Regulación Digital

El nuevo criterio de la Agencia sobre el tratamiento de control de presencia mediante sistemas biométricos

Diciembre 2023

Analizamos la nueva guía sobre el tratamiento de control de presencia mediante sistemas biométricos publicada por la Agencia Española de Protección de Datos

¿Hablamos?

Assumpta Zorraquino
Socia responsable de Regulación Digital en el departamento de New Law de PwC Tax & Legal
assumpta.zorraquino@pwc.com

Alejandra Matas Brancós
Directora en el área de Regulación Digital de PwC Tax & Legal
alejandra.matas.brancos@pwc.com

Samanta Murillo Geiser
Abogada en el área de Regulación Digital en el departamento de New Law de PwC Tax & Legal
samanta.murillo.geiser@pwc.com

El pasado 23 de noviembre, la Agencia Española de Protección de Datos ("AEPD") publicó una guía sobre el tratamiento de control de presencia mediante sistemas biométricos estableciendo los criterios para la utilización de la biometría en el registro de la jornada laboral o el control de acceso con fines laborales y no laborales.

El criterio de la AEPD **generará un impacto significativo** en las empresas que hayan optado por implementar sistemas biométricos para supervisar la presencia de sus empleados. Justificar el tratamiento de datos biométricos para este propósito se vuelve considerablemente **más complejo**, convirtiéndose en una tarea prácticamente imposible dentro del actual marco jurídico español.

1. Antecedentes en el uso de sistemas biométricos para el control de presencia

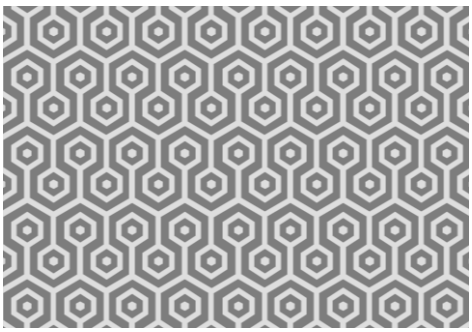
Hasta la publicación de esta Guía, el criterio adoptado por la AEPD era el de considerar que los sistemas de control se restringían a "verificar/autenticar" los rasgos de una persona ya identificada con anterioridad y que, por lo tanto, no se producía un tratamiento de datos biométricos (categoría especial).

Esta interpretación contribuyó significativamente a la expansión del uso de sistemas biométricos para el control de presencia de los empleados. (Informe del Gabinete Jurídico n/ref: 0036/2020).

Desde la óptica jurisprudencial, el Tribunal Supremo en Sentencia de 2 de julio de 2007 (rec. 5017/2003) reconoció que el control de la jornada mediante la lectura biométrica de la mano no se consideraba un exceso, ya que "*no hay norma que prohíba el recurso a la tecnología escogida para realizar el control del cumplimiento del horario de trabajo. Su novedad o complejidad no la convierten en lesiva* de los derechos fundamentales invocado".

No obstante, el pasado 26 de abril de 2023, el European Data Protection Board ("EDPB") actualizó las Directrices 05/2022 publicadas en mayo 2022 sobre el uso del reconocimiento facial para determinar que, tanto la autenticación, como la identificación, están relacionadas con el tratamiento de datos biométricos asociados a una persona física identificada o identificable y, por consiguiente, estamos ante datos de categorías especiales.

(...) en la actual normativa legal española no se contiene autorización suficientemente específica alguna para considerar necesario el tratamiento de datos biométricos con la finalidad de un control horario de la jornada de trabajo.



Frente al criterio del EDPB, la AEPD se ha visto obligada a reconsiderar su enfoque para alinearlo con el sostenido por este organismo, pero no se ha limitado a alinearse con el referido criterio, sino que lleva a cabo un ejercicio adicional, pronunciándose sobre cuestiones no evaluadas por el EDPB, y emitiendo conclusiones adicionales.

2. Análisis efectuado por la AEPD

En primer lugar, la AEPD, tras asumir que los datos biométricos son datos de categoría especial, **centra el debate en la posibilidad de levantar la prohibición** de su tratamiento, al amparo del art. 9.2 del RGPD, letras b) y a): excepción del cumplimiento de obligaciones legales y excepción del consentimiento explícito, respectivamente.

