# LA DOBLE FINALIDAD DE LOS DATOS BIOMÉTRICOS DE LAS PERSONAS TRABAJADORAS EN LA RELACIÓN LABORAL: EL REGISTRO DE JORNADA Y EL CONTROL DE PRESENCIA

## COMENTARIO A LA SENTENCIA DEL JUZGADO DE LO SOCIAL N.º 3 DE A CORUÑA 370/2025

Arturo Montesdeoca Suárez
Profesor Ayudante Doctor
Universidad de Las Palmas de Gran Canaria

***Abstract***

El juzgado de lo Social n.º 3 de A Coruña resuelve la controversia suscitada en torno a la licitud del uso de un sistema de control biométrico mediante huella dactilar implantado por una empresa del sector servicios, a raíz de la demanda interpuesta por la Confederación Intersindical Galega y el Comité de Empresa. El órgano judicial examina la habilitación legal que permite a la empresa efectuar un control horario y un control de presencia mediante el uso de datos biométricos como la huella dactilar. En este sentido, se analizan las bases de legitimación previstas en el marco normativo sobre protección de datos personales respecto al tratamiento de datos biométricos en el ámbito laboral y la lesividad en este derecho fundamental de las personas trabajadoras.

*The Labour Court n.º 3 of A Coruña resolves the dispute concerning the lawfulness of using a biometric fingerprint control system implemented by a company in the services sector, following a claim filed by the Galician Inter-Union Confederation and the Works Council. The court examines the legal basis that enables the employer to carry out working time recording and attendance control through the use of biometric data, such as fingerprints. In this regard, the judgment analyses the grounds for lawful processing established under the personal data protection framework in relation to the processing of biometric data in the employment context, as well as the potential infringement of this fundamental right of employees.*

*Title: The dual purpose of employees' biometric data in the employment relationship: working time recording and attendance control. Commentary on Judgment 370/2025 of the Labour Court n.º 3 of A Coruña.*

Palabras clave: Protección de datos personales; datos biométricos; registro de jornada; control de presencia; finalidad; legitimación; consentimiento.

*Keywords: Personal data protection; biometric data; working time recording; attendance control; purpose; legal basis; consent.*

IUSLabor 1/2026, ISSN 1699-2938, p. 91-111
DOI. 10.31009/IUSLabor.2026.i01.03

Fecha envío: 10.11.2025 | Fecha aceptación: 15.02.2026 | Fecha publicación: 31.03.2026

***Sumario***

## 1. Introducción

La implantación de sistemas biométricos en el ámbito laboral ha ido posicionándose como uno de los debates de interés en materia de gestión empresarial adquiriendo un protagonismo singular en la actualidad. Tras la reforma operada por el Real Decreto-ley 8/2019[1], que impuso la obligación[2] de registro horario en el artículo 34.9 del 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), numerosas empresas han adoptado sistemas de control basados en huella dactilar, reconocimiento facial u otros identificadores biométricos. Sin embargo, la utilización de estos sistemas plantea tensiones entre el poder de dirección empresarial (artículo 20 ET) y los derechos fundamentales a la intimidad y protección de datos personales consagrados en los artículo 18 de la Constitución Española, artículo 8 del Convenio Europeo de Derechos Humanos y el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea).

El cumplimiento de la obligación legal impuesta en el artículo 34.9 ET sobre el registro de jornada conlleva un tratamiento de datos personales. Un tratamiento de datos personales consiste en *"cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción" ex* artículo 4.2 RGPD. Así, esta obligación deviene de la definición "dato personal" aportada por el artículo 4.1 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD) como *"toda información sobre una persona física identificada o identificable"*. Para a continuación referirse al titular de

Este trabajo se ha realizado en el marco del proyecto de investigación: "Inteligencia artificial y garantía de la privacidad de las personas trabajadoras: políticas empresariales y ejercicio de los derechos digitales laborales" (AIPRIVACYLAB), Referencia: PID2024-157896OB-I00. Ministerio de Ciencia, Innovación y Universidades (España). Programa Estatal para la Investigación y el Desarrollo Experimental del Plan Estatal de Investigación Científica, Técnica y de Innovación 2024-2027. Investigador principal: José Eduardo López Ahumada.

[1] TRILLO PÁRRAGA, Francisco, "Registro de jornada diaria efectiva: un paso adelante en el control del tiempo de trabajo (Sentencia Audiencia Nacional 207/2015, de 4 de diciembre, Rec. 301/2015)", *Diario La Ley*, n.º 8875, 2016.

[2] Sobre el debate jurisprudencial que derivó en la reforma, vid., MIÑARRO YANINI, Margarita, "Más allá de las horas extras: la obligatoriedad del registro de la jornada diaria (Comentario a la Sentencia de la Audiencia Nacional 25/2016, de 19 de febrero)", *Revista de Trabajo y Seguridad Social – CEF*, n.º 397, 2016; PRECIADO DOMÈNECH, Carlos Hugo, "El registro de la jornada ordinaria en la nueva doctrina del TS (Comentario a la STS 23 de marzo de 2017, RCUD 81/2016)", *Revista de Información Laboral*, n.º 7, 2017.

estos datos, es decir, al interesado como *"persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona"*.

Por otro lado, la empresa actúa en calidad *de "responsable del tratamiento de datos personales"*, es decir, aquella *"persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros"*, *ex* artículo 4.7 RGPD. El ejercicio de estas funciones como responsable del tratamiento de datos personales se prevén específicamente en el artículo 24 RGPD y 33 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. (LOPDGDD).

En materia de registro de jornada, la empresa lleva a cabo un tratamiento de datos en base al cumplimiento de una obligación legal, en este caso, el registro de jornada *ex* artículo 34.9 ET[3]. A raíz del Real Decreto-ley 8/2019, con la modificación del artículo 34.9 ET, la empresa debe garantizar el registro diario de la jornada, aunque sin prever o señalar un método exclusivo para cumplir este cometido. Por todo ello, el registro de jornada implica un tratamiento de datos personales *ex* artículo 4 RGPD al concretar, como mínimo, las horas de entrada y salida de las personas trabajadoras[4]. Sobre la condición de dato personal de la información contenida en el registro de jornada, la sentencia de 30 de mayo de 2013, asunto C-342/12 (*Worten*), el TJUE señaló que *"el artículo 2, letra a), de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, debe interpretarse en el sentido de que un registro del tiempo de trabajo, como el controvertido en el litigio principal, que incluye la indicación de las horas en que cada trabajador inicia y finaliza la jornada, así como de las pausas o períodos de descanso correspondientes, queda comprendido en el concepto de datos personales a efectos de dicha disposición"*.

