículo 29: *"Al analizar la proporcionalidad de un sistema biométrico propuesto, es preciso considerar previamente si el sistema es necesario para responder a la necesidad identificada, es decir, si es esencial para satisfacer esa necesidad, y no solo el más adecuado o rentable."*

[xvi] Dictamen 3/2012 del Grupo de Trabajo del Artículo 29: "Como *norma general, el uso de la biometría para las exigencias generales de seguridad de los bienes y las personas no puede considerarse un interés legítimo que prevalezca sobre los intereses o los derechos y libertades fundamentales del interesado. Por el contrario, el tratamiento de datos biométricos solo puede justificarse como un instrumento necesario para asegurar los bienes o las personas cuando se disponga de pruebas, sobre la base de las circunstancias objetivas y documentadas, de la existencia de un riesgo considerable. Para ello, el responsable del tratamiento deberá probar que determinadas circunstancias plantean un riesgo considerable específico, que deberá evaluar con especial cuidado."*