ISSN-e: 2792-8322

Datos biométricos y registro horario: el principio de necesidad y el papel de la negociación colectiva

Alba Navalón Arnal

Investigadora no doctora del Departamento de Derecho del Trabajo y de la Seguridad Social. Universitat de València (España)
alba.navalon@uv.es | https://orcid.org/0009-0004-6582-5326

Extracto

Las tecnologías de biometría son uno de los sistemas escogidos para dar cumplimiento a la obligación legal de registro horario del artículo 34.9 del Estatuto de los Trabajadores (ET). A pesar de que esta provisión de la normativa laboral no incluye mención alguna a la privacidad de las personas trabajadoras, el empleo de esta tipología de sistemas implica el tratamiento de datos biométricos y, por tanto, la observancia del Reglamento General de Protección de Datos (RGPD). En este sentido, la Agencia Española de Protección de Datos (AEPD) considera que el artículo 34.9 del ET no es lo suficientemente expreso para levantar la prohibición de tratamiento que el RGPD configura sobre los datos biométricos. No obstante, esta interpretación, que contribuye a la salvaguarda del derecho a la protección de datos, se contrapone, en cierta manera, a una jurisprudencia tendente a considerar que el tratamiento de los datos biométricos con fines de registro horario es proporcional y a una negociación colectiva que se aleja de su tradicional papel garantista. En el presente trabajo se expone cuáles son los criterios de la AEPD y de la jurisprudencia; se plantea si pudieran verse modificados o reforzados a raíz de la reforma propuesta en materia de registro horario, aprobada en segunda vuelta el pasado 6 de mayo de 2025 por el Consejo de Ministros; y se examina cuál es la intervención de la negociación colectiva. Partiendo de este análisis, se propone incluir una prohibición de tratamiento de los datos biométricos para el control horario en la normativa laboral, con el fin de corregir la inseguridad jurídica existente en la materia.

Palabras clave: datos biométricos; registro horario; AEPD; derecho a la protección de datos; negociación colectiva; principio de proporcionalidad; principio de necesidad.

Recibido: 01-04-2025 / Aceptado: 03-06-2025 / Publicado: 04-07-2025

Cómo citar: 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

ISSN-e: 2792-8322

Biometric data and time recording: the principle of necessity and the role of collective bargaining

Alba Navalón Arnal

Non-doctoral Researcher, Department of Labor and Social Security Law. University of Valencia (Spain)
alba.navalon@uv.es | https://orcid.org/0009-0004-6582-5326

Abstract

Biometric technologies are one of the systems chosen to comply with the legal obligation to record working hours in Article 34.9 of the Workers' Statute. Although this provision of labour legislation does not include any mention of the privacy of workers, the use of this type of system implies the processing of biometric data and, therefore, compliance with the General Data Protection Regulation. In this regard, the Spanish Data Protection Agency considers that Article 34.9 of the Workers' Statute is not sufficiently express to lift the prohibition on processing of biometric data that the GDPR sets out. However, this interpretation, which contributes to safeguarding the right to data protection, is to some extent at odds with a case law that tends to consider that the processing of biometric data for time registration purposes is proportional and with collective bargaining that is moving away from its traditional role as a guarantor. The present study reviews the criteria of the Spanish Data Protection Agency and the case law; it considers whether they could be modified or strengthened as a result of the proposed reform on time recording, approved in the second round on 6 May 2025 by the Council of Ministers; and it examines the role of collective bargaining. On the basis of this analysis, it is proposed to include a prohibition on the processing of biometric data for time and attendance control in labour legislation, in order to correct the existing legal uncertainty in this area.

Keywords: biometric data; time recording; AEPD; right to data protection; collective bargaining; proportionality principle; necessity principle.

Received: 01-04-2025 / Accepted: 03-06-2025 / Published: 04-07-2025

Citation: Navalón Arnal, A. (2025). Biometric data and time recording: the principle of necessity and the role of collective bargaining. *Revista de Trabajo y Seguridad Social. CEF*, *487*, 17-52. https://doi.org/10.51302/rtss.2025.24427

Sumario

1. Introducción
2. La obligación legal de registro horario
3. Categorización de los datos biométricos y obligaciones concretas del responsable del tratamiento
4. El criterio de la AEPD en el tratamiento de datos biométricos con fines de control horario
   - 4.1. El levantamiento de la prohibición vía artículo 9.2 b) del RGPD
   - 4.2. La acreditación de la necesidad del sistema de biometría
   - 4.3. El levantamiento de la prohibición vía artículo 9.2 a) del RGPD: consentimiento
   - 4.4. La obligación de efectuar una EIPD
5. Mayor permisibilidad del tratamiento de datos biométricos por la jurisprudencia antes de la aprobación del RGPD
6. Las implicaciones de la reforma del registro de jornada planteada por el proyecto de Ley para la reducción de la duración máxima de la jornada ordinaria de trabajo y la garantía del registro de jornada y el derecho a la desconexión
   - 6.1. La concreción de la obligación de registro
   - 6.2. La superación del principio de proporcionalidad
7. El papel de la negociación colectiva
   - 7.1. El deber de recoger garantías adecuadas
   - 7.2. La observancia del criterio de necesidad
   - 7.3. La inobservancia de la normativa en los convenios colectivos
8. Conclusiones

Referencias bibliográficas

1. Introducción

Las tarjetas magnéticas, las claves PIN, el fichaje mediante aplicaciones informáticas o páginas web, el reconocimiento facial, el escáner de huella dactilar, etc. son algunos de los métodos que permiten dar cumplimiento a la obligación legal de registro de la jornada diaria. No obstante, no todos ellos interfieren de la misma manera en los derechos fundamentales de las personas trabajadoras, teniendo una especial injerencia en el derecho a la protección de datos y en el derecho a la intimidad las tecnologías de biometría, tales como los sistemas de verificación del rostro o de la huella dactilar[1].