La lectura del artículo 34.9 ET permite comprobar que la opción legislativa no ha sido seleccionar un método concreto de registro de jornada, sino dejar un espacio a la

[3] GONZÁLEZ GONZÁLEZ, Carlos, *Registro de la jornada y problemas en la determinación de la jornada efectiva de trabajo*, Pamplona, Aranzadi, 2020, p. 146.

[4] SERRANO GARCÍA, Juana María, *La protección jurídica de los datos de las personas trabajadoras*, Albacete, Bomarzo, 2022, p. 45.

negociación colectiva a fin de concretar y adaptar esta obligación legal conforme a las características del sector o empresa en cuestión. Una situación que, por el momento, contrasta con las propuestas de cambio que el Ministerio de Trabajo y Economía Social con apoyo de los sindicatos quiere implementar[5]. Se está haciendo referencia a la implementación de un registro de jornada, esta vez sí, con carácter exclusivamente digital. En esta propuesta progresista sí que se opta por concretar el método -digital- así como el cumplimiento de unos caracteres intrínsecos mínimos del sistema elegido para cumplir con esta obligación legal.

Pese a que la opción digital ofrezca una lectura de bondades y comodidades por las propias características de la tecnología, ello no puede desconocer otras consecuencias negativas[6]. La elección de uno u otro sistema de registro de jornada, en función de la mayor o menor lesividad para los derechos fundamentales de las personas trabajadoras también podrá conllevar una mayor o menor responsabilidad para la empresa como responsable del tratamiento de datos personales[7]. De acuerdo con la Agencia Española de Protección de Datos (AEPD)[8] el derecho a la protección de datos personales no limita las opciones de una empresa en relación con el sistema de registro horario ya que la base jurídica es la citada obligación legal y no el consentimiento de las personas trabajadoras[9]. Ello no obsta a que se priorice -conforme al espíritu del RGPD- por el sistema menos invasivo posible. En todo caso, las personas trabajadoras tendrán derecho a ser informadas y, en su caso, a ejercitar los derechos de acceso, rectificación, oposición y supresión, con independencia de que el registro sea más o menos sofisticado.

La empresa debe cerciorarse en que el registro de jornada no debe incluir más datos personales que los imprescindibles de conformidad con el principio de minimización *ex* artículo 5.1 c) RGPD. Además, los datos del registro de jornada no pueden ser utilizados con finalidades distintas al control de la jornada de trabajo en cumplimiento del principio de limitación de la finalidad, artículo 5.1 b) RGPD.

---

[5] Esta propuesta ha sido modificada y ampliada desde su firma en el proyecto de reducción de jornada semanal firmado el 20 de diciembre de 2024 por el Gobierno y los sindicatos UGT y CCOO. Esta nueva versión se encuentra en el Real Decreto por el que se desarrolla el texto refundido de la Ley del Estatuto de los Trabajadores en materia de registro de jornada.

[6] MUÑOZ RUÍZ, Ana Belén, *Biometría y sistemas automatizados de reconocimiento de emociones: implicaciones jurídico-laborales*, Valencia, Tirant lo Blanch, 2023, p. 101 y siguientes.

[7] MARCOS HERRERO, José Antonio, "La protección de datos personales de los empleados en el registro de la jornada y los denominados 'derechos digitales'", *Revista Derecho Social y Empresa*, n.º 11, 2019, p. 50.

[8] AEPD, *Guía sobre la protección de datos en las relaciones laborales*, 2025, p. 35-36.

[9] SERRANO GARCÍA, Juana María, *La protección de datos y la regulación de las tecnologías en la negociación colectiva y en la jurisprudencia*, Albacete, Bomarzo, 2019, p. 25.

En consonancia con el tipo de sistema de registro de jornada utilizado, la empresa debe operar desde el cumplimiento de los parámetros de diseño y defecto adoptando las medidas de seguridad que correspondan *ex* artículo 24 RGPD[10]. Deberá evitarse el acceso de personas no autorizadas, inclusive las propias personas trabajadoras si ese acceso permite comprobar datos de otros compañeros.

Las empresas podrán apoyarse en el asesoramiento del delegado de protección de datos (DPD), ya que debería estar presente en todo el ciclo de vida de la documentación vinculada con el registro horario, desde el asesoramiento a la dirección de la empresa para la confección y custodia de esta documentación, la resolución de incidencias que se puedan plantear internamente, hasta la función de interlocución con la AEPD.

Una de las opciones utilizadas en la práctica por las empresas para cumplir con la obligación legal del registro de jornada ha sido la utilización de los datos biométricos. Sobre la discusión en torno a la mayor o menor lesividad, así como las características biométricas, el Instituto Nacional de Ciberseguridad (INCIBE), ha señalado las siguientes: universalidad, ya que todas las personas disponen de ellas; singularidad o univocidad puesto que permiten distinguir a cada individuo; permanencia en el tiempo y en distintas condiciones ambientales; y medibles de forma cuantitativa. Para llevar a cabo este procesamiento de datos personales biométricos, se requieren varios pasos. Así, el INCIBE concreta que este proceso es progresivo y consecutivo: primero se lleva a cabo una captura de tales parámetros biométricos, posteriormente se procesan creando una plantilla biométrica y, por último, se inscribe la plantilla biométrica guardándola en un medio adecuado para efectuar el fin previsto. Por ende, la tecnología biométrica permite a través de procesos automáticos digitales emplear datos personales (huella dactilar, reconocimiento facial, del iris o la voz) a fin de efectuar una verificación o autenticación con fines de verificar y acreditar que una persona es quien dice ser.

En esta ocasión, se ha seleccionado la sentencia del Juzgado de lo Social n.º 3 de A Coruña 370/2025, puesto que dilucidado sobre la licitud del uso de un sistema de control biométrico de huella dactilar implantado por una empresa del sector servicios, a raíz de demanda conjunta de la Confederación Intersindical Galega y el Comité de Empresa. Su análisis constituye una buena oportunidad para adentrarse en la distinción de los conceptos control horario y control de presencia desde la óptica normativa. Con ello, se pretende examinar los parámetros legales -en concreto, sobre las bases de legitimación- que tanto el Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia

[10] LLORENS ESPADA, Julen, "El interés legítimo de la empresa como base de licitud para el tratamiento de datos personales de la persona trabajadora", *Documentación Laboral*, vol. II, n.º 126, 2022, p. 40-41.

artificial (RIA), RGPD y la LOPDGDD prevén sobre el uso de datos biométricos en el entorno laboral.

