

El tratamiento de los datos biométricos para realizar controles de acceso y presencia en el ámbito laboral

José Luis González San Juan

Doctor en Derecho Privado.

Universidad de Salamanca (España)

Ingeniero de Telecomunicaciones.

Universidad Politécnica de Madrid (España)

joselgon2006@usal.es | <https://orcid.org/0000-0002-0613-7302>

Extracto

En este trabajo defendemos la tesis de que será difícil levantar la prohibición general del tratamiento de los datos biométricos de los trabajadores para realizar controles de acceso o de presencia en el ámbito laboral, pues casi siempre existirán alternativas menos lesivas que no requieran utilizar esta categoría especial de datos, y, si bien se permite que un convenio colectivo establezca una autorización expresa del tratamiento (siempre que prevea unas garantías adecuadas), consideramos que esta última opción debe ser normalmente descartada, ya que puede poner en grave riesgo los derechos fundamentales de los trabajadores. Finalmente, abogamos por una prohibición expresa, *de lege ferenda*, de estos tipos de tratamientos en el ámbito laboral.

Palabras clave: datos biométricos; control de acceso; control de presencia; minimización de datos; identificación; autenticación; inteligencia artificial; registro horario.

Recibido: 26-02-2026 / Revisado: 28-03-2026 / Aceptado: 31-03-2026 / Publicado: 07-05-2026

Cómo citar: González San Juan, J. L. (2026). El tratamiento de los datos biométricos para realizar controles de acceso y presencia en el ámbito laboral. *Revista de Trabajo y Seguridad Social. CEF*, 492, 51-80. <https://doi.org/10.51302/rtss.2026.25061>

The processing of biometric data to perform access and attendance controls in the workplace

José Luis González San Juan

PhD in Private Law.

University of Salamanca (Spain)

Telecommunications Engineer.

Technical University of Madrid (Spain)

joselgon2006@usal.es | <https://orcid.org/0000-0002-0613-7302>

Abstract

In this paper we defend the thesis that it will be difficult to lift the general prohibition on the processing of workers' biometric data for access or attendance controls in the workplace, since there will almost always be less harmful alternatives that do not require the use of this special category of data, and, although a collective agreement is allowed to establish an express authorization for the processing (provided that it provides for adequate safeguards), we consider that this last option should normally be discarded, since it can seriously jeopardize the fundamental rights of workers. Finally, we advocate for an express prohibition, *de lege ferenda*, of these types of treatment in the workplace.

Keywords: biometric data; access control; attendance control; data minimization; identification; authentication; artificial intelligence; time tracking.

Received: 26-02-2026 / Reviewed: 28-03-2026 / Accepted: 31-03-2026 / Published: 07-05-2026

Citation: González San Juan, J. L. (2026). The processing of biometric data to perform access and attendance controls in the workplace. *Revista de Trabajo y Seguridad Social. CEF*, 492, 51-80. <https://doi.org/10.51302/rtss.2026.25061>

Sumario

1. Introducción
 2. Cuestiones previas
 - 2.1. La protección de los datos personales como derecho fundamental
 - 2.2. Principales normas que debemos tener en cuenta para nuestro análisis
 - 2.3. Licitud del tratamiento
 - 2.4. Conceptos de dato biométrico y de sistema biométrico
 - 2.5. Categorías especiales de datos
 - 2.6. Identificación, autenticación, control de acceso y control de presencia
 - 2.7. Decisiones automatizadas
 3. Requisitos para realizar un tratamiento de datos biométricos en el ámbito laboral y evaluación de impacto de protección de datos
 - 3.1. Descripción de los tratamientos que se van a realizar, así como los fines buscados
 - 3.2. Levantamiento de la prohibición para tratar datos biométricos en el ámbito laboral con fines de control de acceso o de presencia
 - 3.2.1. Consentimiento explícito del interesado (art. 9.2 a) RGPD)
 - 3.2.2. El tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos (art. 9.2 b) RGPD)
 - 3.2.3. El tratamiento es necesario para la autenticación del interesado y los datos biométricos están bajo su control exclusivo (futuro art. 9.2 l) RGPD, propuesta legislativa de la UE «Ómnibus digital»)
 - 3.3. Licitud del tratamiento (art. 6 RGPD)
 - 3.4. Principio de minimización de datos y triple juicio de proporcionalidad
 - 3.5. Cumplimiento del resto de requisitos del RGPD
 - 3.6. Evaluación de riesgos y garantías organizativas, técnicas y jurídicas
 - 3.7. Otras cuestiones para tener en cuenta en la evaluación de impacto
 4. Conclusiones y propuesta final
- Referencias bibliográficas

1. Introducción

La utilización de datos biométricos en el ámbito laboral para llevar a cabo controles de acceso o de presencia puede dar lugar a vulneraciones de los derechos fundamentales de los trabajadores, y por ello, con carácter general, su tratamiento está prohibido por la normativa de protección de datos al tratarse de una categoría especial de datos personales, si bien se prevén una serie de excepciones que permiten levantar esta prohibición genérica. Además, la presencia cada vez más frecuente de inteligencia artificial (IA) en estos sistemas incrementa aún más los riesgos.

En este artículo estudiaremos si alguna de las excepciones previstas en la normativa de protección de datos podría ser aplicable para levantar la prohibición del tratamiento de los datos biométricos, pero antes de ello, y con un carácter esencialmente propedéutico, vamos a repasar algunos conceptos relevantes que deberán tenerse en cuenta a la hora de profundizar en nuestro análisis.

2. Cuestiones previas

2.1. La protección de los datos personales como derecho fundamental

En primer lugar, es preciso recordar que el derecho a la protección de los datos personales es un derecho fundamental autónomo (González Mendoza, 2025, p. 431) reconocido en el artículo 18.4 de la Constitución Española (CE), así como también en el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea (CDFUE), gozando, por ende, de la protección reforzada que otorga nuestro ordenamiento jurídico a todos los derechos fundamentales. Por ejemplo, el artículo 53.1 de la CE establece la reserva de ley para su regulación (Sierra Hernáiz, 2021, p. 69), y el artículo 53.2 de la CE determina su especial protección ante los tribunales ordinarios mediante un procedimiento basado en los principios de preferencia y sumariedad, así como con el recurso de amparo ante el Tribunal Constitucional (TC), en su caso.

Este derecho se traduce en un poder de disposición del individuo sobre sus propios datos personales, así como también en la facultad de control sobre el uso y destino de estos, con el objetivo de impedir su tráfico ilícito y evitar actuaciones lesivas para la dignidad o los derechos de su titular (Sentencia del Tribunal Constitucional –STC– 292/2000, de 30 de noviembre, FJ 6.º).

Un dato personal es cualquier información que identifique o permita identificar a una persona física, concepto que debe entenderse en un sentido muy amplio (Sierra Hernáiz, 2021, p. 25), de forma que incluye toda la información obtenida como resultado del tratamiento de los propios datos personales, siempre que se refiera a una persona física identificada o identificable. También debe entenderse en sentido amplio el concepto de «tratamiento» (Sentencias del Tribunal de Justicia de la Unión Europea de 4 de mayo de 2023, asunto C-487/21, CRIF GmbH, apdos. 23-27, y de 22 de junio de 2023, asunto C-579/21, Pankki S., apdos. 42-46).

2.2. Principales normas que debemos tener en cuenta para nuestro análisis

En el ámbito de la Unión Europea (UE), la principal norma relativa a los datos personales es el Reglamento (UE) 2016/679, Reglamento general de protección de datos (RGPD), en el que se consagra un modelo de protección de datos desde el diseño y por defecto.

Además, y dado que el tratamiento de los datos biométricos vendrá normalmente acompañado del uso de IA, también habrá que tener en cuenta las previsiones del Reglamento (UE) 2024/1689, Reglamento de IA (RIA).

Y, ya específicamente dentro del ordenamiento jurídico español, resultan relevantes la Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (LOPDGDD), el Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores (ET), el Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público (EBEP), y el Real Decreto-Ley (RDL) 8/2019, de 8 de marzo, de medidas urgentes de protección social y de lucha contra la precariedad laboral en la jornada de trabajo, que modifica el artículo 34 del ET en relación con el registro de la jornada laboral.

En todo caso, conviene aclarar que la enumeración anterior no pretende ser, ni mucho menos, exhaustiva, ya que existen diversas normas específicas que deberán considerarse cuando resulten aplicables a cada caso concreto¹.

¹ Por ejemplo, como bien apunta González Mendoza (2025, p. 432), el Reglamento 2018/1725, de 23 de octubre, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de estos datos, y también la Directiva 2016/680, de 27 de abril, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o ejecución de sanciones penales, y a la libre circulación de dichos datos, directiva transpuesta por 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.

2.3. Licitud del tratamiento

Para que cualquier tratamiento de datos personales sea lícito deberá cumplirse al menos una de las condiciones que se detallan de forma exhaustiva en el artículo 6 del RGPD.

En el ámbito laboral, que es el que nos ocupa, las condiciones de licitud que habitualmente se aplican son las previstas en los apartados b) y c) de dicho artículo, esto es, cuando el tratamiento es necesario para ejecutar un contrato en el que el interesado es parte (que en este caso normalmente será el contrato de trabajo) y cuando se requiere para el cumplimiento de una obligación legal del responsable del tratamiento (por ejemplo, para realizar los pagos a la Seguridad Social). No obstante, también se podría aplicar la condición incluida en el apartado a), el consentimiento del interesado, aunque como veremos *infra* con bastantes limitaciones, porque normalmente este consentimiento no va a ser libre en el ámbito laboral, debido al desequilibrio que prácticamente siempre existe entre el trabajador y el empresario.