2.1. Excepción del cumplimiento de obligaciones legales:

El artículo 9 del RGPD, apartado 2, letra b) levanta la prohibición del tratamiento de categorías especiales cuando *"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".*

Y al respecto, para levantar la prohibición, la AEPD analiza dos cuestiones: la previsión legal y la necesidad del tratamiento.

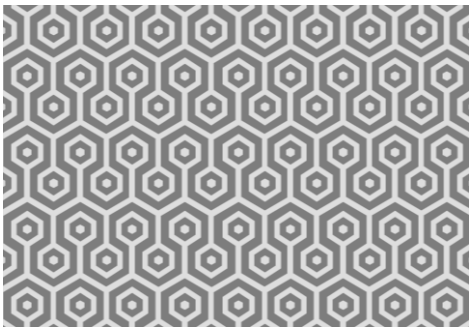
En cuanto a la **previsión legal,** la Agencia señala que la normativa legal actual en España no incluye una autorización lo suficientemente específica que justifique la necesidad de tratar datos biométricos con el propósito de llevar a cabo un control horario de la jornada laboral. Esta autorización específica no está presente para el personal laboral, ni para el personal sujeto a una relación administrativa, ya que ni el Estatuto de los Trabajadores ni el Estatuto Básico del Empleado Público la contemplan.

No obstante, la habilitación legal del artículo 9.2.b) del RGPD establece una alternativa, a la que ya hacía mención el Dictamen 2/2022 de la Autoridad Catalana de Protección de Datos y, citado por la propia Agencia en su guía: ***la previsión de dicha habilitación en el ámbito de un convenio colectivo,*** *siempre que establezca las garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado.*

En este sentido, indica la Autoridad Catalana de Protección de Datos que *"a falta de previsión legal, cabe recordar que, de acuerdo con lo que prevé el artículo 9.2.b) del RGPD, la autorización puede estar prevista en el marco de un convenio colectivo. Previsión a entender también aplicable a los acuerdos sobre condiciones de trabajo del personal funcionario en el marco de la negociación colectiva.*

Por ello, en caso de que el convenio colectivo, el pacto o acuerdo resultante de la negociación prevea la utilización de datos biométricos a tal fin y establezca garantías adecuadas respecto a los derechos fundamentales y de los intereses de las personas interesadas, este instrumento permitiría concluir la concurrencia de la excepción prevista en el artículo 9.2.b) del RGPD" (Dictamen 2/2022).

Siguiendo con el análisis del artículo 9.2 b), la AEPD hace una interpretación, a nuestro criterio excesivamente amplia, del ejercicio que debe llevarse a cabo antes de implementar cualquier sistema, en cuanto a **la necesidad de dicho tratamiento para la consecución de la finalidad pretendida**, en el sentido de que no haya otro medio igual de eficaz y menos intrusivo. Ejercicio que recae en el responsable del tratamiento, que tiene la obligación de **justificar por qué ya no es factible utilizar los sistemas de registro de presencia que se empleaban hasta ese momento**. Además, debe fundamentar por qué el uso de otros sistemas existentes, como tarjetas, certificados, claves, sistemas *contact-less*, etc., que evitan el tratamiento de categorías especiales de datos, no resulta adecuado.



En definitiva, cuestiona la necesidad de la implantación del tratamiento de datos biométricos, al existir otros medios alternativos que, en ocasiones complementándose con intervención humana, puedan razonablemente lograr la finalidad pretendida, evitando que el responsable se ampare únicamente en tendencias tecnológicas.

Frente a este razonamiento, no son pocas las voces que manifiestan estar ante un retroceso tecnológico.

2.2. Excepción del consentimiento explícito:

En este supuesto para levantar la prohibición, la AEPD, además de analizar el consentimiento en el entorno laboral, vuelve a hacer hincapié en el concepto necesidad con una interpretación restrictiva de su acepción.

Así, por un lado, el artículo 9 del RGPD, apartado 2, letra a) levanta la prohibición del tratamiento de categorías especiales cuando *"**el interesado dio su consentimiento explícito** 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*".

El artículo 4.11 del RGPD se refiere al consentimiento del interesado como "toda manifestación de voluntad libre especifica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen".