## 2. Hechos probados

En cuanto a los hechos probados, la empresa, Instituto Policlínico Santa Teresa, S.A., dedica su actividad a la prestación de servicios médicos y sanitarios en A Coruña. Antes de la entrada en vigor del Real Decreto-ley 8/2019, de 8 de marzo, la empresa implantó un sistema de control de acceso y registro de jornada, que fue comunicado tanto al Comité de Empresa como al conjunto de las personas trabajadoras mediante correos electrónicos de 13 de mayo y 24 de julio de 2019, sin que se registraran conflictos o impugnaciones.

Durante la pandemia del COVID-19, concretamente el 16 de marzo de 2020, la empresa comunicó al Comité de Empresa la suspensión temporal del fichaje presencial, dada la situación sanitaria. El Comité respondió el 18 de marzo de 2020, manifestando su conformidad con la medida, entendiendo que era una decisión excepcional y necesaria derivada de la emergencia sanitaria, y que no requería acuerdo formal del órgano de representación. Posteriormente, mediante escrito de 9 de noviembre de 2021, el Comité solicitó la reactivación del sistema de registro de jornada. Sobre la reanudación en el cumplimiento de esta obligación, en la reunión celebrada el 11 de noviembre de 2022, la empresa explicó que la implantación del nuevo sistema se había retrasado por trámites de adquisición y por la imposibilidad técnica de trasladar las huellas del sistema anterior al nuevo dispositivo biométrico.

Ante tales hechos, es decir, la falta de registro horario efectivo, el Comité denunció la situación ante la Inspección de Trabajo el 20 de mayo de 2022. Como resultado, el 11 de octubre de 2022, la Inspección emitió acta de requerimiento, ordenando a la empresa implantar un sistema de registro de jornada que cumpliera los criterios de objetividad, fiabilidad y accesibilidad exigidos por el artículo 34.9 del ET.

Consta en autos un informe técnico emitido el 3 de junio de 2025 por el DPD y ratificado en su declaración testifical, que evalúa los riesgos asociados a distintos sistemas de control. En dicho documento se concluye que el sistema biométrico presenta un riesgo muy bajo de suplantación de identidad y ofrece una mayor eficacia y fiabilidad frente a otros métodos de registro.

Asimismo, obra en autos un informe técnico de 20 de noviembre de 2024, firmado por el Director del departamento de personas y organización, sobre el sistema biométrico para control de presencia con turnos, en el que se detallan las medidas de seguridad aplicadas, entre las que destacan: el uso de plantillas biométricas no interoperables, imposibles de

emplear fuera del dispositivo, la implantación de un sistema de protección contra la manipulación denominado *Secure Tamper*, los datos se eliminan automáticamente si el dispositivo se retira o manipula, la gestión automatizada de registros y eliminación de datos se realiza conforme al RGPD y se lleva a cabo una encriptación completa de la información y certificaciones ISO 27001 e ISO 27701 sobre seguridad y gestión de privacidad.

Además, consta que la empresa consultó a la Agencia Española de Protección de Datos (AEPD) sobre la idoneidad del sistema biométrico de registro de jornada, mediante dos escritos de fecha 11 de enero y 16 de abril de 2024.

Por la parte actora se ejercita una acción de tutela de derechos fundamentales ya que el sistema de registro de jornada con carácter biométrico -huella dactilar- incumple el marco jurídico actual en materia de protección de datos personales. En concreto, señala que se han vulnerado el derecho a la intimidad *ex* artículo 18.1 CE y privacidad *ex* artículo 18.4 CE, el derecho a la libertad sindical *ex* artículo 28 CE y el derecho a la salud *ex* artículo 43 CE. La argumentación se apoya, por un lado, con el criterio del Comité Europeo de Protección de Datos - Directrices 5/2022 sobre el uso de la tecnología de reconocimiento facial en el ámbito de la aplicación de la ley. En suma, este criterio es respaldado por la AEPD ya que en su Guía sobre la utilización de datos biométricos para el control de presencia y acceso, se prevé que *"las personas empleadoras deben utilizar otros sistemas de fichaje que no almacenen ni traten con datos biométricos de las personas empleadas; el consentimiento de la persona empleada no es suficiente para que el fichaje biométrico sea una práctica que respete la privacidad y la legalidad; para levantar la prohibición de tratar los datos biométricos las personas responsables deben contar con tanto de ley que concrete la posibilidad de emplear dicha información biométrica con fines laborales, la cual no se encuentra en la actual normativa española"*. Además, señalan que esta obligación legal impuesta a las empresas puede cumplirse por otros medios o dispositivos de carácter no biométrico como pueden ser los lectores de tarjetas *NFC*, llamadas telefónicas, *app* móvil con posibilidad de geolocalización, lectura de *TAGs* desde el móvil, lectura de códigos *QR*, etc.

Mientras que, por el contrario, a juicio de la demandada, se interesa la desestimación de la demanda por cuanto considera que *"pues niega los hechos alegados de contrario, toda vez que existe normativa para aplicación del sistema de fichar con huella digital y otros sistemas biométricos, tanto a nivel nacional o como a nivel europeo, así como hay otros organismos que a diferencia de la AEPD aceptan la utilización de datos biométricos; y que en el caso presente se ha cumplido con todos los requisitos para su implantación; y en ningún momento se ha vulnerado ningún derecho fundamental"*. Una argumentación

que apoya el MF por cuanto considera que no se ha probado que ningún hecho de la demanda pueda ser constitutivo de vulneración de los derechos fundamentales alegados.

## 3. La fundamentación jurídica del juzgado a debate

El Juzgado de lo Social n.º 3 de A Coruña basa su resolución, principalmente, en tres argumentos que pasan a ser objeto de crítica a continuación.

En primer lugar, el juzgado en apoyo de la argumentación de la parte demandada sostiene que el artículo 34.9 ET impone a todas las empresas la obligación de registrar diariamente la jornada de la plantilla, con el fin de garantizar el cumplimiento de los límites en materia de tiempo de trabajo y descanso. Desde esta perspectiva, considera que dicha obligación constituye una base jurídica suficiente para legitimar el tratamiento de datos personales en el contexto del registro horario, de acuerdo con lo dispuesto en el artículo 6.1.c) RGPD, que permite el tratamiento cuando *"sea necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento"*. De esta forma, el órgano judicial equipara la necesidad de cumplir con la obligación empresarial de registro de jornada con la necesidad de tratar los datos biométricos de la plantilla, entendiendo que ambos supuestos se integran dentro de un mismo fundamento de licitud. En consecuencia, el juzgado no distingue entre la obligación de registrar la jornada—que efectivamente deriva de la norma laboral— y el modo concreto de llevar a cabo dicho registro, asumiendo que cualquier medio técnico elegido por la empresa, incluido el control biométrico, queda automáticamente amparado por la base de legitimación del artículo 6.1.c) RGPD. Esta interpretación, sin embargo, omite la necesaria ponderación entre el cumplimiento de la obligación legal y la elección de un medio que implica el tratamiento de categorías especiales de datos personales, en este caso datos biométricos, lo que exige un análisis de proporcionalidad más estricto y específico conforme al artículo 9 RGPD[11].