Si bien se trata de tecnologías que no pueden ser calificadas como novedosas (Rodríguez-Piñero Royo, 2019, p. 92), la concienciación de las personas trabajadoras sobre sus implicaciones se ha visto acrecentada recientemente. De hecho, la AEPD ha reportado un mayor número de reclamaciones sobre la materia en los últimos años[2]. Ante el aparente incremento de la concienciación y los cambios normativos planteados sobre el registro horario, debe ser señalado que la AEPD y la jurisprudencia sostienen opiniones dispares acerca de la legitimidad del uso de datos biométricos para control horario, lo que ocasiona un escenario de inseguridad y desprotección jurídica.

Así, en el presente trabajo se expondrá cuáles son los criterios sostenidos por la AEPD y la jurisprudencia respecto al tratamiento de datos biométricos con fines de registro horario; si estos pudieran ser susceptibles de algún cambio ante la posible aprobación del proyecto de Ley para la reducción de la duración máxima de la jornada ordinaria de trabajo y la garantía del registro de jornada y el derecho a la desconexión, el registro de jornada y el derecho a la desconexión, y cuál es el papel de la negociación colectiva en esta área. Con todo, se sostendrá, en primer lugar, que incluir una prohibición expresa de tratamiento de datos biométricos con fines de control horario en la normativa laboral permitiría corregir la inseguridad jurídica y adoptar una posición más garantista del derecho a la protección de datos de las

[1] Ello no implica que el resto de los sistemas de registro no puedan suponer un riesgo para la privacidad de las personas trabajadoras, e incluso para otros derechos como el derecho a la vida, a la protección de la salud, a la no discriminación o incluso a la conciliación de la vida laboral y familiar (Gómez-Millán Herencia, 2020, pp. 254-255).

[2] La AEPD recogió, en su Memoria anual de 2023, que:

> Las reclamaciones por el tratamiento de datos no son aún muy numerosas en datos absolutos, pero también están en claro crecimiento, habiéndose triplicado en estos dos años, principalmente por su uso en sistemas de verificación de identidad para el acceso a todo tipo de instalaciones, especialmente en el ámbito laboral y relacionadas con el control de jornada (p. 154).

personas trabajadoras. En segundo lugar, que las tecnologías biométricas de registro horario no cumplen con el requisito de necesidad del principio de proporcionalidad. Y, en tercer lugar, que la reforma propuesta por el proyecto de ley no debería suponer, en principio, el levantamiento de la prohibición de tratamiento que versa sobre los datos biométricos.

2. La obligación legal de registro horario

El artículo 35.5 del ET (RDLeg. 1/1995, de 24 de marzo) recogía la obligación de registrar día a día la jornada laboral de cada persona trabajadora «a efectos del cómputo de horas extraordinarias»[3]. No obstante, aparte de contemplar esta obligación respecto a las horas que excedían de las ordinarias, no desarrollaba la manera en la que debía efectuarse el registro; generando, por tanto, una clara inseguridad jurídica (Rodríguez Martín-Retortillo, 2022). Las dudas que suscitaba la norma –centradas principalmente en el debate de si era necesario efectuar un registro de la jornada completa o únicamente de las horas extraordinarias– no fueron resueltas ni aclaradas con la reforma del ET, aprobada por el Real Decreto Legislativo 2/2015, de 23 de octubre (Montesdeoca Suárez, 2022, p. 174). La normativa conservó y no amplió, en un inicio, los preceptos relativos a la obligación de registro horario; manteniendo así la litigiosidad que giraba en torno a la materia y que resultó en el dictamen de las conocidas sentencias de la Audiencia Nacional (AN) de 4 de diciembre de 2015 (rec. 301/2015) y del Tribunal Supremo (TS) de 23 de marzo de 2017 (rec. 81/2016)[4]. Sin entrar en mayores detalles al respecto, el debate fue zanjado, al menos en lo referente al corazón de la cuestión, con la introducción del apartado noveno del artículo 34 del ET y el pronunciamiento del Tribunal de Justicia de la Unión Europea (TJUE) de 14 de mayo de 2019, asunto C-55/18 (Rodríguez Pastor, 2019, pp. 17-20).

Por una parte, el Real Decreto-Ley 8/2019, de 8 de marzo, de medidas urgentes de protección social y de lucha contra la precariedad laboral en la jornada de trabajo, modificó el artículo 34 del ET, ampliando la obligación de registrar la jornada más allá de las horas extraordinarias, y recogiendo, así, el deber empresarial de contabilizar «el horario concreto

[3] Esta obligación de registrar la jornada laboral se amplió posteriormente para las personas trabajadoras a tiempo parcial, mediante la aprobación del Real Decreto-Ley 16/2013, de 20 de diciembre, de medidas para favorecer la contratación estable y mejorar la empleabilidad de los trabajadores. Además, estaba contemplada en otros supuestos concretos: trabajadores móviles, trabajo en la marina mercante, trabajadores móviles en el transporte ferroviario en servicios de interoperabilidad transfronteriza y trabajadores desplazados (Rodríguez Pastor, 2019, p. 39).