2.4. Conceptos de dato biométrico y de sistema biométrico

El artículo 4.14 del RGPD define «datos biométricos» como aquellos 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. Se trata, pues, de una información generada por el propio cuerpo del titular de los datos (Navalón Arnal, 2025, p. 24).

Según ha puesto de manifiesto la doctrina (Mercader Uguina, 2024, p. 5; Muñoz Ruiz, 2023, p. 29), los datos biométricos son universales (todas las personas los tienen, salvo algunas excepciones), unívocos (permiten distinguir a un individuo), permanentes (normalmente se mantienen en el tiempo) y medibles (pueden ser cuantificados).

Por otra parte, podemos distinguir dos tipos o categorías de datos biométricos (Sierra Hernáiz, 2021, p. 103): por un lado, los que se corresponden con características físicas o fisiológicas del sujeto (por ejemplo, las huellas dactilares o la imagen del rostro), y por otro, aquellos que tienen que ver con su conducta o comportamiento (*v. gr.*, los movimientos al andar o las expresiones faciales). No obstante, también es posible distinguir una tercera categoría, la conformada por aquellos datos que tienen que ver con aspectos psicológicos, como puede ser la respuesta de una persona a una prueba psicológica específica (Mercader Uguina, 2024, p. 9; 2020, p. 9).

No obstante, aunque un determinado dato personal asociado a las características físicas, fisiológicas o conductuales de un sujeto permita su identificación, es posible que el tratamiento esté dirigido a otro fin distinto, y en ese caso podrá no tener la consideración

de dato biométrico. Así, una fotografía puede ser un dato biométrico si se procesa para identificar a una persona física que aparece en ella, pero cuando se utilice para otros fines distintos podría no serlo (considerando 51 RGPD).

El hecho de que los datos biométricos estén ínsitamente asociados a su titular provoca que sea muy sencillo realizar su tratamiento sin que el interesado llegue siquiera a saberlo (Barona Vilar, 2024, p. 320; González Mendoza, 2025, p. 448; Rodríguez-Piñero Royo, 2019, p. 96), por ejemplo, incorporando reconocimiento facial en un sistema de videovigilancia que ya estuviera implantado (González Mendoza, 2025, p. 460), algo que sería tan sencillo como añadir el módulo *software* de reconocimiento facial, pues el resto de la instalación ya estaría realizada (además, en el caso del reconocimiento facial podría verse afectado el derecho a la propia imagen del interesado, ex art. 18.1 de la CE).

Por otra parte, los sistemas biométricos son aquellos que recogen y procesan datos biométricos, que van a ser almacenados normalmente en forma de plantillas biométricas². Una plantilla biométrica no es más que el modo de estructurar los datos para que sean interpretados por una máquina, y normalmente será una representación matemática normalizada (vector de características, conjunto de descriptores, modelo paramétrico, etc.) obtenida a partir del dato biométrico y que contiene toda la información relevante para el tratamiento, de forma que no sea necesario almacenarlo en bruto ni trabajar directamente con él durante el procesado.

Suele exigirse la imposibilidad de reversión de la plantilla como una garantía para su titular, esto es, que no sea posible reconstruir el dato biométrico original a partir de esta (ni tampoco una réplica funcionalmente equivalente).

La plantilla no se asigna a una determinada persona, como ocurre, por ejemplo, con una tarjeta de identificación, sino que es generada directamente a partir de sus características físicas, fisiológicas o conductuales, características que son normalmente únicas e inalterables para cada individuo, y por ello, puede constituir un identificador unívoco de dicha persona, tal y como indica la Agencia Española de Protección de Datos (AEPD, 2023, p. 5).

La principal ventaja de la utilización de datos biométricos es que estos son únicos y permanentes para cada individuo, lo que permite diferenciarlo de forma relativamente sencilla dentro de un colectivo, evitando fraudes, al ser muy complicada (o incluso imposible) la cesión del dato biométrico a otra persona para que, por ejemplo, fiche en su lugar, algo que resulta más sencillo en un sistema basado en tarjetas con pin o contraseña (Navalón Arnal, 2025, p. 24; Fernández Orrico, 2020, epígrafes III y V.2).

² Barona Vilar (2024, pp. 305-317) ha recopilado una lista con los sistemas biométricos más utilizados actualmente y sus principales características.

No obstante, como cualquier otra tecnología, también puede ser vulnerada. Bajo determinadas circunstancias se podrían reproducir o simular los datos biométricos para engañar al sistema³ o bien sustituir o falsificar las plantillas biométricas, y el problema es que la intrusión podría traducirse en un robo de identidad perpetuo, pues una contraseña o un pin se pueden cambiar, pero los datos biométricos no pueden modificarse, como bien indica la Agencia Catalana de Protección de Datos (APDCAT, 2022, p. 11), pudiendo, además, afectar no solo al sistema atacado sino a cualquier otro en el que el sujeto utilice ese concreto dato biométrico (Navalón Arnal, 2025, p. 24).

Finalmente, conviene tener presente que los sistemas biométricos no son perfectos (realmente, ningún sistema lo es), de forma que siempre existirá un porcentaje de error, tanto por falsos positivos (el resultado del tratamiento es una aceptación cuando debería haber sido un rechazo) como por falsos negativos (se rechaza cuando tendría que aceptarse).

2.5. Categorías especiales de datos

Los datos biométricos son, por su propia naturaleza, datos cuyo tratamiento puede dar lugar a graves vulneraciones de los derechos fundamentales de sus titulares. Además, tienen la peculiaridad de que pueden ser utilizados muy fácilmente para otros fines adicionales a los inicialmente buscados, lo cual incrementa enormemente sus riesgos (AEPD, 2023, p. 12). De hecho, el Comité Europeo de Protección de Datos (CEPD, 2023, pp. 15-16), en un documento sobre directrices relativas al reconocimiento facial, ha venido a indicar que el tratamiento de datos biométricos, en cualquier circunstancia y con independencia del resultado, constituye una injerencia en los derechos fundamentales de los interesados (González Mendoza, 2025, p. 454).

Por todo ello, el artículo 9 del RGPD establece que los datos biométricos dirigidos a identificar de manera unívoca a una persona física son una categoría especial de datos cuyo tratamiento queda prohibido con carácter general, si bien se establecen ciertas excepciones en ese mismo artículo, algunas ciertamente bastante amplias, que, no obstante, entendemos habrán de ser interpretadas de forma restrictiva (Sierra Hernáiz, 2021, p. 87). Se incluyen en la prohibición tanto la identificación como la autenticación, y el concepto de «categoría especial» igualmente debe interpretarse de manera amplia (AEPD, 2023, p. 13).

Adicionalmente, también podría estar prohibido el tratamiento cuando revele información sensible del sujeto (origen étnico, datos de salud, etc.), algo que resulta relativamente

³ Por ejemplo, en los tratamientos de huellas dactilares, copiándolas mediante un molde o con fotos o escaneos del dedo, y cuando se utilice reconocimiento facial, mediante máscaras o bien utilizando fotos o vídeos *deepfakes* (González San Juan, 2022, pp. 600-601).

sencillo cuando se procesan datos biométricos, ya que, como esta información está implícita en los propios datos, el titular no puede impedir su recogida⁴.

El concepto «revele» nuevamente habrá de ser interpretado de forma amplia, y deberá tenerse en cuenta que los datos biométricos normalmente permiten inferir y recoger muy fácilmente esas otras categorías especiales de datos, como datos relativos a la salud o datos que evidencien el origen étnico o racial (AEPD, 2023, p. 13; Muñoz Ruiz, 2023, pp. 31-32). Por ejemplo, es relativamente sencillo obtener la temperatura o la presión sanguínea del sujeto al registrar su huella dactilar, o incluso información relativa a sus hábitos de consumo, pues es posible detectar trazas de drogas, explosivos, medicamentos consumidos u otras sustancias con las que ha estado en contacto (Bailey, 2018).

Además, el desarrollo tecnológico actual permite inferir también la actitud, el estado de ánimo, o incluso prever el comportamiento futuro de un sujeto a partir del análisis de sus datos biométricos, por ejemplo, mediante reconocimiento facial predictivo o el procesado de su voz⁵.

2.6. Identificación, autenticación, control de acceso y control de presencia

La identificación es un tratamiento de datos cuyo fin es determinar la identidad de una persona, esto es, singularizarla dentro de un conjunto determinado de individuos (operación 1 a N), mientras que la autenticación es la verificación de que un sujeto es realmente quien dice ser (operación 1 a 1). No obstante, aunque en ambos casos se llega finalmente a conocer la identidad de la persona (González Mendoza, 2025, p. 453), los riesgos asociados a la identificación (operación 1 a N) son sustancialmente mayores (AEPD, 2025, p. 5).

Por otra parte, el control de acceso es un tipo de tratamiento orientado a permitir o denegar a un sujeto la entrada a un determinado lugar o la utilización de un recurso concreto, mientras que el control de presencia tiene por finalidad registrar el tiempo que la persona física ha estado en ese sitio o ha utilizado dicha facilidad.

Tanto el control de acceso como el control de presencia pueden realizarse con fines laborales o con otros objetivos ajenos a una relación laboral.