En segundo lugar, respecto al criterio de proporcionalidad, el juzgado considera que el sistema de huella dactilar constituye un medio idóneo, necesario y eficaz para garantizar la autenticidad y fiabilidad del registro horario, descartando la utilización de otros métodos como tarjetas magnéticas, claves personales o firmas manuales, que podrían ser objeto de suplantación o manipulación. Desde esta óptica, la resolución valora positivamente la fiabilidad técnica del sistema biométrico, estimando que su implementación responde a una finalidad legítima —asegurar la veracidad del registro horario— y que las medidas de seguridad incorporadas (cifrado de datos, almacenamiento limitado y no interoperabilidad de las plantillas biométricas) resultan suficientes para minimizar los riesgos. El razonamiento judicial se centra, por tanto, en la eficacia

[11] BAZ RODRÍGUEZ, Jesús, *Privacidad y protección de datos de los trabajadores en el entorno digital*, Madrid, Bosch, 2019, p. 247.

tecnológica del sistema más que en su proporcionalidad jurídica. No realiza un análisis completo del principio de minimización (artículo 5.1.c) RGPD), ni del juicio de necesidad en sentido estricto[12] —esto es, si existen medios menos invasivos capaces de cumplir la misma función—, limitándose a afirmar que el método biométrico es más seguro. De esta manera, llega a concluir que *"la utilización de la huella es un dato sensible, pero queda acreditado que el uso de la misma está justificado en un centro hospitalario pues tiene amparo legal. El uso del mismo está justificado, pues se acredita que se trata del uso de una plantilla que no tiene valor identificativo; y que existe un control de su uso, poco evasivo, que está justificado y es idóneo y proporcionado del mismo para la finalidad que se destina"*.

En suma, pone en valor el resultado del análisis de necesidad de la evaluación de impacto, una prueba un tanto incongruente en el fondo en tanto en cuanto si bien el objetivo era respaldar su implementación, no se entiende el valor otorgado a tenor de lo siguiente: *"a pesar que el tratamiento de datos de los empleados tiene asociado un riesgo alto debido al impacto que han determinado los factores de riesgo, existe un plan de tratamiento para su minimización y se han establecido medias técnicas y organizativas que reducen el riesgo inherente"*. Y sobre el control de presencia, detalla la evaluación de impacto que *"se ha verificado el cumplimiento de los principios y obligaciones establecidas en la normativa de protección de datos personales. Esto no ha permitido obtener una visión en detalle que facilita la identificación de las amenazas y los riesgos a los que están expuestos los datos personales asociados al mismo. Siendo el riesgo total acumulado muy alto, se ha realizado un análisis de la idoneidad, necesidad y proporcionalidad del tratamiento. Teniendo en cuenta todo lo anterior, no es necesario realizar la consulta previa del artículo 36 de RGPD a la Agencia Española de Protección de Datos (AEPD), siendo posible el tratamiento, siempre y cuando se observen las medidas de seguridad, así como los principios y obligaciones establecidas en la norma con el fin de garantizar los derechos y libertades de las personas y la seguridad de los datos"*.

En tercer lugar, el fundamento jurídico tercero incide en que la empresa para llevar a cabo implantación del registro de jornada llevó a cabo un proceso informativo tanto con la plantilla como con sus representantes legales, como consta en reuniones con el Comité de Empresa donde se le informa del sistema en fecha 14 y 18 de noviembre de 2022. Un aspecto que no puede pasar desapercibido es que la empresa incluye en los propios contratos unas cláusulas anejas al contrato en las que se les informa sobre el tratamiento de datos personales. Esta información se ha ampliado de forma verbal en cuanto a las características del sistema de registro de jornada con tecnología biométrica, así como con

[12] MERCADER UGUINA, Jesús R., "Datos biométricos en los centros de trabajo", en BAZ RODRÍGUEZ, Jesús (director), *Los nuevos derechos digitales laborales de las personas trabajadoras en España*, 1.ª ed., Madrid, Wolters Kluwer, 2021, p. 185.

carácter permanente en el portal del empleado, donde se les informa sobre el control del cumplimiento de registro de jornada y se les da la posibilidad de pinchar en un enlace sobre más información de datos biométricos. Esta información que parece ser suficiente y conforme a la legalidad vigente a la vista del fallo judicial, prevé que *"es imposible reconstruir una imagen de huella dactilar a partir de una plantilla de huella dactilar que es solo datos numéricos de las características de una huella dactilar, (II) no se almacena ningún tipo de información biométrica de los trabajadores"*. En suma, porque la empresa no almacena la huella digital *"sino determinados puntos de la huella digital, donde existen muchas medidas de seguridad que protegen los datos de carácter personal de los trabajadores y por supuesto cumplen con los límites del principio de conservación de los datos personales"*. E incluso, se incide en que otros sistemas como aquellos basados en la geolocalización pueden llegar a ser más intrusivos que la huella digital.

De hecho, el juzgado se desmarca del criterio de la AEPD respecto a las restricciones a utilizar sistemas de registro biométricos de control de jornada diaria. Para ello, se remite a las consideraciones del Centro Nacional de Protección de Infraestructuras Críticas (CNPIC), que en su recomendación de buenas prácticas habilita a utilizar controles biométricos en los accesos de usuarios[13].

En definitiva, se concluye que el hospital se encuentra legitimado para implementar un sistema de registro de jornada biométrico, en concreto, basado en una huella dactilar a tenor de la excepción prevista en el artículo 9.2 i) RGPD, además de haber superado satisfactoriamente una EIPD.

## 4. La confusión entre control horario y control de presencia: un apunte a las bases de legitimación y la finalidad del tratamiento de datos personales

El elemento central de controversia en la resolución judicial analizada radica en la equivalencia conceptual que el juzgado establece entre el control horario y el control de presencia, equiparación que utiliza como justificación de la base jurídica del tratamiento de datos biométricos. Esta confusión no es meramente terminológica, sino que comporta consecuencias jurídicas significativas, ya que ambas figuras responden a fundamentos normativos y finalidades distintas dentro del marco del poder de dirección empresarial y del derecho fundamental a la protección de datos personales.