[4] Por una parte, la AN consideró que la única forma de controlar si se superaban los límites de la jornada ordinaria era registrando la jornada diaria completa (FJ 2). Y, por otra parte, el TS, resolviendo el recurso de casación interpuesto frente a la sentencia de la AN, entendió que el articulado no contemplaba la obligación de un registro de jornada diaria, por lo que no podía ser exigido, a pesar de que fuera conveniente una reforma de la norma (FJ 5).

de inicio y finalización de la jornada de trabajo de cada persona trabajadora». Con escasa diferencia de tiempo, por otra parte, se pronunció el TJUE, en el asunto C-55/18, acerca de la adecuación de la normativa española a la Directiva 2003/88, de 4 de noviembre de 2003, relativa a determinados aspectos de la ordenación del tiempo de trabajo. En dicha sentencia se reconoció que para poder comprobar que se ha respetado la duración máxima del tiempo de trabajo semanal (art. 6 de la directiva) y los periodos mínimos de descanso diario y semanal (arts. 3 y 5) era esencial determinar el número de horas de trabajo diario y semanal (FJ 49).

En este sentido, si bien tanto la reforma normativa como la resolución del TJUE permitieron zanjar la duda respecto a la obligatoriedad de llevar un registro de la jornada diaria de cada persona trabajadora, estos instrumentos jurídicos introdujeron escasas referencias sobre la forma en la que debía ser efectuado dicho registro (Rodríguez-Piñero Royo, 2020; Gómez-Millán Herencia, 2020, p. 223).

Así, el artículo 34.9 del ET traslada la facultad de organizar y documentar el registro horario a la negociación colectiva o a los acuerdos de empresa; añadiendo que, en ausencia de ambos, la empresa podrá decidir la forma de efectuarlo unilateralmente, no obstante, previa consulta con los órganos de representación de las personas trabajadoras en su caso (Cristóbal Roncero, 2020, p. 609). Y en adición a esta remisión expresa a la negociación colectiva, el precepto únicamente indica que los registros deberán conservarse durante cuatro años y permanecer «a disposición de las personas trabajadoras, de sus representantes legales y de la Inspección de Trabajo y de la Seguridad Social». De esta forma, la empresa debe permitir que las personas interesadas puedan acceder a la documentación en cualquier momento; información que debe estar físicamente en el centro de trabajo o ser accesible desde el mismo[5].

Por otra parte, en relación con la regulación europea, el Tribunal de Justicia indica, en la resolución de 14 de mayo de 2019, que para «garantizar el efecto útil de los derechos recogidos en la Directiva 2003/88 [...] los Estados miembros deben imponer a los empresarios la obligación de implantar un sistema objetivo, fiable y accesible [...]» (FJ 60).

De esta manera, la normativa actual, tanto europea como española, no impone una forma concreta de conducir el registro de la jornada; sino que recoge, por el contrario, unas directrices generales (Alfonso Mellado, 2019, p. 59). Se entiende, por tanto, y así lo ha plasmado el Ministerio de Trabajo, Migraciones y Seguridad Social, en la Guía sobre el registro de jornada, que se admite «cualquier sistema o medio, en soporte papel o telemático, apto

[5] En este sentido se pronuncia la Inspección de Trabajo y Seguridad Social, en el Criterio Técnico 101/2019, en materia de registro de jornada (p. 12).

para cumplir el objetivo legal, esto es, proporcionar información fiable, inmodificable y no manipulable *a posteriori*». Aunque cabe matizar que la AN consideró que la firma en papel no era un sistema fiable (Sentencia 22/2022, de 15 de febrero).

En un inicio, esta falta de concreción puede entenderse como un rasgo positivo porque otorga a la empresa la libertad de escoger el mecanismo o sistema de registro que mejor se adapta a sus circunstancias concretas[6,7]. No obstante, tal margen de maniobra sin garantías también puede jugar en detrimento de los derechos fundamentales de las personas trabajadoras[8]. En este sentido, la normativa laboral abarca aspectos estrictamente laborales, absteniéndose de pronunciarse sobre los derechos fundamentales a la intimidad y a la protección de datos que pudieran verse afectados en el proceso de fichaje (Muñoz Ruiz, 2023, p. 36).

Una de las áreas en las que se reflejan las consecuencias de este desamparo jurídico es en el empleo de herramientas de registro horario que implican el tratamiento de datos biométricos, tales como sistemas de reconocimiento facial o de escaneo de la huella dactilar. Así, de la lectura exclusiva del artículo 34.9 del ET se podría concluir que este tipo de tecnologías son plenamente válidas para el cumplimiento de la obligación de registro, por cuanto proporcionan información fiable sobre el inicio y fin de la jornada. Y esto sería así siempre y cuando no se contemplase la normativa en materia de protección de datos y, en concreto, el RGPD (Reglamento 2016/679)[9].