⁴ Además, si se utiliza IA este tratamiento podría estar prohibido ex artículo 5.1 g) del RIA (Navalón Arnal, 2025, p. 25).

⁵ El artículo 5.1 f) del RIA prohíbe expresamente los sistemas de IA que permitan inferir las emociones de una persona física en los lugares de trabajo.

En el ámbito laboral, la forma más habitual de control de presencia es el registro de jornada, que fue regulado por el RDL 8/2019, de 8 de marzo, por el que se modifica el artículo 34.9 del ET, y que constituye tanto una obligación de la empresa como un derecho de los trabajadores y de sus representantes legales. Navalón Arnal (2025, p. 21) ha recopilado una breve revisión de la evolución de la obligación legal del registro de jornada en los últimos años.

La implantación del registro de jornada podrá llevarse a cabo mediante negociación colectiva o acuerdo de empresa, o, en su defecto, por decisión del empresario previa consulta con los representantes legales de los trabajadores, y deberá permanecer a disposición del trabajador, de sus representantes legales y de la Inspección de Trabajo y Seguridad Social durante cuatro años (art. 34.9 ET).

En cuanto al control de acceso, en principio quedaría justificado con base en la facultad de dirección y control del empresario, ex artículo 20.3 del ET (AEPD, 2023, p. 7), siempre que no se utilicen categorías especiales de datos personales.

Todos los procesos anteriores (identificación, autenticación, control de presencia y control de acceso) requieren el tratamiento de datos personales y a su vez pueden llevarse a cabo mediante sistemas biométricos o bien a través de otros medios que no utilicen esta categoría especial de datos personales.

2.7. Decisiones automatizadas

En el caso de que el tratamiento de los datos biométricos diese lugar a decisiones automatizadas que pudieran afectar a los trabajadores, entonces deberá aplicarse el artículo 22 del RGPD, a tenor del cual no cabe realizar el tratamiento salvo que este se base en el consentimiento (9.2 a) RGPD) o en un interés público esencial (9.2 g) RGPD). Además, tendrán que tomarse medidas específicas para salvaguardar los derechos y libertades, así como los intereses legítimos del interesado (art. 22.4 RGPD).

Y dado que la forma más eficaz que existe hoy en día para llevar a cabo decisiones automatizadas es utilizar IA, la mayoría de los sistemas biométricos existentes actualmente la utilizan en mayor o menor grado, por lo que deberemos tener en cuenta el RIA, y especialmente su anexo III, en el que se indica cuáles son los sistemas de alto riesgo. De hecho, existen actualmente aplicaciones que permiten el uso de IA para la toma de decisiones en prácticamente todas las fases de la relación laboral (Rodríguez Pérez, 2025, p. 56).

Pero estos sistemas de IA incrementan aún más los riesgos asociados al tratamiento de los datos biométricos, añadiendo problemas de sesgos que pueden dar lugar a la denominada discriminación algorítmica, y también haciendo que el sistema funcione como una

caja negra en la que solamente se conocen las entradas (datos biométricos) y los resultados, pero es muy complicado (o a veces imposible) comprender cómo ha sido tomada la decisión, incluso para los propios desarrolladores del sistema.

Para intentar minimizar los riesgos de esta opacidad intrínseca a la IA se desarrolló una reforma legislativa, con el objetivo de tener mayor transparencia sobre sus algoritmos cuando sea implantada en el entorno laboral. En concreto, el artículo 64.4 d) del ET establece el derecho de los representantes de los trabajadores a ser informados sobre los parámetros, reglas e instrucciones en los que se basan los algoritmos que afecten a las decisiones laborales (transparencia algorítmica).

No obstante, parte de la doctrina, con la que coincidimos, critica la falta de detalle de esta regulación, pues no establece claramente ni el momento ni la forma en que debe suministrarse la información, ni garantiza la intervención previa de la representación legal de los trabajadores (RLT) ante la implantación de un sistema de IA, ni tampoco se prevé qué ocurre cuando no existe RLT en una empresa (Rodríguez Pérez, 2025, p. 55). Es, por ello, un derecho a la información meramente pasivo.

En todo caso, es necesario tener presente que se trata de una cuestión complicada, puesto que la opacidad algorítmica, ínsita en los sistemas de IA, será normalmente un obstáculo para poder proporcionar una información útil, ya que, de hecho, muchas veces ni los diseñadores ni los programadores de los sistemas conocen los detalles del verdadero proceso que existe detrás de las tomas de decisiones de los algoritmos, especialmente cuando se trate de sistemas de aprendizaje profundo (*deep learning*), pues su funcionamiento dependerá, en gran medida, de la forma en que han sido entrenados, así como de los concretos datos utilizados para el proceso de aprendizaje.

Y, por otra parte, las empresas suministradoras de estos sistemas serán reticentes a dar una información que podría caer en manos de la competencia perjudicando su negocio, además de que puede estar protegida por derechos de propiedad intelectual en sentido estricto (normalmente derechos de autor) o de propiedad industrial (casi siempre secreto industrial).

3. Requisitos para realizar un tratamiento de datos biométricos en el ámbito laboral y evaluación de impacto de protección de datos

Como hemos visto, los datos biométricos son un tipo de dato personal especialmente protegido debido a que su utilización puede afectar gravemente a los derechos fundamen-

tales de sus titulares⁶, y, por ende, queda prohibido su tratamiento con carácter general, siendo posible solamente cuando se cumpla alguna de las excepciones previstas en el artículo 9.2 del RGPD.

Por ello, el responsable del tratamiento que vaya a implantar un sistema de control de presencia o de acceso en el ámbito laboral deberá, en primer lugar, levantar dicha prohibición general de tratamiento sobre la base de alguna de las circunstancias previstas en el artículo 9.2 del RGPD, que es una lista exhaustiva.

Pero el levantamiento de la prohibición general del tratamiento no exime del cumplimiento de la licitud ex artículo 6 del RGPD, esto es, será preciso determinar también, en segundo lugar y una vez levantada la prohibición general de tratamiento, la condición que lo hace lícito, dentro de las enumeradas en la lista incluida en el artículo 6 del RGPD, también exhaustiva.

Y lo anterior deberá hacerse para cada uno de los fines con los que se vaya a realizar el tratamiento, tanto en lo que se refiere al levantamiento de la prohibición como a la licitud del tratamiento y, además, con carácter previo a la implantación del sistema.

Finalmente, en tercer lugar y nuevamente también con carácter previo a la puesta en marcha (Montesdeoca Suárez, 2024, p. 144), como el tratamiento de datos biométricos va a ser de alto riesgo en la práctica totalidad de los casos, deberá realizarse una evaluación de impacto de protección de datos (EIPD) ex artículo 35 del RGPD, y en su caso una consulta previa a la AEPD, pues, a tenor del artículo 36 del RGPD, el responsable del tratamiento deberá consultar con carácter previo a la AEPD cuando una evaluación de impacto muestre que el tratamiento entrañaría un alto riesgo si el responsable no tomara medidas para mitigarlo.

Un tratamiento es de alto riesgo cuando sea probable que se puedan vulnerar los derechos y libertades de las personas físicas, especialmente cuando se utilizan nuevas tecnologías (art. 35 RGPD). A tenor del artículo 35.4 del RGPD, la AEPD publica la lista de los criterios para determinar si existe alto riesgo⁷, de forma que normalmente existirá cuando se cumplan dos o más criterios de la lista. Y como los tratamientos de datos biométricos para identificación o autenticación cumplen como mínimo los criterios 4, 5 y 10 de dicha lista, consideramos que prácticamente siempre serán de alto riesgo, requiriendo, por ende, la EIPD.

⁶ En principio, la implantación de un sistema biométrico en una empresa no supondrá una modificación sustancial de las condiciones de trabajo, ex artículo 41 del ET, al no afectar a ninguna de las materias contempladas en dicho artículo (Mercader Uguina, 2020, epígrafe 5.1; Muñoz Ruiz, 2023, p. 39).

⁷ <https://www.aepd.es/documento/listas-dpia-es-35-4.pdf>

No obstante, la realización de la EIPD no excluye el cumplimiento del resto de requisitos establecidos en la normativa de protección de datos.

También es preciso recordar que el responsable del tratamiento debe establecer una gestión del riesgo (art. 24.1 RGPD), aplicando las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme al RGPD. Y todo ello tiene que realizarse desde el diseño y por defecto *ex* artículo 25 del RGPD (AEPD, 2023, p. 23).

Además, el artículo 24.1 del RGPD indica que es responsabilidad del encargado del tratamiento revisar y actualizar las medidas siempre que sea preciso, correspondiéndole también la carga de la prueba (principio de responsabilidad proactiva, art. 5.2 RGPD).

Y si bien la EIPD deberá realizarse, como ya hemos indicado, con carácter previo al inicio del tratamiento, esto no excluye que deba actualizarse periódicamente o cuando las circunstancias así lo aconsejen.

En la EIPD entendemos que deberán incluirse, como mínimo, los siguientes puntos:

1. Descripción de los tratamientos que se van a realizar, así como los fines buscados.
2. Justificar el levantamiento de la prohibición general para el tratamiento de los datos biométricos según el artículo 9.2 del RGPD, para cada uno de los fines.
3. Justificar la licitud del tratamiento (art. 6 RGPD), también para cada uno de los fines.
4. Justificar el cumplimiento de los principios de minimización y de proporcionalidad.
5. Justificar el cumplimiento del artículo 22 del RGPD, cuando aplique, así como con el resto de los principios, derechos y obligaciones establecidas en el RGPD, y si se utilizara IA, también de las garantías reguladas en el RIA.
6. Evaluación de riesgos y descripción de las garantías organizativas, técnicas y jurídicas que vayan a establecerse para minimizar los efectos del tratamiento.
7. Detallar cualquier otra circunstancia presente en el caso concreto y que pudiera afectar a los riesgos del tratamiento o a sus consecuencias.

