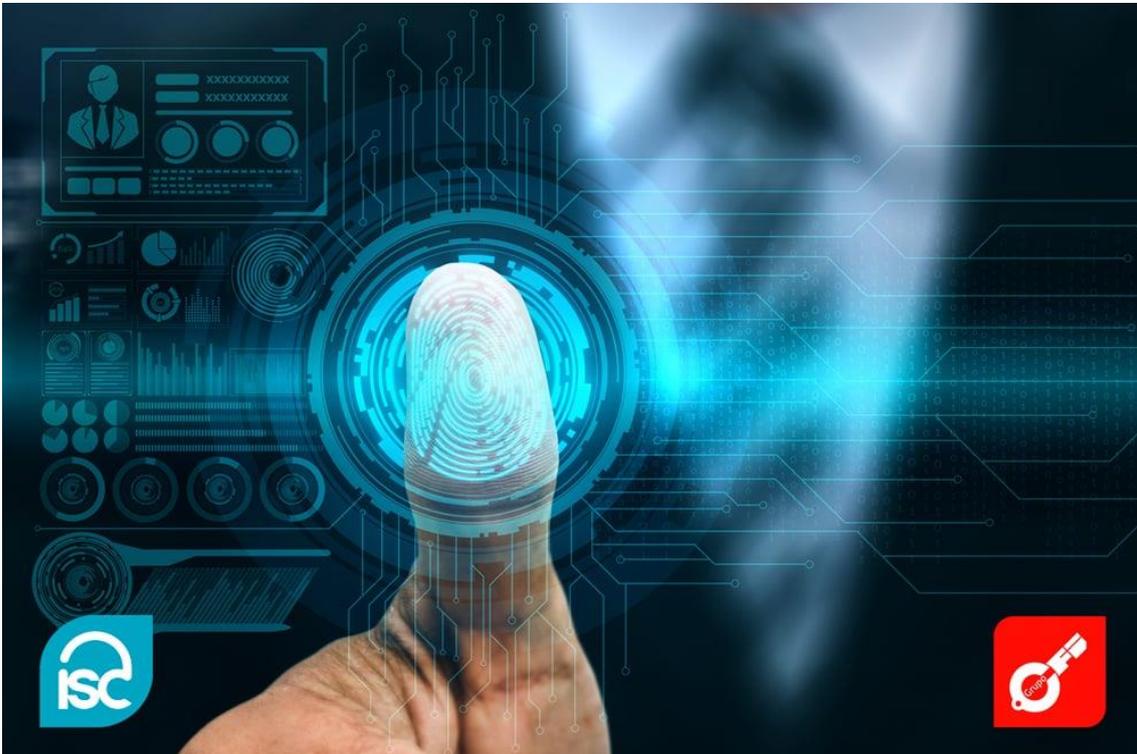


¿Es legal fichar con huella dactilar o con reconocimiento facial en el trabajo?

¡Todas las claves!



La obligación del registro de la jornada laboral entró en vigor en el año 2019, con la aprobación del [Real Decreto-ley 8/2019](#), 8 de marzo. Desde entonces hasta la actualidad, muchas empresas han utilizado diversos métodos de control y registro de horario, con el fin de registrar la actividad laboral de sus empleados. Ahora bien, **¿es legal fichar con huella dactilar o mediante reconocimiento facial?** En la *'Guía sobre tratamientos de control de presencia mediante sistemas biométricos'*, publicada recientemente por la Agencia Española de Protección de Datos (AEPD), fija los criterios para la utilización de la biometría para el control de acceso. **¡Sigue leyendo!** A continuación, te contamos **todas las claves**.

¿Qué son los datos biométricos?

El artículo 4.14 del Reglamento General de Protección de Datos (RGPD) recoge la siguiente definición sobre los **datos biométricos**. Estos son: "*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.*"

¿Son una categoría especial los datos biométricos?

Sí, el **artículo 9** del RGPD, que regula el tratamiento de categorías especiales de datos personales, recoge los datos biométricos como categoría especial, y

establece que “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 orientaciones sexuales de una persona física.”

Guía de la AEPD sobre el uso de datos biométricos. ¿Es legal fichar con datos biométricos en el trabajo?

La AEPD, el pasado 23 de noviembre de 2023, publicó ‘[La Guía sobre tratamientos de control de presencia mediante sistemas biométricos](#)’, donde considera como no lícito el tratamiento de control laboral o control de presencia, usando datos biométricos para identificar o autenticar a una persona, las **claves** de este nuevo criterio son que:

- El **dato biométrico** pertenece a las categorías especiales de datos, como son también los datos de salud, opiniones políticas, vida sexual, etc.;
- Se necesita una **norma con rango de ley** que justifique este tratamiento tan concreto, **ahora no existe**;
- El **consentimiento** del personal laboral **no es válido** para este tipo de tratamientos;
- El consentimiento **para otras finalidades** (control de presencia), requiere de un **medio alternativo de identificación**, lo que invalida la necesidad de implantar el sistema biométrico, que es más invasivo;
- Aunque el **registro de jornada es obligatorio**, hacerlo mediante un **patrón biométrico no lo es**, pueden usarse otros medios que no requieran tratar categorías especiales de datos;
- Aun teniendo una justificación válida, debemos hacer una **Evaluación de Impacto de Protección de Datos (EIPD)** sobre ese tratamiento, que podría resultar negativa y nos impediría el tratamiento, y que conlleva un coste añadido a la implementación del sistema en cuestión.