El hecho de que el poder legislativo en el artículo 34.9 del ET haya omitido cualquier referencia al derecho a la protección de datos o a las garantías en el tratamiento de datos biométricos que la normativa específica contempla, genera o, más bien, aumenta la inseguridad jurídica, dado que promueve la disparidad de criterios sostenidos, en la materia, por la jurisprudencia y la AEPD[10]. Para comprender la problemática, es relevante señalar la naturaleza de esta tipología de datos personales y su regulación en el RGPD.

6 La normativa reconoce flexibilidad a la empresa siempre y cuando el sistema empleado garantice «la fiabilidad y veracidad de los datos» (García Coca, 2020).

7 En este sentido, el TJUE, en la Sentencia de 14 de mayo de 2019, entendió que recae sobre los Estados miembros la facultad de definir el sistema, «especialmente la forma que este debe revestir, teniendo en cuenta, en su caso, las particularidades propias de cada sector de actividad de que se trate e incluso las especificidades de determinadas empresas, como su tamaño» (FJ 63).

8 En términos generales, la digitalización en ámbito laboral, ante «la falta de un marco legal adecuado coloca a las personas trabajadoras en una situación de desventaja» (Pérez del Prado, 2023, p. 118).

9 La Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (LOPDPGDD) no incluye una regulación adicional sobre el control biométrico, a pesar de que sí que regula otros instrumentos de control digital (arts. 87, 89 y 90) (González Moreno, 2019).

10 Véase Rodríguez-Piñero Royo (2019).

3. Categorización de los datos biométricos y obligaciones concretas del responsable del tratamiento

Los datos biométricos hacen referencia a las características físicas, fisiológicas o conductuales de una persona física que permiten o confirman la identificación única de la misma (art. 4.14 RGPD)[11]. En términos generales, engloba toda aquella información que es generada por el propio cuerpo del sujeto (Gómez Sánchez, 2021, p. 1043).

Como indica el GT29, en su Dictamen 3/2012 sobre la evolución de las tecnologías biométricas, dentro de esta tipología de datos se incluyen múltiples rasgos del individuo tales como: el rostro, la huella dactilar, el iris, la retina, la voz, el ADN, la firma manuscrita, la forma de caminar, etc. De esta manera, los datos biométricos no son tratados exclusivamente cuando se emplean técnicas de reconocimiento facial o de escaneo de la huella dactilar. No obstante, deben ser resaltadas estas dos tecnologías en concreto porque son las que generalmente se emplean en el registro horario, o al menos las que están presentes en los procedimientos conducidos por la AEPD (entre otros, PS/00617/2010, PS/00232/2015, PS/00218/2021, PS/00544/2022, PS/0074/2024, PS/00545/2023).

El hecho de que los datos biométricos sean únicos y permanentes, permitan distinguir a una persona concreta (Rodríguez-Piñero Royo, 2019, p. 94) y eviten, en gran medida, la posibilidad de que el registro horario sea efectuado por otra persona trabajadora constituye una de las principales razones por la que las empresas deciden implantar sistemas que implican su tratamiento (Poquet Catalá, 2020)[12].

En este sentido, dado que los datos biométricos engloban características de las que la persona no puede liberarse, desprenderse o modificar en la mayoría de los casos (Garriga Domínguez, 2023, p. 124), el tratamiento de esta tipología de datos puede entrañar una notable intromisión en los derechos y libertades fundamentales de la persona titular de estos (considerando 51 RGPD). A este respecto, la AEPD señala reiteradamente en sus resoluciones que una intrusión en el sistema en el que está almacenado el dato biométrico puede suponer un robo de identidad perpetuo (por todas, AEPD, PS/00074/2024). Se trata de una incidencia que además afecta al resto de sistemas en los que la persona trabajadora tenía introducidos sus datos biométricos como, por ejemplo, aplicaciones bancarias o sanitarias

[11] El Grupo de Trabajo del artículo 29 (GT29), en su Dictamen 3/2012 sobre la evolución de las tecnologías biométricas incluyó también como datos biométricos los elementos psicológicos (Rodríguez-Piñero Royo, 2019).

[12] La evitación del fraude es la ventaja por excelencia que proporcionan las tecnologías de biometría. Esto se debe a que, a diferencia de lo que ocurre con las tarjetas magnéticas, los datos biométricos son, en principio, «absolutamente intransferibles» (Selma Penalva, 2010). No obstante, también influye en la decisión de emplearlas el progreso tecnológico que han experimentado estas tecnologías (Rodríguez-Piñero Royo, 2019, p. 92) y el reducido coste de su instalación (Fernández Orrico, 2020).

a las que se accede identificando a la persona usuaria mediante el reconocimiento de su rostro o de su huella dactilar (AEPD, PS/00218/2021).

También debe ser subrayado que los datos biométricos pueden contener información adicional de la persona que identifican referente a su salud, origen étnico o racial, religión e incluso hábitos o lugar de residencia[13] (*European Data Protection Board* –EDPB-, 2023), pudiendo, por tanto, un uso indebido de los mismos acrecentar la injerencia en la vida privada de la persona (Poquet Catalá, 2020)[14].

Es por estas razones por las que el RGPD ha querido otorgar al tratamiento de datos biométricos una protección que podría ser calificada como reforzada o especial (Garriga Domínguez, 2023, p. 120). Y ello parte de la categorización de este tipo de datos como datos de carácter sensible (art. 9.1 RGPD).