A continuación, vamos a comentar cada uno de estos puntos.

3.1. Descripción de los tratamientos que se van a realizar, así como los fines buscados

En la evaluación de impacto de protección de datos deben detallarse los tratamientos que se pretende implantar, así como los fines buscados. Eso implica describir la naturaleza del tratamiento, indicando los datos que se tratarán (con referencia a si alguno de ellos es de categoría especial), el tiempo y la forma en que van a conservarse, así como cualquier otra información relevante. Es preciso añadir, además, el contexto en el que se efectuará el tratamiento y los medios que se utilizarán para realizarlo, haciendo especial referencia a la tecnología o tecnologías que van a ser empleadas.

También debe detallarse quién es el responsable del tratamiento y, en su caso, el encargado del tratamiento, así como el público objeto de este, esto es, indicar si va a afectar a todos los empleados de la empresa o únicamente a ciertos colectivos, y si comprenderá también a los trabajadores de las subcontratas y/o al público visitante.

Además, hay que especificar el alcance físico del tratamiento, esto es, dónde va a realizarse: si se va a implantar solo en determinadas zonas concretas de las instalaciones de la empresa, si va a afectar únicamente a un centro de trabajo o a todos los centros (cuando hubiera varios), etc.

3.2. Levantamiento de la prohibición para tratar datos biométricos en el ámbito laboral con fines de control de acceso o de presencia

Como hemos visto, para llevar a cabo el tratamiento de una categoría especial de datos personales es preciso levantar la prohibición general establecida en el artículo 9.1 del RGPD. Por ello, el responsable del tratamiento debe justificar cuál de las excepciones previstas en el artículo 9.2 del RGPD resulta aplicable.

En el caso de la utilización de datos biométricos en el ámbito laboral podrían ser aplicables, en principio, las dos siguientes: a) que exista consentimiento del interesado (art. 9.2 a) RGPD); b) que el tratamiento sea necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos (art. 9.2 b) RGPD).

No obstante, es preciso tener en cuenta la Propuesta de Reglamento del Parlamento Europeo y del Consejo por la que se modifican los Reglamentos (UE) 2016/679, (UE) 2018/1724, (UE) 2018/1725, (UE) 2023/2854 y las Directivas 2002/58/CE, (UE) 2022/2555 y (UE) 2022/2557 en lo que respecta a la simplificación del marco legislativo digital y se derogan los Reglamentos (UE) 2018/1807, (UE) 2019/1150, (UE) 2022/868 y la Directiva (UE) 2019/1024 (Ómnibus digital) {SWD(2025) 836 final}.

En esta reforma, que está actualmente tramitándose en la UE, se prevé añadir dos nuevas excepciones en el artículo 9.2 del RGPD (letras k y l), y una de ellas hace referencia al tratamiento de los datos biométricos, autorizándolo expresamente cuando sea necesario para la autenticación y los datos estén bajo control exclusivo del interesado (futuro art. 9.2 l) RGPD).

3.2.1. Consentimiento explícito del interesado (art. 9.2 a) RGPD)

La primera excepción que podría considerarse es la prevista en el artículo 9.2 a) del RGPD, esto es, la existencia de un consentimiento explícito del interesado para realizar el tratamiento de los datos biométricos para ese fin o fines concretos.

Además de explícito, y de conformidad con el artículo 4.11 del RGPD, el consentimiento debe ser libre, específico, informado e inequívoco. Pero, según se indica en el considerando 43 del RGPD, para garantizar que este consentimiento se haya prestado libremente, no será considerado válido cuando exista un desequilibrio claro entre el interesado y el responsable del tratamiento.

Y, como en las relaciones laborales prácticamente siempre va a existir un desequilibrio de poder entre el empresario y el trabajador, consideramos, coincidiendo con la posición prácticamente unánime de la doctrina (AEPD, 2023, pp. 20-21; APDCAT, 2022, pp. 10 y 13; Rodríguez-Piñero Royo, 2019, p. 107; Róo García, 2024, pp. 4-5), que el consentimiento rara vez va a ser libre en el ámbito laboral, y por ende, que no puede establecerse, con carácter general, como una base jurídica válida para levantar la prohibición del tratamiento de los datos biométricos, ex artículo 9.2 a) del RGPD, con fines de control de acceso o de presencia.

Sin embargo, esto no significa que no se pueda utilizar el consentimiento en el ámbito laboral en ningún caso, pues cabrá hacerlo cuando el empresario pueda demostrar que el hecho de no otorgar el consentimiento no tendrá consecuencias adversas para el trabajador. Esto podría conseguirse, por ejemplo, ofreciendo una alternativa equivalente al empleado que no implicara un tratamiento de sus datos biométricos, y, por ende, que no necesitara su consentimiento para levantar la prohibición (Consejo de Transparencia y Protección de Datos de Andalucía –CTPDA–, 2023, p. 4). Pero esto implicaría automáticamente que el tratamiento de los datos biométricos no sería realmente necesario para conseguir los fines buscados, de forma que se estaría vulnerando el principio de minimización de datos si se utilizaran datos biométricos para conseguir unos resultados que podrían alcanzarse perfectamente sin ellos. Además, recordamos que la carga de la prueba corresponde al encargado del tratamiento, con base en el principio de responsabilidad proactiva, ex artículo 5.2 del RGPD (APDCAT, 2022, p. 10).

Por todo ello y en nuestra opinión, el consentimiento solamente va a ser libre en el ámbito laboral en circunstancias excepcionales, y normalmente con respecto a tratamientos

accesorios a la relación laboral, por ejemplo, cuando se otorgue para publicar en la intranet fotografías del empleado tomadas durante una cena de empresa.

En cualquier caso, si en alguna situación se llegara a prestar un consentimiento libre en el ámbito laboral, consideramos que es imprescindible que se permita su revocación en cualquier momento y, obviamente, también sin consecuencias para el trabajador (Montes-deoca Suárez, 2024, p. 134). No obstante, esto no afectaría a la licitud de los tratamientos realizados con anterioridad a la retirada de ese consentimiento que fue otorgado válidamente (art. 13.2 c) RGPD).

3.2.2. El tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos (art. 9.2 b) RGPD)

De conformidad con el artículo 9.2 b) del RGPD, sería posible levantar la prohibición general del tratamiento de los datos biométricos cuando este sea necesario para el cumplimiento de obligaciones y el ejercicio de derechos del responsable o del interesado y en la medida que 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 la conveniencia del interesado.

Esta excepción requiere, en primer lugar, que se cumpla el requisito de necesidad, esto es, que el tratamiento de esos datos especialmente protegidos sea imprescindible para cumplir las obligaciones o ejercitar los derechos, y, en segundo lugar, una vez establecida la necesidad, que el tratamiento esté autorizado por una norma o un convenio colectivo.

A continuación, comentaremos cada una de esas condiciones.

1. Requisito de necesidad

Para poder levantar la prohibición, el tratamiento de los datos biométricos debe ser necesario para el cumplimiento de obligaciones o el ejercicio de derechos, bien del responsable del tratamiento o bien del interesado. Y este requisito es aplicable tanto en el caso de que la autorización esté prevista en una norma como cuando lo contemple un convenio colectivo.

El requisito de necesidad implica que el cumplimiento de las obligaciones o el ejercicio de los derechos no podría realizarse sin el tratamiento de los datos de categoría especial, y consideramos que en el caso que estamos analizando (tratamiento de datos biométricos para realizar controles de acceso o presencia en el ámbito laboral) difícilmente va a cumplirse este requisito de necesidad, pues siempre van a existir alternativas mucho menos invasivas que permiten cumplir las obligaciones o ejercitar los derechos.

Para que realmente fuera necesario, el tratamiento de datos biométricos debería ser esencial para lograr los fines buscados, no basta con que sea mejor o más conveniente, mejore los costes, o se trate de una técnica más moderna o novedosa. En este sentido, coincidimos con Róo García (2024, p. 2), que afirma:

En muchas ocasiones, las administraciones se dejan llevar por presuntas pseudo-corrientes de modernidad que incorporan las nuevas tecnologías, sin tener en cuenta la protección de datos personales, como por ejemplo el uso de los datos de biométricos para realizar actividades de verificación y control de la presencia en el puesto de trabajo.

Y si bien se refiere a un sistema de reconocimiento facial de un ayuntamiento, su opinión resulta perfectamente trasladable a cualquier empresa y a todo tipo de tratamiento de datos biométricos.

En relación con este tema, procede traer a colación la reciente Sentencia de la Sala de lo Social del Tribunal Superior de Justicia de Galicia 144/2026, de 15 de enero⁸, que resuelve un asunto relativo a un sistema de reconocimiento facial implantado por la empresa Make Packing, SL, para el fichaje de sus trabajadores, condenando a dicha mercantil a pagar 7.501 euros a la demandante en concepto de indemnización por daños y perjuicios, por haber vulnerado sus derechos fundamentales a la propia imagen y a la protección de datos.