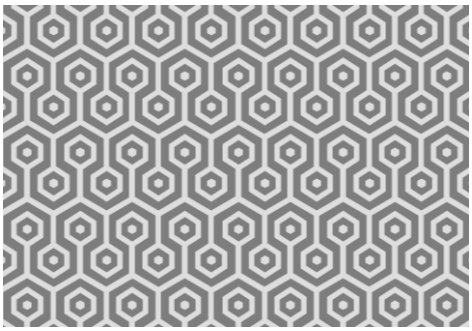
De acuerdo con las Directrices 5/2020 sobre el consentimiento en el contexto del RGPD del EDPB, en general, en las relaciones laborales existe **un desequilibrio de poder entre el empleado y el empleador,** lo que impide que el consentimiento se otorgue de manera libre y, por lo tanto, no resulta ser una base jurídica idónea. Sin embargo, el propio EDPB deja abierta la posibilidad de que los empleadores utilicen el consentimiento como base jurídica para el tratamiento de datos de sus empleados, siempre y cuando puedan demostrar que dicho consentimiento se ha otorgado de manera libre. Así las cosas, según el EDPB, los **empleados solo pueden otorgar su consentimiento libre en circunstancias excepcionales, donde la decisión de dar o no ese consentimiento no conlleve consecuencias adversas.**

La Agencia asume tal criterio, al afirmar que, en situaciones donde haya opciones realmente equivalentes y disponibles para todos los trabajadores, **se podría analizar la validez del consentimiento**, siempre y cuando se cumplan los requisitos establecidos en el artículo 4.11 del RGPD y las demás condiciones requeridas por la normativa.

No obstante, en una suerte de exigencia de la cuadratura del círculo para la AEPD, la propia existencia de estos "tratamientos/opciones equivalentes" que impliquen menor riesgo para los derechos y libertades de las personas cuyos datos personales se van a tratar**, comporta que el tratamiento de datos biométricos deja de ser necesario**.

Dicha conclusión choca frontalmente con la que alcanzó durante el pasado mes de Octubre la autoridad de protección de datos británica, ***Information Comissioner's Office*** **(ICO)** que, siguiendo el criterio del EDPB, consideró que si se proporciona un método alternativo para aquellos que deseen optar por no usar datos biométricos, y los trabajadores no están en desventaja con dicha decisión, **el consentimiento es la base legal más probable para aplicar al uso de datos biométricos para el control de acceso.**

Al sostener la Agencia que de existir alternativas/opciones menos intrusivas ya no es necesario el uso de sistemas biométricos, **se está asociando el término "*necesidad*" a la existencia de una "*alternativa*" o "*tratamientos/opciones equivalentes*".** Esto constituye un cambio, más que discutible, respecto a la práctica convencional de recoger el consentimiento proporcionando una opción en lugar de otra (por ejemplo, permitir que el empleado elija entre registrar su jornada mediante huella dactilar o código PIN/tarjeta).



Uno de los requisitos esenciales para que un consentimiento sea válido según el RGPD es que sea "libre". Y es que, según las Directrices 5/2020 sobre el consentimiento en el sentido del RGPD del EDPB, "libre" implica que "*los interesados* ***deben tener una elección y un control real*****".**

Es por ello que, para garantizar la existencia de un consentimiento y la viabilidad de elegir, resulta necesario ofrecer diversas opciones o alternativas al interesado. Aunque algunas de estas opciones o alternativas equivalentes pueden ser percibidas como menos intrusivas que otras (como, por ejemplo, pagar en efectivo frente al pago con tarjeta de crédito), no implicando automáticamente que las demás opciones o alternativas deban considerarse como innecesarias.

3. Evaluación de Impacto para la Protección de Datos (EIPD) y garantías organizativas, técnicas y jurídicas

Para concluir, la Agencia recuerda que es indispensable que, con carácter previo a cualquier decisión de implantación de un sistema de control de presencia a través de sistemas biométricos, debe realizarse una **Evaluación de Impacto para la Protección de Datos** que incluya y también supere el triple juicio de idoneidad, necesidad y proporcionalidad requerido por el RGPD y también previsto por la doctrina del Tribunal Constitucional.

Al respecto del juicio de necesidad, será necesario demostrar que el tratamiento resuelve un problema real, presente o inminente, y crítico para el funcionamiento del tratamiento, así como explicar con pruebas por qué otras alternativas posibles no son suficientes para satisfacer esta necesidad.