Así, atendiendo a los artículos 6, 9 y 35 del RGPD, para poder realizar un tratamiento de datos biométricos, deben ser observados y superados tres elementos[15]. En primer lugar, sobre los datos biométricos, al formar parte de la categoría especial de datos personales, se ciñe una prohibición general de tratamiento (art. 9.1 RGPD), que únicamente puede ser levantada si confluye una de las excepciones descritas en el apartado segundo de dicho precepto. De esta forma, previa instalación de un sistema de reconocimiento facial o de escaneo de la huella dactilar, la empresa deberá cerciorarse de que el tratamiento se encuentra justificado sobre la base de algunas de las excepciones contempladas en el artículo. En segundo lugar, tras quedar levantada la prohibición de tratamiento, se deberá comprobar si concurre una base legitimadora del tratamiento de datos personales; es decir, si el empleo de los datos biométricos es lícito, por cuanto se cumple al menos una de las condiciones descritas en el artículo 6.1 del RGPD (AEPD, 2023). Y, por último, con carácter previo a la instalación del sistema, la empresa tendrá la obligación de elaborar –y superar– una evaluación de impacto relativa a la protección de datos (EIPD), que deberá incluir, entre otros aspectos, una demostración de la idoneidad, necesidad y proporcionalidad del tratamiento

[13] De hecho, el Reglamento de Inteligencia Artificial (Reglamento (UE) 2024/1689, de 13 de junio de 2024) prohíbe, en su artículo 5.1 g):

> La introducción en el mercado, la puesta en servicio para este fin específico o el uso de sistemas de categorización biométrica que clasifiquen individualmente a las personas físicas sobre la base de sus datos biométricos para deducir o inferir su raza, opiniones políticas, afiliación sindical, convicciones religiosas o filosóficas, vida sexual u orientación sexual [...].

[14] Como señala Escajedo San Epifanio (2017), han sido realizados estudios que indican que las peculiaridades de las impresiones dactilares pueden revelar, por ejemplo, la existencia de leucemia, esquizofrenia o trastorno bipolar.

[15] Se recalcan tres elementos, lo que no exime del cumplimiento del resto de los preceptos del RGPD, entre los que se incluyen los principios del tratamiento (art. 5) o el derecho de información (arts. 12, 13 y 14).

(AEPD, 2023), así como una evaluación de los potenciales riesgos para los derechos de las personas trabajadoras y una previsión de medidas concretas para mitigarlos (art. 35.7 RGPD).

Con todo lo expuesto, considerando las exigencias recogidas en la normativa de protección de datos y la obligación de registro del artículo 34.9 del ET, la AEPD entiende que no pueden ser tratados los datos biométricos con fines de control horario.

4. El criterio de la AEPD en el tratamiento de datos biométricos con fines de control horario

Por una parte, la AEPD razona que la empresa inicialmente sí que está legitimada para tratar los datos personales de la plantilla, por cuanto, debido a la existencia de una relación contractual, concurre la base de licitud del artículo 6.1 b): «el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte [...]» (por todas, PS/00545/2023). No obstante, si bien se puede entender superado el artículo 6 del RGPD, la AEPD (2023) recuerda que ello no implica que se permita el tratamiento de datos biométricos, dado que se deberá acreditar el levantamiento de la prohibición que versa sobre el mismo. En este sentido, existen dos excepciones aplicables al presente supuesto: que la persona interesada haya prestado su consentimiento (art. 9.2 a), o que el tratamiento sea necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos de la persona responsable del tratamiento o de la persona interesada 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 de la persona interesada (art. 9.2 b).

4.1. El levantamiento de la prohibición vía artículo 9.2 b) del RGPD

Comenzando por la segunda de ellas, el criterio actual de la AEPD (2023) es conciso: el artículo 34.9 del ET no es lo suficientemente explícito para levantar la prohibición de tratamiento (ni por ende el art. 20.3 ET[16]). Se trata de una interpretación efectuada en vista de la jurisprudencia del Tribunal Constitucional (TC) y del TJUE. Por una parte, el TC en sus

[16] Antes de la introducción del apartado noveno del artículo 34 del ET, la Autoridad Catalana de Protección de Datos, en su Dictamen CNS 63/2018, entendió que la utilización del artículo 20.3 del ET como obligación legal habilitante para el levantamiento de la prohibición de tratamiento de datos biométricos podía generar dudas, por cuanto el precepto en ningún momento hacía referencia a una autorización para el empleo de categorías especiales de datos con fines de control horario o de otro tipo.

Sentencias 76/2019 y 292/2000 indica que cualquier injerencia a un derecho fundamental regulada por ley debe realizarse mediante reglas precisas que permitan previsiblemente conocer los límites que imponen. Siguiendo esta línea, el TJUE ha argumentado, en múltiples resoluciones (p. ej., de 4 de julio de 2023, asunto C-252/21), que el artículo 9.2 del RGPD debe ser interpretado de manera restrictiva, puesto que introduce excepciones a la prohibición de tratamiento de categorías de datos sensibles, que requieren de una especial protección. Atendiendo a la ausencia de mención expresa al tratamiento de datos biométricos, la AEPD (2023) entiende que el artículo 34.9 del ET no incorpora una obligación legal habilitante a la luz del artículo 9.2 b) del RGPD.