Esta sentencia ha sido objeto de múltiples noticias de prensa, especialmente durante el mes de febrero de 2026, y en muchas de ellas se afirmaba que la empresa había sido condenada a pagar más de 50.000 euros por haber implantado un sistema de reconocimiento facial para control horario. No obstante, procede aclarar que la mercantil fue condenada realmente a abonar 46.266,90 euros por despido improcedente y 7.501 euros por daños morales, pero en algunas noticias se suman ambas cantidades sin dar más explicaciones.

En el FJ 3.º de la Sentencia 144/2026 se afirma lo siguiente:

Sin embargo, en el caso que nos ocupa, el tratamiento no era necesario, ya que existían otros medios para registrar la jornada y el horario sin interferir con los derechos fundamentales, como el control mediante una tarjeta que la propia empresa indicó en el acta de la reunión (3.ª FP revisada).

2. Existencia de una norma con rango de ley que autorice el tratamiento

El artículo 9.2 b) del RGPD determina que, además de ser necesario, el tratamiento debe estar autorizado por el derecho de la Unión de los Estados miembros (o por un

⁸ Comentada en esta misma revista y número. *Vid.* Montesdeoca Suárez (2026).

convenio, como veremos en el apartado siguiente). En el caso del Estado español, esta autorización deberá estar prevista en una norma con rango de ley, debido a que la protección de datos es un derecho fundamental para cuyo desarrollo se contempla reserva de ley (art. 53.1 CE).

En nuestra opinión, el considerando 41 del RGPD también lo indica indirectamente, pues afirma:

Cuando el presente Reglamento hace referencia a una base jurídica o a una medida legislativa, esto no exige necesariamente un acto legislativo adoptado por un parlamento, sin perjuicio de los requisitos de conformidad del ordenamiento constitucional del Estado miembro de que se trate.

Y en el caso de España, el artículo 53.1 de la CE establece reserva de ley para el desarrollo de los derechos fundamentales, entre ellos la protección de datos.

Adicionalmente, el artículo 52.1 de la CDFUE indica que «Cualquier limitación del ejercicio de los derechos y libertades reconocidos por la presente Carta deberá ser establecida por la ley y respetar el contenido esencial de dichos derechos y libertades» y, como ya vimos, el derecho a la protección de datos de carácter personal está reconocido en el artículo 8 de dicha Carta (González Mendoza, 2025, p. 455).

Teniendo en cuenta lo anterior, podría argumentarse que el artículo 20.3 del ET sería una justificación válida para el levantamiento de la prohibición del tratamiento, al establecer la capacidad de control del empresario⁹, o que también lo sería el RDL 8/2019 relativo al registro de jornada, que impone al empresario la obligación del control horario, pero aunque ambas sean normas con rango de ley, consideramos que ninguna de ellas puede levantar la prohibición, por los motivos que veremos a continuación.

En efecto, no basta simplemente con que la norma con rango de ley autorice el tratamiento de los datos, sino que, además, «ha de expresar todos y cada uno de los presupuestos y condiciones de la intervención» (STC 76/2019, de 22 de mayo, FJ 5.º), exigiéndose, por tanto, precisión de la ley en la limitación del derecho, esto es, que exista previsibilidad (AEPD, 2023, pp. 14-15).

Así pues, la afectación del derecho que se derive de la norma debe ser previsible y no lo es una ley que no concreta expresamente la posibilidad de utilizar datos biométricos para identificación o autenticación, y adicionalmente, «la norma debe establecer garantías adecuadas cuando se traten categorías especiales de datos» (APDCAT, 2022, p. 6).

⁹ Delgado Martín (2021) defiende esta posición en relación con el control horario mediante huella dactilar, pero entendemos que sus argumentos, con los que discrepamos, serían fácilmente trasladables al control de presencia o de acceso mediante el tratamiento de cualquier otro tipo de dato biométrico.

De hecho, nuestro TC requiere que la norma que autoriza el tratamiento establezca garantías adecuadas, incluso aunque no se trate de categorías especiales de datos (STC 292/2000, de 30 de noviembre, FJ 10.º). También se exigen estas garantías adecuadas en el artículo 6 del Convenio 108 del Consejo de Europa, en este caso para poder realizar el tratamiento de los datos biométricos que identifiquen unívocamente a una persona, así como el de otros datos de categoría especial enumerados en dicho artículo.

Por ello, el CTPDA (2023, p. 6), en su Dictamen 1/2023, y en relación con el uso de reconocimiento facial o huella dactilar para control horario en un ayuntamiento, afirma lo siguiente:

El levantamiento de la referida prohibición no puede ampararse en la actualidad en la concurrencia de la circunstancia prevista en el artículo 9.2 b) del RGPD puesto que en la actual normativa legal española no se contiene autorización para considerar necesario el tratamiento de datos biométricos con la finalidad de un control horario de la jornada de trabajo.

Y esta posición está en plena consonancia con la de la autoridad catalana (APDCAT, 2022, pp. 6-7) y también ha sido asumida por la AEPD (2023, pp. 16 y 29), como ha puesto de manifiesto la doctrina (Muñoz Ruiz, 2024, p. 4).

Por tanto, podemos concluir que, actualmente, no existe en el ordenamiento jurídico español una norma con rango de ley que permita levantar la prohibición general del tratamiento de datos biométricos para llevar a cabo controles de acceso o presencia en el ámbito laboral, aunque sí que sería posible que lo habilitara expresamente un convenio colectivo, como veremos a continuación.

3. Autorización del tratamiento mediante un convenio colectivo

El artículo 9.2 b del RGPD también posibilita que la prohibición general del tratamiento de los datos biométricos pueda ser levantada por un convenio colectivo que lo autorice expresamente, y siempre que, además de ser un tratamiento necesario para el cumplimiento de obligaciones y el ejercicio de derechos del responsable o del interesado, en el mismo se establezcan garantías adecuadas para el respeto de los derechos fundamentales y de los intereses del trabajador.

Y, como nos indica Mercader Uguina (2024, p. 18), con quien coincidimos, este artículo se está refiriendo a los convenios colectivos estatutarios (regulados en el ET), que son fuente de derecho a tenor de los artículos 3.1 b y 82.3 del ET.

Cabe, por tanto, que un convenio colectivo autorice el tratamiento de estos datos de categoría especial, siempre que se cumplan los requisitos indicados en los dos párrafos anteriores, pero esto plantea el problema de trasladar a la negociación colectiva la responsabilidad de establecer las medidas adecuadas para garantizar el respeto de los derechos fundamentales y los intereses de los trabajadores.

Es más, el propio artículo 91 de la LOPDGDD indica que «Los convenios colectivos podrán establecer garantías adicionales de los derechos y libertades relacionados con el tratamiento de los datos personales de los trabajadores y la salvaguarda de derechos digitales en el ámbito laboral» (Rodríguez-Piñero Royo, 2019, p. 99).

En cierta manera, se estaría supliendo la falta de detalle de la que adolece la normativa¹⁰, para trasladar la responsabilidad a las mesas de negociación, con el riesgo que esto supone, ya que puede traducirse en una desprotección de los trabajadores cuando finalmente el convenio colectivo no establezca medidas de protección realmente eficaces.

De esta forma, y al igual que ocurre en relación con el uso de la IA en el entorno laboral (Rodríguez Pérez, 2025, p. 65), la negociación colectiva se presenta como el principal instrumento para suplir las deficiencias legislativas en relación con la utilización de los datos biométricos en los centros de trabajo.

No obstante, puede ocurrir perfectamente que los integrantes de las mesas de negociación no tengan conocimientos técnicos avanzados sobre protección de datos (Navalón Arnal, 2025, p. 47), de forma que se corre el riesgo de que los convenios se limiten a reproducir la normativa aplicable (especialmente el RGPD y la LOPDGDD) o incluso a no prevenir ningún tipo de medidas, cuando lo que deberían hacer es establecer nuevas garantías eficaces para salvaguardar los derechos y los intereses de los trabajadores.

Así, los propios convenios colectivos se tornarían en un medio idóneo para provocar vulneraciones de los derechos de los trabajadores, cuando su papel debería ser precisamente el contrario: establecer derechos y garantías adicionales a los ya consagrados *ex lege* (Cruz Villalón, 2020; Navalón Arnal, 2025, p. 41).

Pero, si finalmente se optara por incluir esta autorización del tratamiento en un convenio colectivo, entendemos que tanto la justificación del requisito de la necesidad como el establecimiento de las garantías deberán realizarse en el momento de la negociación, y no en la fase posterior en la que la empresa o empresas, sobre las que se proyecte un convenio ya vigente, implanten los tratamientos.

Coincidimos con Navalón Arnal (2025, p. 45), que considera que el momento de justificar la necesidad del tratamiento para el cumplimiento de obligaciones o el ejercicio de derechos, bien del responsable del tratamiento o bien del interesado, debe ser el de la negociación, pues en caso contrario el convenio colectivo podría ser declarado ineficaz. De la

¹⁰ Tanto la AEPD (2025, p. 8) como una parte relevante de la doctrina consideran que es necesaria una regulación más detallada del tratamiento de los datos biométricos (Barona Vilar, 2024, p. 318; Fernández Orrico, 2020, apartado VII; Sierra Hernáiz, 2021, p. 199).

misma forma, las garantías para salvaguardar los derechos e intereses de los trabajadores deberán establecerse también en el momento de la negociación colectiva e incluirse en el propio convenio.