[13] En apoyo a esta tesis por el grado mínimo de afectación a la esfera íntima, SELMA PENALVA, Alejandra, "El control de accesos por medio de huella digital y sus repercusiones prácticas sobre el derecho a la intimidad de los trabajadores. Comentario a la STSJ de Murcia, de 25 de enero de 2010", *Revista Doctrinal Aranzadi Social*, n.º 3, 2010.

Por otra parte, en cuanto a las finalidades del tratamiento de datos personales, puede estarse de acuerdo con que los datos biométricos utilizados -control de registro de jornada y de presencia- atienden a *"propósitos o finalidades diferentes".* Por tales motivos, la empresa deberá cumplir para alcanzar dicho propósito una serie de principios y obligaciones derivadas del RGPD[14].

A este respecto, el tratamiento de datos personales deberá llevarse a cabo de manera lícita, leal y transparente *ex* artículo 5.1 a) RGPD; los datos personales obtenidos deben atender a finalidades determinadas, ser explícitos y legítimos de conformidad con el principio de limitación del tratamiento *ex* artículo 5.1 b) RGPD; de conformidad con el principio de minimización *ex* artículo 5.1 c) RGPD, los datos personales deben ser adecuados, pertinentes y limitados, es decir, en su justa adecuación a la finalidad para la que se ha determinado su tratamiento[15]. Además, esta actuación requiere la exteriorización de un ejercicio trasparente de trasladado de la información a la persona interesada, en este caso, la persona trabajadora. De tal manera que, conforme al artículo 12.1 RGPD, "*el responsable del tratamiento tomará las medidas oportunas para facilitar al interesado toda información indicada en los artículos 13 y 14, así como cualquier comunicación con arreglo a los artículos 15 a 22 y 34 relativa al tratamiento, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño. La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos"*.

En referencia al registro de jornada diaria *ex* artículo 34.9 ET, tiene como objetivo acreditar el cumplimiento de la jornada pactada a fin de evitar abusos en cuantos a los límites de jornada y asegurar el respeto de los periodos de descanso de conformidad con la Directiva 2003/88/CE. Se trata de una obligación impuesta a la empresa y en la que participan activamente las personas trabajadoras al cumplimentar personalmente el registro del inicio y fin de la jornada de forma objetiva y verificable. Por tanto, cuando el empleador trata datos personales para cumplir esta obligación, la base de legitimación aplicable es la prevista en el artículo 6.1.c) RGPD, esto es, el tratamiento necesario para el cumplimiento de una obligación legal.

La base de legitimación *ex* artículo 6.1 c) RGPD en correspondencia con el artículo 34.9 ET parece que no arroja dudas al respecto, *sensu contrario*, en el caso de la utilización de datos biométricos sí que se despiertan mayores dudas. Téngase en cuenta que, a tenor del

[14] AGUILERA IZQUIERDO, Rafael, "Las implicaciones de la digitalización en las facultades empresariales de dirección y control de la prestación: el control del tiempo de trabajo", en AA.VV., *El estatuto jurídico del trabajador en la era digital*, Valencia, Tirant lo Blanch, 2024, p. 335 y siguientes.

[15] ARAGÜEZ VALENZUELA, Lucía, *Hacia la eticidad algorítmica en las relaciones laborales*, Murcia, Ediciones Laborum, 2024, p. 44-45.

artículo 9 RGPD *"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".* Como primera aproximación, puede comprobarse que existe una imposibilidad legal tajante a la utilización de los datos biométricos con finalidad de identificar de manera unívoca a una persona física. Aunque, en el artículo 9.2 b) RGPD, puede encontrarse una habilitación para levantar la prohibición del tratamiento de categorías especiales de datos 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"*. Empero, en esta ocasión, el tratamiento de datos personales de carácter biométrico no es "necesario" para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable, es decir, el registro de jornada[16].

La empresa en este caso no estaba obligada legalmente a implantar un sistema biométrico, ya que el ET no exige que el registro horario se realice mediante la captación categorías

[16] Tampoco *ex* artículo 88 RGPD podría ser válido que el Convenio Colectivo habilite al tratamiento de datos biométricos a tenor del fallo STJUE de 19 de diciembre 2024 (Asunto C-65/23, K GmbH). Vid., al respecto en MUÑOZ RUÍZ, Ana Belén, "Negociación colectiva y derecho fundamental de protección de datos de los trabajadores: líneas rojas desde la UE", *Diario La Ley*, n.º 10653, 2024. La doctrina constitucional que admite la limitación de derechos individuales a través de la negociación colectiva exige, no obstante, la existencia de una compensación o equilibrio que evite un sacrificio desproporcionado del trabajador. A este respecto, la STC 58/1985, de 30 de abril, aclara que *"desde un punto de vista general, los problemas derivados de las relaciones entre autonomía colectiva y autonomía individual han de solventarse mediante la conjunción de dos principios básicos: Primero, que la negociación colectiva no pueda anular la autonomía individual, pues ésta, garantía de la libertad personal, ha de contar con un margen de actuación incluso en unos ámbitos como los de la Empresa en los que exigencias de índole económica, técnica o productiva reclaman una conformación colectiva de condiciones uniformes; y segundo, que no puede en modo alguno negarse la capacidad de incidencia del Convenio en el terreno de los derechos o intereses individuales, pues ello equivaldría a negar toda virtualidad a la negociación colectiva, en contra de la precisión constitucional que la configura como un instrumento esencial para la ordenación de las relaciones de trabajo, y contradiría el propio significado del Convenio en cuya naturaleza está el predominio de la voluntad colectiva sobre la individual y de los intereses de la colectividad sobre los concretos de los individuos que la componen, siendo en ocasiones preciso la limitación de algunos de éstos para la efectiva promoción de aquéllos"*. En suma, *"siendo la Ley, en este caso, la que determina la extensión de los derechos individuales, así como el ámbito de actuación de la negociación colectiva, no puede considerarse inconstitucional que se permita que mediante el Convenio pueda fijarse un límite temporal al derecho individual, en la medida en que no se establezca sin compensación para el afectado"*.

especiales de datos personales de las personas trabajadoras. Existen alternativas igualmente válidas —como tarjetas, códigos personales o aplicaciones digitales— que permiten cumplir la obligación legal con un menor grado de intrusión en la esfera personal[17]. Todo ello sin olvidar el principio de minimización *ex* artículo 5.1 c) RGPD, compartiendo el criterio la Agencia Catalana de Protección de Datos (APDCAT)[18] *"las exigencias derivadas de la protección de datos en el diseño (artículo 25.1 RGPD) y, en especial, del principio de minimización, obligan a elegir la tecnología que resulte menos intrusiva desde el punto de vista de la protección de datos. El principio de minimización no se manifiesta sólo a la hora de optar por alternativas que no impliquen el tratamiento de datos personales, o de llevar a cabo el tratamiento de datos de forma que se empleen los datos mínimos indispensables, sino que también comporta que, si se puede alcanzar una determinada finalidad sin tener que tratar datos de categorías especiales, esta opción debe prevalecer ante otras opciones que sí impliquen el tratamiento de este tipo de datos".* Por tanto, la utilización de huellas dactilares no puede justificarse al amparo del artículo 6.1.c) RGPD, ya que dicho precepto se refiere a tratamientos estrictamente necesarios para cumplir una obligación legal, y el uso de datos biométricos no es necesario, sino opcional[19].