¿Según la AEPD, qué medidas mínimas por defecto se deben aplicar para garantizar la protección de los datos personales?

Tal y como destaca la AEPD en su Guía, en el planteamiento de un control de presencia con operaciones biométricas, además de una base jurídica del tratamiento, de una circunstancia que levante la prohibición de tratar categorías especiales de datos, y el cumplimiento de las condiciones del **art. 22 del RGPD**, es necesario establecer desde el diseño medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento.

Estas medidas, teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, **deben ser las adecuadas para gestionar el riesgo e, independientemente del nivel de riesgos, debes implementar, además, protección de datos por defecto.**

Entre las medidas mínimas por defecto, la AEPD, en su Guía “*La protección de datos en las relaciones laborales*”, ya estableció el siguiente conjunto de garantías, que se pueden extender a todo tratamiento de control de presencia:

- **Informar a los sujetos** de los datos sobre el tratamiento biométrico. Esto implanta, como señala el **considerando 39 del RGPD**, que “las personas físicas deben tener conocimiento de los riesgos” con relación a los tratamientos, en este caso biométrico.
- 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 las imposibilidades 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.**

Todas estas exigencias son condiciones necesarias, pero no suficientes, que han de ejecutarse, evaluarse objetivamente y documentarse, para que el control de acceso basado en procesos biométricos cumpla con los requisitos de proporcionalidad de tratamiento.



¿Qué pasa si en tu empresa se sigue utilizando la huella dactilar o el reconocimiento facial como control laboral?

Si la empresa en la que trabajas sigue utilizando un sistema biométrico para el registro de la jornada laboral, **puede ser sancionada por la AEPD** porque está utilizando un **método invasivo**, ya que el fichaje por huella dactilar y el reconocimiento facial, tal y como explicamos anteriormente, se consideran como **categoría especial**.

Aunque el artículo 20.3 del Estatuto de los Trabajadores, [Real Decreto Legislativo 2/2015, de 23 de octubre](#), menciona que “el empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad y teniendo en cuenta, en su caso, la capacidad real de los trabajadores con discapacidad.”

No obstante, el art. 9 del RGPD ‘Tratamiento de categorías especiales de datos personales’, establece una **prohibición de su tratamiento**, tal y como se ha señalado anteriormente, **salvo en las excepciones** que recoge este artículo, y en el caso concreto que nos ocupa, en relación con el control laboral, la excepción sería el **art.9.2. 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 respecto de los derechos fundamental y de los intereses del interesado.”

Además, en las directrices publicadas por el [Comité Europeo de Protección de Datos](#), aprobadas en abril de 2023, especifican que el uso de la huella dactilar o

el reconocimiento facial son **datos sensibles** y, por tanto, para utilizarlas como método de registro laboral, tendría que estar dentro de las excepciones que trata el **art. 9.2 del RGPD**.

«Si bien ambas funciones (autenticación e identificación) son distintas, ambas se relacionan con el procesamiento de datos biométricos relacionados con una persona física identificada o identificable y, por lo tanto, constituyen un tratamiento de datos personales, y más concretamente un tratamiento de categorías especiales de información personal.» (Traducción del inglés)

Conclusión

El control biométrico como método de registro ha estado sujeto a polémicas y a distintos puntos de vista desde su entrada en vigor hasta la actualidad. Para poder aclarar todas las dudas relativas a este tema, la AEPD hizo pública en 2023, la “*Guía sobre el control de presencia mediante sistemas biométricos*”. En ella, recoge que el **uso de sistemas mediante huella dactilar o reconocimiento facial son ilegales**, ya que “la utilización de tecnologías biométricas en el control de presencia supone un tratamiento de alto riesgo que incluye categorías especiales de datos.”

En la mencionada guía, se especifica que es necesario que exista una circunstancia para **levantar la prohibición** de tratar las categorías especiales de datos y, además, una condición que legitime el tratamiento, es decir:

- En el caso de registro de jornada y control de acceso con fines laborales, si el **levantamiento de la prohibición** se basa en el **art. 9.2.b del RGPD**, el responsable debe contar con una **norma de rango de ley** que concrete la posibilidad de utilizar datos biométricos para dicha finalidad, que no se encuentra en la actual normativa legal española.
- En el caso de registro de jornada o control de acceso en el ámbito laboral, **el consentimiento no puede levantar la prohibición** del tratamiento, ni ser una base para determinar la licitud, al existir de forma general una situación de desequilibrio entre el interesado y el responsable del tratamiento.

En el supuesto caso de que una empresa siga utilizando datos biométricos como método para registrar la actividad laboral de sus empleados, puede ser sancionada con una multa grave por parte de la AEPD