4.2. La acreditación de la necesidad del sistema de biometría

Además, el propio artículo 9.2 b) del RGPD exige el cumplimiento de un segundo requisito: la acreditación de la necesidad del tratamiento de esta tipología de datos. Se trata de un supuesto en el que se vincula la legitimidad del tratamiento a la observancia del principio de minimización de datos personales del artículo 5.1 c) del RGPD (Troncoso Reigada, 2021, p. 876).

El principio de minimización de datos implica que solamente serán tratados los datos personales cuando sean adecuados, pertinentes y limitados a lo necesario para los fines previstos. En este sentido, el considerando 39 incluye una puntualización al respecto, indicando que los datos personales únicamente deberán ser empleados si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios. Así, el GT29, en su Dictamen 3/2012 sobre la evolución de las tecnologías biométricas, recoge que «es preciso considerar previamente si el sistema es necesario para responder a la necesidad identificada, es decir, si es esencial para satisfacer esa necesidad» (p. 8). Asimismo, matiza que se debe ponderar si «la pérdida de intimidad resultante es proporcional a los beneficios esperados», entendiendo que la comodidad o el ahorro económico no suponen un beneficio relevante (p. 8).

De esta forma, con el fin de acreditar la necesidad del tratamiento, deben ser analizadas todas las opciones de sistemas de registro disponibles, y razonar por qué ha sido escogida una tecnología de biometría (AEPD, PS/00170/2023) y por qué no existe otro sistema apropiado menos intrusivo para los derechos de las personas trabajadoras (Rodríguez-Piñero Royo, 2020)[17].

[17] A este respecto, se pronunció el Comité de Ministros del Consejo de Europa en la Recomendación CM/Rec (2015) 5 relativa al tratamiento de datos personales en el entorno laboral indicando que: «The collection and further processing of biometric data should only be undertaken when it is necessary to protect the legitimate interests of employers, employees or third parties, only if there are no other less intrusive means available […]».

Este «test de necesidad» está íntimamente relacionado con el juicio de proporcionalidad de la medida implantada (Troncoso Reigada, 2021, p. 882). El GT29, en el Dictamen 2/2017 sobre el tratamiento de datos en el trabajo, razona que, previo tratamiento de los datos personales

> se debe realizar una prueba de proporcionalidad con el fin de determinar si el tratamiento es necesario para lograr un fin legítimo, así como las medidas que deben adoptarse para garantizar que las violaciones de los derechos a la vida privada y al secreto de las comunicaciones se limiten al mínimo (p. 4).

Se trata de una provisión que es reiterada en el artículo 35.7 b) del RGPD, cuando se recoge que la EIPD deberá incluir «una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad».

En este sentido, la AEPD, cuando evalúa la legitimidad de la tecnología de biometría, valora si supera el principio de proporcionalidad a la luz de la doctrina constitucional (AEPD, PS/00074/2024). El TC entiende que la constitucionalidad de cualquier medida restrictiva de derechos fundamentales debe observar el principio de proporcionalidad (por todas, Sentencia 39/2016, de 3 de marzo)[18]; consistente en el cumplimiento de tres requisitos o condiciones: si la medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad), y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto) (por todas, Sentencia 186/200, de 10 de julio).

Bajo estas premisas, en aplicación del principio de minimización de datos y de proporcionalidad, la AEPD descarta, entre otros aspectos, que la elección de la medida se efectúe exclusivamente escogiendo la más rentable (AEPD, PS/00218/2021)[19]. Además, señala que no debe confundirse la necesidad con la utilidad del sistema, por lo que no debe optarse por el medio más práctico o ágil si es más invasivo para la intimidad de las personas trabajadoras (AEPD, PS/00170/2023). Por otra parte, remarca que no puede entenderse acreditado el carácter necesario cuando la empresa indirectamente demuestra que podía aplicar otro sistema menos intrusivo; dado que, por ejemplo, durante la tramitación del expediente, retira

[18] Asimismo, este principio de proporcionalidad es un principio general de la legislación de la Unión Europea (Muñoz Ruiz, 2023, p. 34), por cuanto se encuentra recogido en el artículo 52.1 de la Carta de los Derechos Fundamentales de la Unión Europea, que indica que, respecto a los derechos y libertades de la carta: «Solo se podrán introducir limitaciones, respetando el principio de proporcionalidad, cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás».

[19] En este sentido, se pronuncia igualmente el GT29, en su Dictamen 3/2012 (p. 8).

el sistema de reconocimiento facial e implementa un sistema de tarjetas eficaz para el cumplimiento de la misma obligación (AEPD, PS/00361/2023). Por último, la AEPD no considera que sea suficiente acreditar o argumentar que el sistema de biometría no guarda la imagen del rostro o de la huella dactilar en sí. En ocasiones, la tecnología empleada crea una plantilla biométrica, a partir de unos patrones extraídos del rasgo personal, guardando exclusivamente unos puntos de este y no almacenando la imagen completa (Muñoz Ruiz, 2023, p. 27). La AEPD entiende, a este respecto, que, si bien se trata de una medida de seguridad, no determina que el sistema no suponga un riesgo para la protección de los datos de las personas afectadas, por cuanto, la plantilla o *hash* permite identificar inequívocamente a la persona trabajadora (de lo contrario, no cumpliría su función) (entre otras, PS/00361/2023).