Y no consideramos que el requisito de contar con el consentimiento informado del trabajador pueda ser una garantía válida para salvaguardar sus derechos e intereses, porque por mucho que se regule en un convenio, seguirá siendo un consentimiento que difícilmente podrá ser prestado libremente en términos individuales, al existir un desequilibrio de poder entre empresario y trabajador. Y debe tenerse muy presente que el consentimiento es un acto personalísimo del interesado, de forma que no puede ser sustituido por una suerte de «consentimiento colectivo» acordado en un convenio.

Así pues, es frecuente encontrar convenios colectivos que no cumplen con estos requisitos o lo hacen de una forma muy deficiente. No obstante, es cierto que muchos son anteriores al año 2023, año en que se publicó la *Guía sobre tratamientos de control de presencia mediante sistemas biométricos* de la AEPD (2023), y por ello no siguen las directrices que en ella se establecen.

Por eso, algunos autores, con los que coincidimos, consideran que tras la publicación de la guía de la AEPD la mayoría de esos convenios tendrían que ser revisados, depurando las cláusulas que legitimen el uso de datos biométricos para el control horario sin incluir garantías eficaces (Muñoz Ruiz, 2024, p. 4).

Además, muchos convenios colectivos se limitan a reproducir algunas previsiones ya establecidas en la normativa y, normalmente, tampoco justifican adecuadamente el requisito de necesidad o simplemente lo ignoran.

Por ejemplo, el Convenio colectivo del sector del comercio en las Islas Baleares 2019-2023 (Muñoz Ruiz, 2023, pp. 48-49), que sigue vigente actualmente al no haber sido denunciado y estar prevista su prorroga tácita, autoriza, en su artículo 32.2, letra e, la implantación de sistemas de reconocimiento facial para control de presencia (registro de jornada) sin establecer ningún tipo de garantía (ni siquiera se alude a las previstas en la normativa de protección de datos) y obviando completamente el requisito de necesidad.

Por todo ello, y si bien el artículo 9.2 b) del RGPD contempla el levantamiento de la prohibición general del tratamiento de los datos biométricos mediante un convenio colectivo como una alternativa perfectamente válida, consideramos que no es una opción recomendable, ya que se corre el riesgo de que los convenios agraven y legitimen la intromisión en los derechos fundamentales de los trabajadores y/o produzcan resultados contrarios a sus intereses, perdiendo, de esta forma, el papel que tradicionalmente han venido manteniendo los convenios colectivos como garantes de tales derechos.

3.2.3. El tratamiento es necesario para la autenticación del interesado y los datos biométricos están bajo su control exclusivo (futuro art. 9.2 I) RGPD, propuesta legislativa de la UE «Ómnibus digital»)

Como hemos adelantado, actualmente existe una reforma legislativa en trámite en la UE denominada «Ómnibus digital», que prevé incluir dos nuevas excepciones en el artículo 9.2 del RGPD (letras k y l), una de las cuales podría ser aplicable a la materia que estamos analizando. En concreto, la prevista en la nueva letra l), cuyo tenor es el siguiente: «l) cuando el tratamiento de datos biométricos sea necesario para confirmar la identidad de un interesado (verificación), cuando los datos biométricos o los medios necesarios para la verificación estén bajo el control exclusivo del interesado».

Si esta nueva excepción es finalmente aprobada con su redacción actual, será exclusivamente aplicable al tratamiento de datos biométricos con fines de autenticación, por lo que, en principio, podría parecer que viene a autorizar (o cuando menos a facilitar en gran medida) el establecimiento de controles de acceso o de presencia basados en datos biométricos, tanto en el entorno laboral como en cualquier otro ámbito, y siempre que se cumplan las condiciones indicadas.

Para aplicar esta nueva excepción se exigen dos requisitos: en primer lugar, que el tratamiento sea necesario para llevar a cabo la autenticación del interesado, y, en segundo lugar, que los datos biométricos o los medios necesarios para realizar la verificación estén bajo control exclusivo del interesado.

La segunda de las condiciones sería relativamente sencilla de cumplir, pues bastaría con almacenar la plantilla biométrica en una tarjeta con chip (o en cualquier otro dispositivo dotado de una memoria digital) que estuviera bajo control exclusivo del interesado, de forma que la plantilla se comparara en tiempo real con el dato biométrico obtenido del interesado en el mismo momento del fichaje, sin almacenar ni el dato biométrico ni la plantilla en los equipos del sistema de autenticación.

Pero, en lo que respecta al requisito de necesidad, entendemos que normalmente será difícil de justificar, pues resultan aplicables los mismos argumentos que hemos detallado en el epígrafe 3.2.2., apartado 1, ya que, prácticamente siempre, existirán alternativas igualmente eficaces para lograr las finalidades del tratamiento que no van a requerir el procesamiento de datos biométricos, y que deberían ser elegidas en aplicación de los principios de minimización de datos y de proporcionalidad, como explicaremos detalladamente en el epígrafe 3.4.

Por tanto, en nuestra opinión, esta nueva excepción difícilmente podrá ser utilizada, con carácter general, para levantar la prohibición de tratamiento de los datos biométricos de los trabajadores en los centros de trabajo, al menos con su redacción actual.

3.3. Licitud del tratamiento (art. 6 RGPD)

Una vez levantada la prohibición general del tratamiento de los datos biométricos, el responsable del tratamiento deberá justificar que este es lícito (principio de licitud, ex art. 5.1 a) del RGPD), y para ello, tendrá que estar amparado por alguna de las bases jurídicas previstas en el artículo 6.1 del RGPD.

Parte de la doctrina, con la que discrepamos, considera que se podría justificar la licitud del tratamiento de los datos biométricos sobre la base del artículo 6.1 b) del RGPD, al ser este necesario para la ejecución del propio contrato de trabajo. Por ejemplo, Delgado Martín (2021, p. 1), en el contexto del tratamiento de la huella dactilar para control horario, afirma que este sería lícito ya que es necesario para la ejecución del contrato de trabajo (argumento que podría extenderse fácilmente a cualquier otro dato biométrico). Pero no estamos de acuerdo con su tesis, pues entendemos que el tratamiento de datos biométricos, como es el caso concreto de la huella dactilar, con fines de autenticación o identificación no es, ni mucho menos, necesario para la ejecución del contrato de trabajo, ya que existen alternativas tecnológicas que no requieren realizar el tratamiento de esta categoría especial de datos personales.

No obstante, podría entenderse que, en el caso de que el fin sea el control de presencia en el ámbito laboral, la base jurídica válida sería el cumplimiento de una obligación legal del responsable del tratamiento (art. 6.1 c) RGPD), en concreto, la establecida en el artículo 34.9 del ET, relativo a la obligación del registro de jornada.

Y, por otra parte, cuando se trate de controles de acceso, también en el ámbito laboral, sería posible argumentar que podría justificarse su licitud con base en el artículo 6.1 f) del RGPD (satisfacción de intereses legítimos del responsable del tratamiento) en relación con el poder de organización y control del empresario ex artículo 20.3 del ET.

Sin embargo, es preciso realizar algunas matizaciones importantes respecto de los dos párrafos anteriores.

Es cierto que, cuando el levantamiento de la prohibición se ha realizado sobre la base de la existencia de una norma con rango de ley que habilite el tratamiento, dicha norma también justificaría la licitud del tratamiento con base en los artículos 6.1 c) o 6.1 f) del RGPD.

Pero, tal y como ha puesto de manifiesto la AEPD (2023, pp. 21-22), el problema es que no existe en nuestro ordenamiento jurídico una norma con rango de ley que autorice este tratamiento de los datos biométricos con fines de control de presencia o de acceso con carácter general, y tampoco podría levantarse la prohibición basándose en el consentimiento del interesado, al no ser este libre, como hemos visto.

Por ello, solo cabría justificar la licitud del tratamiento mediante el artículo 6.1 c) del RGPD en relación con el artículo 34.9 del ET, o el 6.1 f) del RGPD en relación con el 20.3 del ET, cuando el tratamiento esté expresamente autorizado en un convenio colectivo, opción que, como ya hemos indicado, no consideramos que sea la más recomendable, al poner en riesgo los derechos fundamentales de los trabajadores.

Finalmente, entendemos que, con carácter general, en el ámbito laboral deberá descartarse la justificación de la licitud con base en el artículo 6.1 a) del RGPD (consentimiento del interesado), incluso aunque no se trate de datos de categoría especial, puesto que, como ya hemos visto, el consentimiento del trabajador rara vez va a poder ser prestado libremente.

3.4. Principio de minimización de datos y triple juicio de proporcionalidad

El artículo 5.1 c) del RGPD establece el principio de minimización como un elemento esencial del tratamiento de los datos personales, y sobre la base de este, los datos deben ser adecuados, pertinentes y estrictamente limitados a lo necesario en relación con los fines para los que son tratados (este principio se aplica a todos los datos personales, aunque no sean de categoría especial).

Por ello, no es posible extender el tratamiento a datos que no resulten necesarios para lograr la finalidad buscada, de forma que no deben tratarse si los objetivos del tratamiento pueden lograrse razonablemente por otros medios (considerando 39 RGPD), y todo esto se debe garantizar desde el diseño y por defecto, teniendo en cuenta, además, los riesgos del tratamiento en relación con los derechos y libertades de los individuos ex artículo 25.1 del RGPD (AEPD, 2023, p. 7).