En este momento resulta de interés las aportaciones de la Guía sobre tratamientos de control de presencia mediante sistemas biométricos publicada por la AEPD[20]. La sentencia acierta al indicar que dicha guía carece de fuerza jurídica vinculante. No obstante, su contenido resulta útil como referencia interpretativa, en la medida en que recoge criterios alineados con los parámetros del marco normativo de protección de datos aplicables al supuesto analizado.

Por un lado, en el caso del control de accesos no se comparte que la base de legitimación sea el artículo 9.2 i) RGPD. A este respecto, se estima favorable un interés legítimo del responsable del tratamiento, en este caso, el hospital *ex* artículo 6.1f) así como un tratamiento por razones de interés público proporcional al objetivo perseguido –garantizar únicamente los accesos autorizados a lugares con autorización previa- adoptando las medidas adecuadas y específicas para salvaguardar los derechos fundamentales, entre otros, el derecho a la protección de datos personales. En este punto,

[17] Vid., en LLORENS ESPADA, Julen, "Aplicaciones informáticas (app) para el registro diario de la jornada laboral. Condiciones de licitud", *Labos*, vol. 3, n.º 1, 2022, p. 80-88.

[18] Dictamen CNS 2/2022 de la Autoridad Catalana de Protección de Datos (APDCAT).

[19] GRACIA GARCÍA, David, "El impacto de la privacidad en los sistemas biométricos de control de acceso y horario laboral tras el Dictamen 63/2018 de la Autoridad Catalana de Protección de Datos", *Consultor de los ayuntamientos y de los juzgados: Revista técnica especializada en administración local y justicia municipal*, n.º 8, 2019, p. 56-65.

[20] MUÑOZ RUÍZ, Ana Belén, "Datos biométricos y control horario de los empleados: la nueva Guía de la Agencia Española de Protección de Datos (1)", *La Ley Privacidad*, n.º 19, 2024.

la base nacional sería el artículo 43 de la Ley 33/2011, de 4 de octubre, General de Salud Pública al prever que *"1. En todos los niveles del sistema de información en salud pública se adoptarán las medidas necesarias para garantizar la seguridad de los datos. 2. Los trabajadores de centros y servicios públicos y privados y quienes por razón de su actividad tengan acceso a los datos del sistema de información están obligadas a mantener secreto"*.

Por otro y como se ha podido comprobar en la fundamentación jurídica de la sentencia, los datos biométricos -huella dactilar- se han utilizado para atender a dos finalidades distintas: control de jornada y control de accesos. Una actuación que requiere mucha cautela en el análisis de los parámetros del RGPD como se ha previsto en líneas anteriores, ya que *"todos estos propósitos, que muchas veces se presentan como ventajas adicionales a la decisión de implementar el tratamiento de registro de jornada o el control de acceso con operaciones biométricas, han de ser considerados tratamientos con finalidades distintas a los efectos de la normativa de protección de datos personales. Por lo tanto, la posibilidad de ejecutar dichos tratamientos depende del cumplimiento de todos los principios, derechos y obligaciones establecidos en el RGPD"*.

Sobre la utilización de los datos biométricos el Centro Criptológico Nacional (CCN), respecto al cumplimiento de la normativa (RGPD y LOPDGDD) de los sistemas de control de acceso basados en la obtención de una plantilla biométrica moderna como son las Referencias Biométricas Renovables (RBR) que reúnen las siguientes características: irreversible, anónima, privada, no interoperable, uso controlado, renovación y cifrado en origen. En su análisis también incorpora la conformidad de las plantillas RBR con el RIA, que parte de una distinción del reconocimiento biométrico entre la identificación y verificación biométrica. Sobre esta cuestión, señala que *"los sistemas de identificación biométrica no remotos en los que existe participación activa del usuario, así como los sistemas de verificación biométrica no están prohibidos y están calificados de riesgo bajo o nulo"*. Y, puntualiza, nuevamente, la falta de vulneración de DDFF de la ciudadanía tomando en consideración el criterio de la irreversibilidad de los datos biométricos contenidos en una base de datos de referencia.

No obstante, para minimizar los riesgos advertidos el CCN recomienda para el nivel alto de seguridad el uso de sistemas de control de acceso basados en el uso de plantillas biométricas RBR, que dispongan de una evaluación y certificación conforme a las normas y estándares nacionales e internacionales sobre la materia.

Incluso frente al discurso más restrictivo, la empresa podría alegar y justificar otra causa para levantar la prohibición en el tratamiento de datos especialmente sensibles, a través del consentimiento de la persona trabajadora *ex* artículo 9.2 a) RGPD. Sin perder de vista

que en la relación laboral existe un desequilibrio de poder empresa-persona trabajadora[21], esta posibilidad se diluye puesto que *"para garantizar que el consentimiento se haya dado libremente, este no debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal en un caso concreto en el que exista un desequilibro claro entre el interesado y el responsable del tratamiento, en particular cuando dicho responsable sea una autoridad pública y sea por lo tanto improbable que el consentimiento se haya dado libremente en todas las circunstancias de dicha situación particular"*, de conformidad con el considerando 43 RGPD. Ello no sería posible, en tanto en cuanto, el consentimiento de la persona trabajadora debe consistir en una *"manifestación de voluntad libre, específica, 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"*, *ex* artículo 4.11 RGPD.

En definitiva, esta opción jurídica de optar por el consentimiento en el ámbito de las relaciones labores debe evaluarse con cautela ante las dudas que puede generar la validez del consentimiento de la persona trabajadora ante un tratamiento de datos biométricos[22], la no superación del principio de necesidad, así como por la viabilidad real de utilizar una alternativa para cumplir con esta obligación legal menos gravosa para el derecho fundamental a la protección de datos personales *ex* artículo 18.4 CE.