Y en relación con el juicio de necesidad, de nuevo la Agencia indica que *"[…] un tratamiento de registro de jornada implementando con técnicas biométricas, y que levante la prohibición del 9.1 del RGPD basándose en un consentimiento libre del interesado,* ***no supera un análisis de necesidad en el marco de una EIPD"***.

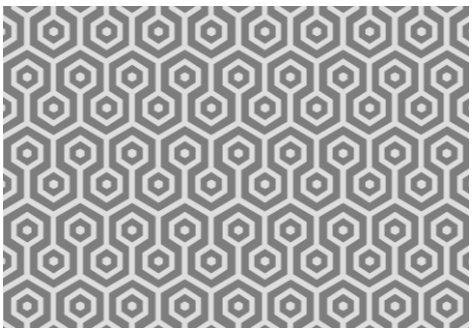
En su caso, superada la EIPD, así como todos los requisitos de cumplimiento de los principios generales del RGPD, la Agencia considera que como mínimo deben implementarse las siguientes medidas por defecto:

- Informar a los interesados sobre el tratamiento biométrico y los riesgos elevados asociados al mismo.
- Utilizar cifrado para proteger la plantilla biométrica.
- Implementar en el sistema la posibilidad de revocar el vínculo de identidad entre la plantilla biométrica y la persona física. o Implementar medios técnicos para asegurarse la imposibilidad de utilizar las plantillas para cualquier otro propósito.
- Imposibilitar la interconexión de bases de datos biométricos y la divulgación de datos.
- Suprimir los datos biométricos cuando no se vinculen a la finalidad que motivó su tratamiento.
- Aplicar la minimización de los datos biométricos recogidos.
- En el caso de registro de presencia o control de acceso en el ámbito laboral, se deben recoger en los convenios colectivos el conjunto de garantías con relación a estos tratamientos.

4. Tengo implementado un sistema biométrico y ¿ahora qué?

El reciente **cambio de criterio de la AEPD** sorprende, especialmente por la inseguridad jurídica que podría generar al interpretar el "*consentimiento*" de manera diferente a otras autoridades de protección de datos, al vincular la "*necesidad*" con la existencia de "*alternativas*" o "*tratamientos/opciones equivalentes*".

No obstante, **la Agencia no impone prohibiciones**; si no que detalla las condiciones para la legalidad del tratamiento biométrico en el control de presencia. Estas **condiciones son más complejas** que las anteriores, pero no inalcanzables.



Atendiendo a lo anterior, y al hecho de que actualmente no existe una norma con rango de ley que concrete la posibilidad de utilizar datos biométricos, **las empresas que hayan implementado el sistema biométrico** para supervisar la presencia de los empleados, **fundamentándolo en el cumplimiento de una obligación legal** (artículo 9.2.b) del RGPD), **deberán finalizar dicho tratamiento** de manera urgente y emplear un sistema alternativo para la supervisión de la presencia de los empleados.

No obstante, **si existe un convenio colectivo aplicable a la empresa** que especifique la posibilidad de utilizar datos biométricos, se deberá analizar el sistema biométrico. Si este análisis no se ha llevado a cabo previamente, **es necesario realizarlo y superar favorablemente una EIPD**.

Asimismo, y **dada la nueva interpretación de la AEPD sobre la base legal del consentimiento explícito** (artículo 9.2.a del RGPD), si la empresa ha implementado un sistema biométrico basándose en el consentimiento del empleado, recomendamos **llevar a cabo una reevaluación del tratamiento atendiendo a los nuevos criterios**, **al objeto de** determinar si es posible seguir utilizándolo, en el caso de que la empresa pueda **demostrar que (a) emplea la base legal del consentimiento explícito sin encontrar alternativas equivalentes; (b) supera el análisis de necesidad; y (c) además supera favorablemente una EIPD que incluya el triple juicio de idoneidad, necesidad y proporcionalidad**.

Considerando que **la AEPD no ha proporcionado un periodo de gracia** para los responsables del tratamiento que han implementado dichos sistemas biométricos con el fin de adaptarse a este nuevo criterio, persistir en su uso sin cumplir con los mencionados criterios conlleva el riesgo de enfrentarse a posibles reclamaciones iniciadas por parte de los trabajadores y, por consiguiente, potenciales sanciones por parte de la Agencia.