Pero el principio de minimización no solo se limita a la obligación de tener que utilizar los datos personales mínimos indispensables para alcanzar el fin del tratamiento (eligiendo en su caso cualquier alternativa que no utilice datos personales), sino que también implica que, si una determinada finalidad puede alcanzarse sin realizar el tratamiento de categorías especiales de datos, esta opción debe prevalecer frente a otras que sí lo requieran (APDCAT, 2022, p. 11).

Además, también es necesario garantizar, y muy especialmente cuando el tratamiento se proyecte sobre datos de categoría especial, y de acuerdo con la doctrina del TC (STC 39/2016, FJ 5.º), que el tratamiento se ajusta al principio de proporcionalidad, debiéndose superar, para ello y con carácter previo al tratamiento, el triple juicio de proporcionalidad (Navalón Arnal, 2025, p. 28; Montesdeoca Suárez, 2024, pp. 141-142): a) juicio de idoneidad; b) juicio de necesidad; c) juicio de proporcionalidad en sentido estricto.

En primer lugar, para superar el juicio de idoneidad, la medida debe ser susceptible de conseguir el objetivo propuesto, esto es, que el tratamiento pueda realmente lograr los fines buscados utilizando esos datos personales.

En segundo lugar, se superará el juicio de necesidad cuando no exista otra medida más moderada para la consecución de tal propósito con igual eficacia. Y coincidimos con Navalón Arnal (2025, pp. 21 y 28), que afirma que no debe confundirse necesidad con utilidad y que las tecnologías biométricas no cumplen el requisito de necesidad del principio de proporcionalidad.

Por otra parte, entendemos que tampoco bastaría con una supuesta mejora en la seguridad del sistema (evitación de fraudes), pues si bien es cierto que la utilización de datos biométricos evita el riesgo de suplantación, no es el único sistema que permite hacerlo. Por ejemplo, cuando se asocia la tarjeta a una contraseña personal junto con la existencia de personal de seguridad en el punto de fichaje (físicamente o bien con observación mediante sistemas de videovigilancia), el sistema puede ser igual de eficaz frente a la suplantación, sin que resulte necesario el tratamiento de datos biométricos. Así lo considera la APDCAT (2022, p. 11), con la que estamos de acuerdo.

Y finalmente, en tercer lugar, para vencer el juicio de proporcionalidad en sentido estricto la medida debe ser ponderada o equilibrada, esto es, que de la misma se deriven más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto. Para ello, deberá evaluarse el alcance del riesgo sobre los derechos y libertades de los trabajadores que el tratamiento provoca, en contraposición con las ventajas o beneficios asociados al mismo, teniendo en cuenta que no basta con que exista una mayor comodidad o un ligero ahorro asociado al tratamiento de datos biométricos para superar este último juicio.

3.5. Cumplimiento del resto de requisitos del RGPD

Cualquier tratamiento de datos personales, aunque estos no sean de categoría especial, deberá cumplir todos los principios y obligaciones establecidos en el RGPD, y ello deberá justificarse también en la EIPD antes del inicio del tratamiento cuando sea necesario realizarla.

Con carácter general, se deberán cumplir todos los principios aplicables al tratamiento de los datos personales (art. 5.1 RGPD): minimización de datos y proporcionalidad (que ya hemos visto), licitud, lealtad y transparencia, limitación a la finalidad, exactitud, limitación del plazo de conservación, integridad y confidencialidad, calidad de los datos, responsabilidad proactiva del responsable del tratamiento, etc. (Sierra Hernáiz, 2021. p. 27). Además, sería aconsejable que el tratamiento se ajustara a los principios previstos en la Recomendación CM/Rec(2015)5 del Consejo de Europa, relativa al tratamiento de datos personales en el ámbito laboral (Sierra Hernáiz, 2021. p. 40).

También, en el caso de que el tratamiento vaya a dar lugar a decisiones automatizadas, deberá justificarse el cumplimiento del artículo 22.4 del RGPD, y como en la práctica totalidad de los casos actualmente se utiliza IA para llevar a cabo estas decisiones automáticas, adicionalmente será preciso justificar que se han cumplido las previsiones contempladas en el RIA, como ya comentamos en la primera parte del presente trabajo.

3.6. Evaluación de riesgos y garantías organizativas, técnicas y jurídicas

La EIPD deberá incluir una evaluación de riesgos, en la que, además de indicar los diferentes riesgos asociados al tratamiento, se deberá establecer su valoración asociada a la gravedad (consecuencias que puede tener), probabilidad y el nivel de riesgo antes y después de aplicar las medidas para minimizarlos.

De forma no exhaustiva, algunos de los riesgos más comunes que se deben incluir son los siguientes: riesgo de vulneración de los distintos derechos fundamentales, riesgo de discriminación, riesgo de pérdida de confidencialidad, riesgo de suplantación de identidad, riesgo de daño reputacional, riesgo de pérdida de control sobre los datos, riesgos psicosociales, etc.

También deberán indicarse todas las medidas y garantías, organizativas, técnicas y jurídicas, que vayan a implantarse para minimizar esos riesgos, con el objetivo de evitar que el tratamiento se traduzca en vulneraciones inadmisibles de los derechos de los trabajadores. Estas medidas y garantías deberán contemplarse desde el diseño y por defecto.

A título ejemplificativo y sin ánimo de exhaustividad, las medidas que se deberían implantar podrían ser algunas de las indicadas a continuación, la mayor parte recomendadas por la AEPD (2023, pp. 28 y 30), aunque hemos incluido algunas medidas adicionales: optar por sistemas de autenticación biométrica evitando la identificación siempre que sea posible, que las plantillas biométricas estén almacenadas en dispositivos bajo el exclusivo control de los usuarios (por ejemplo, en una tarjeta con chip) evitando almacenamientos centralizados o en la nube, imposibilidad de reversión (que no sea posible obtener el dato biométrico a partir de la plantilla), posibilidad de revocar el vínculo entre la plantilla biométrica y la persona física en cualquier momento, asegurar la imposibilidad del uso de las plantillas biométricas para otros propósitos, no permitir la interconexión de la base de datos biométrica con otras bases de datos, garantizar que la toma de datos se realice de forma consciente por el trabajador realizando alguna acción positiva para iniciarla, implantar fecha de caducidad en los datos biométricos y mecanismos automáticos de supresión, cifrado robusto de las plantillas biométricas, seudonimización de los datos siempre que sea posible, informar a los usuarios sobre el tratamiento y sus riesgos y garantizarles una for-

mación adecuada que se actualice periódicamente, implantar auditorías externas periódicas y mecanismos de supervisión, etc.

Siempre que sea posible, deberían incluirse estas medidas y garantías en los convenios colectivos, a tenor del artículo 91 de la LOPDGDD, algo que entendemos que sería obligatorio en el caso de que el levantamiento de la prohibición general del tratamiento se haya sustentado en la autorización expresa del mismo mediante un convenio colectivo (art. 9.2 b) RGPD).

Por último, consideramos que todas las medidas y garantías implantadas deberán revisarse y actualizarse periódicamente y siempre que sea necesario por algún cambio en las mismas, en las características del tratamiento, o bien porque se haya producido un incidente o una brecha de seguridad, revisando, para ello, la EIPD. De hecho, la AEPD (2025, p. 8) defiende, *de lege ferenda*, que la evaluación de impacto debería actualizarse cada cuatro años o siempre que se produzcan incidentes relevantes o modificaciones sustanciales del tratamiento, propuesta con la que coincidimos.

3.7. Otras cuestiones para tener en cuenta en la evaluación de impacto

Finalmente, en la EIPD deberá hacerse referencia a cualquier otra circunstancia que pueda afectar al tratamiento o a sus consecuencias, por ejemplo, las siguientes:

Implementación: ha de tenerse en cuenta la forma concreta de implementación del sistema, pues puede dar lugar a la aparición de riesgos adicionales, por ejemplo, transferencias internacionales de datos cuando no existan garantías adecuadas en el caso de que los datos en la nube se almacenen fuera de la UE.

Contexto del tratamiento: se deberá evaluar el contexto en el cual se realiza el tratamiento, puesto que también puede tener importantes consecuencias en los riesgos.

Brechas de datos personales: el responsable del tratamiento deberá plantear posibles escenarios de brechas de seguridad, para implementar garantías que minimicen su probabilidad y los eventuales impactos. Como mínimo, filtrado o pérdida de patrones, uso malicioso de patrones, intrusión en el sistema, interceptación, *DoS* (*Denial of Service*) o *DDoS* (*Distributed Denial of Service*), discontinuidad del servicio, etc.

Subcontratación de trabajadores: si existiera subcontratación, es preciso evaluar el cumplimiento de todos los requisitos que hemos visto también respecto de los trabajadores de la empresa subcontratada, pues en caso contrario no será posible realizar el tratamiento de sus datos personales.

4. Conclusiones y propuesta final

Consideramos que, con carácter general, no será posible llevar a cabo el tratamiento de datos biométricos en el ámbito laboral para realizar controles de acceso o de presencia, por aplicación de los principios de minimización y de proporcionalidad, puesto que normalmente existirán alternativas asimismo eficaces para lograr esos fines que no requieran la utilización de datos biométricos, por lo que difícilmente se superará el juicio de necesidad.