## 5. Conclusiones al debate jurídico planteado

La sentencia del Juzgado de lo Social n.º 3 de A Coruña refleja, por un parte, un apoyo incuestionable a la luz de la experiencia judicial al uso de datos biométricos por las empresas para cumplir con la obligación legal del registro de jornada[23]. Por otro, se puede estar de acuerdo con que se está efectuando una incorrecta aplicación del compendio normativo de protección de datos personales, muy probablemente, por el carácter técnico y falta de acomodación a un ámbito tan específico y singular como las relaciones laborales.

[21] Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, versión 1.1, adoptadas el 4 de mayo de 2020.

[22] Hay voces muy críticas sobre la restricción a la utilización del consentimiento como base de legitimación válida, mostrándose contrarios al criterio aplicado por la AEPD en su Guía sobre el tratamiento de control de presencia mediante sistemas biométricos. Por un lado, ante una incongruencia en la aplicación del RGPD y el RIA, así como por la restricción de derechos digitales del ciudadano. Vid., RAZQUIN LIZARRAGA, Martín María y ALENZA GARCÍA, José Francisco (directores), *Biometría, derecho administrativo y datos*, Cizur Menor, Aranzadi, 2025, p. 453-455.

[23] Como se señalada desde la doctrina, una *"medida neopanóptica de vigilancia",* FERNÁNDEZ RAMÍREZ, Marina, *El derecho del trabajador a la autodeterminación informativa en el marco de la actual empresa "neopanóptica"*, Pamplona, Aranzadi, 2021, p. 33.

La crítica principal radica en considerar que el artículo 34.9 ET legitima *per se* el tratamiento de datos biométricos tomando como base de legitimación el artículo 6.1.c) RGPD. Ello supone una confusión entre control horario (obligación legal) y control de presencia (interés empresarial), con consecuencias relevantes para la protección de derechos fundamentales como es la protección de datos personales *ex* artículo 18.4 CE.

Este debate se ha trasladado desde la perspectiva tuitiva de los derechos de las personas trabajadoras en cumplimiento de los requisitos de objetividad, fiable y accesible, [(STJUE de 14 de mayo de 2019, (C-55/18)] a la perspectiva empresarial en la tesis de implementar un método infalible que descarte cualquier posibilidad de suplantación de la identidad personal de cada persona trabajadora[24]. A mi juicio, la opción de decantarse por los sistemas biométricos de registro de jornada justificados por una razón de "seguridad" o la "evitación del fraude", puede desenmascarar una posible tentación empresarial de priorizar el control absoluto sobre el respeto a los derechos fundamentales[25]. De hecho, esta posibilidad real de fraude por las personas trabajadoras puede llevarse a cabo por cualquier tipo de método de registro de jornada y, además, ya está siendo objeto de previsión en el régimen sancionador de los convenios colectivos[26]. Por lo que, se antoja un argumento de poca solidez para priorizar su utilización frente a otros métodos menos invasivos y proporcionados con la finalidad perseguida.

Una cuestión cierta es que en la práctica el criterio de la AEPD[27] y de los tribunales está generando una incertidumbre a las empresas en sus opciones para cumplir con la obligación legal del registro de jornada. No obstante, sí que es momento de puntualizar que no existe una base jurídica a tenor del marco normativo en materia de protección de

[24] Auto del Tribunal Constitucional 57/2007, de 26 de febrero, sentencia del Tribunal Supremo 5017/2003, de 2 de julio de 2007, sentencia del Tribunal Superior de Justicia de Andalucía Sala de lo Contencioso-Administrativo n.º 874/2007 de 3 de diciembre de 2007, la sentencia del Tribunal Superior de Justicia de Murcia Sala de lo Social n.º 47/2010 de 25 de enero de 2010 y la sentencia del Tribunal Superior de Justiciade Canarias Sala de lo Social n.º 914/2012 de 29 de mayo de 2012.

[25] Así se constata por el autor quien desarrolla este nuevo concepto de "biovigilancia" explorando los beneficios como los riesgos de la IA en el marco de las relaciones laborales. LÓPEZ AHUMADA, J. Eduardo, "La repercusión de la inteligencia artificial y la biovigilancia desde la perspectiva del control de la actividad laboral de las personas trabajadoras", en BALAGUER CALLEJÓN, Francisco y ESCAJEDO SAN-EPIFANIO, Leire (directores), *Vigilancia biométrica masiva, inteligencia artificial y derechos fundamentales*, Cizur Menor, Aranzadi, 2025, p. 402-404.

[26] Por ejemplo, artículo 77 de la Resolución de 1 de abril de 2022, de la Dirección General de Trabajo, por la que se registra y publica el IV Convenio colectivo de Ilunion Seguridad, SA. Artículo 32.2 de la Resolución de 31 de agosto de 2022, de la Dirección General de Trabajo de la Consejería de Economía, Hacienda y Empleo, sobre registro, depósito y publicación del convenio colectivo de la empresa Unión Sindical de Madrid Región. Artículo 49 de la Convenio colectivo para el sector de las industrias de derivados del cemento de Álava.

[27] Expediente n.º EXP20222960, EXP202213615, EXP202304834.

datos personales que habilite con total libertad a las empresas a implementar sistemas biométricos para cumplimentar el registro de jornada *ex* artículo 34.9 ET a tenor de los argumentos esgrimidos. Además, el consentimiento explícito de la persona trabajadora como base de legitimación *ex* artículo 9.2 a), plantea serias dudas ante el desequilibrio propio de la relación laboral; máxime si no existen alternativas de libre elección al registro garantizando un consentimiento libre, específico, informado e inequívoco de la persona trabajadora.

El responsable del tratamiento de datos biométricos debe realizar, previamente, una evaluación de impacto *ex* artículo 35 RGPD a fin de evaluar, *"en particular, el origen, la naturaleza, la particularidad y la gravedad de dicho riesgo. El resultado de la evaluación debe tenerse en cuenta cuando se decidan las medidas adecuadas que deban tomarse con el fin de demostrar que el tratamiento de los datos personales es conforme con el presente Reglamento"* (considerando 84 RGPD). Y en referencia a la puesta en práctica, de conformidad con el artículo 5.1 c) y artículo 25.2 RGPD, el responsable deberá emplear las medidas técnicas y organizativas[28] a fin de que *"solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. (...) Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas"*. Puede tomarse de ejemplo las aportaciones realizadas por la AEPD[29], que contempla actuaciones como informar a las personas trabajadoras sobre el tratamiento de datos biométricos, así como los riesgos asociados a este; emplear un sistema biométrico con la posibilidad de revocar el vínculo de identidad entre la plantilla biométrica y la persona a quien corresponda; implementar las medidas técnicas necesarias para evitar el trasvase o utilización no conforme con el propósito inicial; utilización de cifrado para conseguir la confidencialidad, disponibilidad e integridad de la plantilla biométrica; seleccionar correctamente un formato o tecnología que impida el trasvase o interconexión de datos biométricos que puedan permitir una fuga de datos; permitir la supresión de los datos biométricos una vez que no atiendan a la finalidad que justificó su tratamiento inicial; y procurar la minimización de los datos biométricos que han sido objeto de recogida sin que pueda derivarse en una revelación adicional de datos de carácter especial.