4.3. El levantamiento de la prohibición vía artículo 9.2 a) del RGPD: consentimiento

Quedando descartada la posibilidad de levantar la prohibición vía artículo 9.2 b) del RGPD –a criterio de la autoridad española–, cabe analizar si pudiera alzarse mediante el consentimiento de las personas trabajadoras afectadas por la instalación de un sistema de registro biométrico (art. 9.2 a) RGPD). Para dar respuesta a este planteamiento, se debe tener en cuenta la naturaleza de las relaciones laborales (Todolí Signes, 2022). El desequilibrio contractual existente entre las partes se contagia a cualquier tratamiento de datos personales que pueda ocurrir en el lugar de trabajo (Cruz Villalón, 2020). Esta circunstancia dificulta que pueda entenderse cumplido uno de los requisitos que exige el RGPD para interpretar que el consentimiento ha sido válidamente prestado: que el mismo sea libre[20] (art. 4.11 y considerando 43[21]).

Sobre esta materia, se pronunció el GT29 en sus Directrices sobre el consentimiento en el sentido del Reglamento 2016/679, señalando que, atendiendo a la dependencia que caracteriza la relación entre la parte empleadora y la parte empleada, difícilmente podía interpretarse que la persona trabajadora tenía la capacidad de negar el consentimiento «sin experimentar temor o riesgo real de que su negativa produzca efectos perjudiciales» (p. 7). A este respecto, el TS, en su Sentencia de 21 de septiembre de 2015 (rec. 259/2014), consideró que el consentimiento no podía ser libre y voluntario por completo cuando la cláusula que autorizaba a la empresa a tratar los datos personales se encontraba incluida en el pro-

[20] No puede calificarse como libre un consentimiento prestado por una persona que no se encuentra en una «situación real de poder elegir» (Del Castillo Vázquez, 2021, p. 952).

[21] El considerando 43 puntualiza 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 [...].

pio contrato de trabajo inicial. Y ello debido a que, en estos supuestos, existe el temor de la persona trabajadora a no ser contratada si muestra su desacuerdo (Todolí Signes, 2021a).

No obstante, las dificultades que plantea la naturaleza de las relaciones laborales no impiden que el consentimiento pueda entenderse libremente prestado, siempre y cuando, como indica el GT29 en las Directrices sobre el consentimiento en el sentido del Reglamento 2016/679, la empresa así lo demuestre (p. 7). En este sentido, el EDPB, en sus *Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679* (adoptada el 4 de mayo de 2020) (EDPB, 2020)[22], plantea una opción para revertir ese desequilibrio que se genera entre las partes. Así, se contempla la posibilidad de que el consentimiento sea libre si la persona trabajadora dispone de una forma alternativa para dar cumplimiento a la obligación de registro que no implique la prestación del consentimiento –por cuanto no se requiera el empleo de datos sensibles–, y a condición de que la elección efectuada no tenga consecuencias adversas y se trate de servicios equivalentes (en interpretación de los apdos. 22 y 37). De esta forma, el consentimiento para el tratamiento de datos biométricos con fines de control horario podría ser válido si la persona trabajadora tuviera la opción de cumplir el deber de fichar el inicio y el fin de la jornada, en las mismas condiciones (idéntico momento y lugar), con un sistema que no exigiese su consentimiento como podría serlo el empleo de una clave PIN.

En este sentido, la AEPD (2023) entiende que si existe una alternativa que no implica el tratamiento de datos sensibles significa que la tecnología de biometría no sería estrictamente necesaria. Por lo que, nuevamente, en términos generales –salvo que la empresa acreditase que el consentimiento es libre–, quedaría impedido el levantamiento de la prohibición, en este caso, vía consentimiento en relación con la preceptiva observancia del principio de necesidad.

4.4. La obligación de efectuar una EIPD

Por último, el RGPD, en el artículo 35.1, establece que es obligatoria la realización de una EIPD[23] cuando sea probable que el tratamiento «entrañe un alto riesgo para los derechos y libertades de las personas físicas». Con el fin de concretar los tratamientos que implican un alto riesgo, la norma europea reconoce a las autoridades de control la facultad de elaborar y publicar una lista de los tipos de operaciones de tratamiento que requieran de una evaluación de impacto (apdo. cuarto). A este respecto, la AEPD elaboró la Listas de

[22] https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_es.pdf

[23] A este respecto, la AEPD publicó en junio de 2021 una Guía sobre la gestión del riesgo y evaluación de impacto en tratamientos de datos personales (https://www.aepd.es/guias/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf) en la que se detallan las instrucciones necesarias para la elaboración de la EIPD.

tipos de tratamiento de datos que requieren evaluación de impacto relativa a protección de datos (art. 35.4) (publicada el 6 de mayo de 2019), en la que incluyó expresamente los tratamientos que impliquen el uso de datos biométricos con el propósito de identificar de manera única a una persona física.

Dicho esto, es relevante matizar que el deber de realizar una evaluación de impacto se enmarca en la obligación general de la persona responsable de gestionar adecuadamente los riesgos derivados del tratamiento (art. 24.1 RGPD); es decir, forma parte de las medidas de responsabilidad proactiva (Muñoz Ruiz, 2023, p. 77)[24]. Así es indicado por el GT29, en sus Directrices sobre la EIPD y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679, cuando reconoce que la EIPD es un «proceso concebido para describir el tratamiento, evaluar su necesidad y proporcionalidad y ayudar a gestionar los riesgos para los derechos y libertades de las personas físicas derivados del tratamiento de datos personales evaluándolos y determinando las medidas para abordarlos» (p. 4).