Adicionalmente, entendemos que no existe actualmente una base jurídica adecuada para levantar la prohibición general del tratamiento de los datos biométricos, puesto que no cabe el consentimiento del interesado, ya que este no puede otorgarse libremente al existir un desequilibrio entre empresario y trabajador, ni tampoco existe en el ordenamiento jurídico español una norma con rango de ley que autorice expresamente este tratamiento, y en cuanto a la habilitación del mismo mediante un convenio colectivo, no consideramos que sea una vía adecuada para garantizar la protección de los derechos fundamentales de los trabajadores, es más, existe un riesgo importante de que, si se utiliza, se torne en una herramienta que permita legitimar la vulneración de estos derechos.

Tampoco consideramos que la nueva excepción prevista en la propuesta de reforma legislativa actualmente en tramitación en la UE, «Ómnibus digital», relativa a los sistemas de autenticación biométrica, si finalmente es aprobada con su redacción actual, vaya a poder ser aplicada de forma generalizada para levantar la prohibición del tratamiento de los datos biométricos de los trabajadores en el ámbito laboral, pues entendemos que difícilmente se cumplirá el requisito de necesidad en la práctica totalidad de los casos.

Además, si empezáramos a admitir algunos tratamientos de datos biométricos que puedan parecernos razonables o de poco riesgo, iremos acostumbrándonos poco a poco a estos tratamientos y acabaremos normalizándolos. Esto moverá la ventana de Overton, haciendo que cada vez sean aceptados sistemas más peligrosos que finalmente acabarán vulnerando gravemente los derechos fundamentales de los trabajadores o vaciándolos de contenido.

Por todo ello, y con el objetivo de conseguir una mayor seguridad jurídica y una adecuada protección de los derechos de los trabajadores, minimizando los riesgos presentes y futuros, proponemos, *de lege ferenda*, que se incluya, tanto en el ET como en el EBEP, o mejor aún, en la LOPDGDD, una prohibición expresa de la utilización de datos biométricos para llevar a cabo controles de acceso o de presencia en el ámbito laboral, salvo en aquellas situaciones específicas y concretas que estén expresamente autorizadas en una norma con rango de ley que establezca garantías adecuadas para la protección de los derechos fundamentales de los trabajadores¹¹.

¹¹ Coincidimos, en esencia, con Navalón Arnal (2025, p. 20), que aboga por introducir una prohibición expresa de tratamiento de los datos biométricos con fines de control horario en el ámbito laboral, si bien

Referencias bibliográficas

- AEPD. (2023). *Guía sobre tratamientos de control de presencia mediante sistemas biométricos*. Agencia Española de Protección de Datos. <https://www.aepd.es/guias/guia-control-presencia-biometrico.pdf>
- AEPD. (2025). Consulta Previa (Art. 36 RGPD). Ref. REGAGE25e00024730156. Agencia Española de Protección de Datos. <https://www.aepd.es/documento/regage25e00024730156.pdf>
- APDCAT. (2022). *Dictamen en relación con la consulta formulada por un Ayuntamiento relativa a la conformidad con la normativa de protección de datos del uso de dispositivos de control de presencia en el puesto de trabajo mediante reconocimiento facial*. Autoridad Catalana de Protección de Datos. <https://seu.apdcat.cat/ca/documentPublic/download/4727>
- Bailey, M. (2018). The hidden data in your fingerprints. *Scientificamerican*. <https://www.scientificamerican.com/article/the-hidden-data-in-your-fingerprints/>
- Barona Vilar, S. (2024). Tecnología biométrica y datos biométricos. Bondades y peligros. No todo vale. *Actualidad jurídica iberoamericana*, 21, 298-331. <https://producciocientifica.uv.es/documentos/66c38db00bd02a62166084fb>
- CEPD. (2023). *Directrices 5/2022 sobre el uso de la tecnología de reconocimiento facial en el ámbito de la aplicación de la ley*. Comité Europeo de Protección de Datos. https://www.edpb.europa.eu/system/files/2024-05/edpb_guidelines_202304_frtlawenforcement_v2_es.pdf
- Cruz Villalón, J. (2020). El impacto de la digitalización sobre los derechos fundamentales laborales. En M. Rodríguez-Piñero Royo y A. Todolí Signes (Coords.), *Vigilancia y control en el Derecho del Trabajo Digital* (pp. 35-67). Thomson Reuters Aranzadi.
- CTPDA. (2023). *Dictamen 1/2023. Relativo al tratamiento de categorías especiales de datos biométricos mediante el uso de dispositivos de reconocimiento facial y/o huella dactilar para el control horario del personal de un Ayuntamiento, de conformidad con la normativa de protección de datos*. Consejo de Transparencia y Protección de Datos de Andalucía. <https://www.ctpdandalucia.es/sites/default/files/inline-files/dictamen-1-2023.pdf>
- Delgado Martín, J. (2021). Notas sobre datos biométricos en las relaciones laborales: sistema de control horario mediante huella dactilar. *Diario La Ley*, 50, 1-3.
- Fernández Orrico, F. J. (2020). Límites a la biometría como medio de identificación y control de los trabajadores: necesidad de su regulación. En M. Rodríguez-Piñero Royo y A. Todolí Signes (Coords.), *Vigilancia y control en el Derecho del Trabajo Digital* (pp. 301-326). Thomson Reuters Aranzadi.
- González Mendoza, D. P. (2025). Los datos biométricos y las tecnologías que los utilizan para su funcionamiento. *Revista Vasca de Administración Pública*, 132, 427-464. <https://doi.org/10.47623/ivap-rvap.132.2025.12>

consideramos que la prohibición debería extenderse también al control de acceso y admitir excepciones para casos muy concretos siempre que vengan expresamente establecidas en una norma con rango de ley que prevea garantías adecuadas (por ejemplo, para instalaciones militares o policiales de alta seguridad).

- González San Juan, J. L. (2022). Vídeos *deepfakes* y sus problemas jurídicos. En A. Madrid Parra y L. Alvarado Herrera (Dirs.), *Derecho digital y nuevas tecnologías* (pp. 593-614). Thomson Reuters Aranzadi.
- Mercader Uguina, J. R. (2020). Datos biométricos en los centros de trabajo. *Trabajo y Derecho: nueva revista de actualidad y relaciones laborales*, Extra-11, 1-23. <https://e-archivo.uc3m.es/rest/api/core/bitstreams/4b68f997-5533-4ce5-bb51-d33be97e2b74/content>
- Mercader Uguina, J. R. (2024). El «Big Bang» de la biometría laboral. De la huella dactilar a los neurodatos. *Labos: Revista de Derecho del Trabajo y Protección Social*, 5(2), 4-23. <https://doi.org/10.20318/labos.2024.8749>
- Montesdeoca Suárez, A. (2024). El *software* de reconocimiento facial como instrumento de control de la jornada laboral: la incidencia de la tecnología en los derechos fundamentales de las personas trabajadoras. *Revista Electrónica de Direito. RED*, 33(1), 128-146. https://doi.org/10.24840/2182-9845_2024-0001_0006
- Montesdeoca Suárez, A. (2026). La extinción del contrato por incumplimiento grave de la empresa. Vulneración del derecho a la propia imagen y a la protección de datos personales por el uso del registro biométrico de jornada. Comentario a la Sentencia del Tribunal Superior de Justicia de Galicia 144/2026, de 15 de enero. *Revista de Trabajo y Seguridad Social. CEF*, 492, 166-172. <https://doi.org/10.51302/rtss.2026.25029>
- Muñoz Ruiz, A. B. (2023). *Biometría y sistemas automatizados de reconocimiento de emociones: implicaciones jurídico-laborales*. Tirant lo Blanch.
- Muñoz Ruiz, A. B. (2024). Datos biométricos y control horario de los empleados: la nueva Guía de la Agencia Española de Protección de Datos. *La Ley Privacidad*, 19, 1-5.
- Navalón Arnal, A. (2025). Datos biométricos y registro horario: el principio de necesidad y el papel de la negociación colectiva. *Revista de Trabajo y Seguridad Social. CEF*, 487, 17-52. <https://doi.org/10.51302/rtss.2025.24427>
- Rodríguez Pérez, M. C. (2025). Trabajo, derechos y algoritmos: la inteligencia artificial como reto para el derecho del trabajo. *Revista de Trabajo y Seguridad Social. CEF*, 489, 45-76. <https://doi.org/10.51302/rtss.2025.24581>
- Rodríguez-Piñero Royo, M. (2019). Las facultades de control de datos biométricos del trabajador. *Temas laborales: Revista andaluza de trabajo y bienestar social*, 150, 91-109. <https://dialnet.unirioja.es/descarga/articulo/7224369.pdf>
- Río García, M. D. (2024). El tratamiento de datos biométricos requiere algo más que el consentimiento de los empleados públicos. *La Ley Privacidad*, 20, 1-6.
- Sierra Hernáiz, E. (2021). *Las categorías especiales de datos del trabajador. Estudio de los límites y garantías legales para su tratamiento en la relación laboral*. Thomson Reuters Aranzadi.

José Luis González San Juan. Doctor en Derecho Privado (USAL, 1919) e Ingeniero de Telecomunicaciones (UPM, 1991). Trabaja principalmente como ingeniero de telecomunicaciones desde 1991 hasta la actualidad, compaginándolo con el ejercicio como abogado litigante desde finales de 2014, también hasta la actualidad, y ocasionalmente como profesor titular en diversas instituciones (Ayuntamiento de Salamanca, Facultad de Informática de la UPSA y Escuela de Transmisiones del Ejército del Aire). Publicaciones: 1 monografía, 17 artículos en revistas y 10 colaboraciones en obras colectivas. <https://orcid.org/0000-0002-0613-7302>