[28] Sobre esta cuestión, la AEPD ha avalado la instalación de un registro de control de accesos en la Guardia Civil ya que consiste en *"un conjunto relevante de garantías técnicas orientadas a la minimización del impacto, con medidas como la generación local de identificadores no reversibles, su validez limitada a los períodos autorizados, el control exclusivo del interesado sobre sus datos y su no interoperabilidad. El diseño, además, limita el reconocimiento a la persona situada directamente frente a la cámara, reduciendo el riesgo de tratamientos accidentales o masivos. Estas configuraciones permiten restringir el alcance del tratamiento y previenen usos indebidos o accesos no autorizados"*. Vid., AEPD – Consulta Previa (artículo 36 RGPD), Ref. REGAGE25e00024730156.

[29] AEPD, *Guía sobre tratamientos de control de presencia mediante sistemas biométricos*, 2023.

## 6. Bibliografía

AGUILERA IZQUIERDO, Rafael, "Las implicaciones de la digitalización en las facultades empresariales de dirección y control de la prestación: el control del tiempo de trabajo", en AA.VV., *El estatuto jurídico del trabajador en la era digital*, Valencia, Tirant lo Blanch, 2024, p. 317-348.

ARAGÜEZ VALENZUELA, Lucía, *Hacia la eticidad algorítmica en las relaciones laborales*, Murcia, Ediciones Laborum, 2024.

BAZ RODRÍGUEZ, Jesús, *Privacidad y protección de datos de los trabajadores en el entorno digital*, Madrid, Bosch, 2019.

FERNÁNDEZ RAMÍREZ, Marina, *El derecho del trabajador a la autodeterminación informativa en el marco de la actual empresa "neopanóptica"*, Pamplona, Aranzadi, 2021.

GONZÁLEZ GONZÁLEZ, Carlos, *Registro de la jornada y problemas en la determinación de la jornada efectiva de trabajo*, Pamplona, Aranzadi, 2020.

GRACIA GARCÍA, David, "El impacto de la privacidad en los sistemas biométricos de control de acceso y horario laboral tras el Dictamen 63/2018 de la Autoridad Catalana de Protección de Datos", *Consultor de los ayuntamientos y de los juzgados: Revista técnica especializada en administración local y justicia municipal*, n.º 8, 2019, p. 56-65.

LÓPEZ AHUMADA, J. Eduardo, "La repercusión de la inteligencia artificial y la biovigilancia desde la perspectiva del control de la actividad laboral de las personas trabajadoras", en BALAGUER CALLEJÓN, Francisco y ESCAJEDO SAN-EPIFANIO, Leire (directores), *Vigilancia biométrica masiva, inteligencia artificial y derechos fundamentales*, Cizur Menor, Aranzadi, 2025, p. 402-436.

LLORENS ESPADA, Julen, "Aplicaciones informáticas (app) para el registro diario de la jornada laboral. Condiciones de licitud", *Labos*, vol. 3, n.º 1, 2022, p. 80-88.

LLORENS ESPADA, Julen, "El interés legítimo de la empresa como base de licitud para el tratamiento de datos personales de la persona trabajadora", *Documentación Laboral*, vol. II, n.º 126, 2022, p. 27-50.

MARCOS HERRERO, José Antonio, "La protección de datos personales de los empleados en el registro de la jornada y los denominados 'derechos digitales'", *Revista Derecho Social y Empresa*, n.º 11, 2019, p. 44-69.

MERCADER UGUINA, Jesús R., "Datos biométricos en los centros de trabajo", en BAZ RODRÍGUEZ, Jesús (directora), *Los nuevos derechos digitales laborales de las personas trabajadoras en España*, 1.ª ed., Madrid, Wolters Kluwer, 2021, p. 169-198.

MIÑARRO YANINI, Margarita, "Más allá de las horas extras: la obligatoriedad del registro de la jornada diaria (Comentario a la Sentencia de la Audiencia Nacional 25/2016, de 19 de febrero)", *Revista de Trabajo y Seguridad Social – CEF*, n.º 397, 2016.

MUÑOZ RUÍZ, Ana Belén, *Biometría y sistemas automatizados de reconocimiento de emociones: implicaciones jurídico-laborales*, Valencia, Tirant lo Blanch, 2023.

MUÑOZ RUÍZ, Ana Belén, "Datos biométricos y control horario de los empleados: la nueva Guía de la Agencia Española de Protección de Datos (1)", *La Ley Privacidad*, n.º 19, 2024.

MUÑOZ RUÍZ, Ana Belén, "Negociación colectiva y derecho fundamental de protección de datos de los trabajadores: líneas rojas desde la UE", *Diario La Ley*, n.º 10653, 2024.

PRECIADO DOMÈNECH, Carlos Hugo, "El registro de la jornada ordinaria en la nueva doctrina del TS (Comentario a la STS 23 de marzo de 2017, RCUD 81/2016)", *Revista de Información Laboral*, n.º 7, 2017, p. 147-162.

RAZQUIN LIZARRAGA, Martín María y ALENZA GARCÍA, José Francisco (directores), *Biometría, derecho administrativo y datos*, Cizur Menor, Aranzadi, 2025.

SELMA PENALVA, Alejandra, "El control de accesos por medio de huella digital y sus repercusiones prácticas sobre el derecho a la intimidad de los trabajadores. Comentario a la STSJ de Murcia, de 25 de enero de 2010", *Revista Doctrinal Aranzadi Social*, n.º 3, 2010.

SERRANO GARCÍA, Juana María, *La protección de datos y la regulación de las tecnologías en la negociación colectiva y en la jurisprudencia*, Albacete, Bomarzo, 2019.

SERRANO GARCÍA, Juana María, *La protección jurídica de los datos de las personas trabajadoras*, Albacete, Bomarzo, 2022.

TRILLO PÁRRAGA, Francisco, "Registro de jornada diaria efectiva: un paso adelante en el control del tiempo de trabajo (Sentencia Audiencia Nacional 207/2015, de 4 de diciembre, Rec. 301/2015)", *Diario La Ley*, n.º 8875, 2016.