De esta forma, en la EIPD, aparte de demostrar que el sistema supera el triple juicio de proporcionalidad, se deberá incluir necesariamente un análisis de los riesgos (incluida la tasa de falsa aceptación[25]) y una descripción de las medidas técnicas, organizativas y de seguridad implementadas (AEPD, PS/00170/2023, PS/00074/2024), tales como: la codificación de la plantilla o el no almacenamiento de esta en internet (AEPD, PS/00361/2023). Además, se trata de una obligación que debe completarse, en todo caso, en un momento anterior a la instalación del sistema e incluso previa decisión de su implantación[26]. Por ello, se descarta que pueda elaborarse cuando la decisión ya estaba avanzada (AEPD, PS/00419/2024).

[24] Las consecuencias negativas en los derechos y libertades de las personas trabajadoras que pueden surgir de no haber mitigado correctamente los riesgos «pueden suponer la comisión de diversas infracciones (por ejemplo: incumplimiento de obligaciones o principios, o bien no atender adecuadamente a derechos de las personas afectadas)» e incluso «pueden llegar a producir daños y perjuicios materiales o morales, algunos irreparables» (Miralles López, 2021, p. 2155). En todo caso, no realizar la EIPD cuando es obligatoria puede ser sancionado con hasta 10.000.000 euros o hasta una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior (art. 83.4 a) RGPD).

[25] Respecto a este punto, es relevante señalar que el reconocimiento biométrico no es una tecnología infalible. Por ello, se debe hacer un estudio de la probabilidad de que el sistema rechace a un individuo registrado o acepte a otro que no lo está. Como remarca Escajedo San Epifanio (2017), se debe tener en cuenta la tasa de aceptación errónea y la tasa de falso rechazo.

[26] El GT29, en las Directrices sobre la EIPD (adoptadas el 4 de abril de 2017), aparte de mencionar que «la EIPD debe iniciarse tan pronto como sea viable en el diseño de la operación de tratamiento incluso aunque algunas de las operaciones de tratamiento no se conozcan aún», remarca que se trata de un proceso continuo que debe actualizarse cuando se producen cambios (p. 16).

En términos generales, la AEPD concibe la EIPD como un verdadero juicio que debe superarse (PS/00170/2023), y no, según señala en la Guía sobre gestión del riesgo y evaluación de impacto en tratamientos de datos personales, como un mero trámite formal «plasmado en un documento sobre el que se puedan realizar cambios mínimos para adaptarlo a cualquier tratamiento» (p. 25). Igualmente, resulta de interés remarcar que, aunque pueda servir para demostrar la observancia de las exigencias del RGPD (p. ej., si se plasma en la evaluación cuál es la base legitimadora del tratamiento)[27], la verificación del cumplimiento normativo es un requisito previo a su ejecución. Así, la AEPD –en el documento titulado: Lista de verificación para determinar la adecuación formal de una EIPD y la presentación de consulta previa[28]– entiende que «la ausencia de una base jurídica constituiría un requisito no subsanable mediante otras medidas de cumplimiento» (p. 10).

En atención a las particularidades de la evaluación de impacto, las resoluciones de la AEPD suelen sancionar a las personas responsables por incumplir con el deber del artículo 35 del RGPD; principalmente debido a la ausencia de elaboración de este proceso (AEPD, PS/00074/2024, PS/00361/2023) y a la no superación del principio de proporcionalidad (AEPD, PS/00419/2024, PS/00170/2023).

Por todo lo expuesto, se puede concluir que, en definitiva, el criterio de la AEPD descarta cualquier posibilidad de interpretar que el tratamiento de datos biométricos con fines de registro horario –a la vista del art. 34.9 ET– se adecúa a la normativa de protección de datos. No obstante, esta posición garantista del derecho a la protección de datos que ostenta la AEPD entra en contraposición con la línea jurisprudencial sostenida en la materia hasta la fecha.

5. Mayor permisibilidad del tratamiento de datos biométricos por la jurisprudencia antes de la aprobación del RGPD

En 2007, el TS se pronunció sobre la licitud del empleo de un sistema de control de horario –instaurado por el Gobierno de Cantabria– que funcionaba a través de la lectura biométrica de la mano de las personas trabajadoras. En su Sentencia de 2 de julio de 2007 (Sala de lo Contencioso-administrativo, rec. 5017/2003), reconoció que el uso de esta tecnología no suponía una vulneración del artículo 18 de la Constitución española (CE), sino que respondía a una finalidad «plenamente legítima» (FJ 7). En referencia al mismo sistema de registro, el TC, en el Auto 57/2007, de 26 de febrero, inadmitió un recurso de amparo

[27] Esta facultad es detallada por el GT29, en las Directrices sobre la evaluación de impacto (p. 4).

[28] Se trata de uno de los documentos elaborados por la AEPD para ayudar a las personas responsables del tratamiento a elaborar la EIPD: https://www.aepd.es/documento/lista-verificacion-eipd-consulta-previa.docx

por carecer de contenido constitucional, al entender que la tecnología implantada por la Administración cántabra no lesionaba el derecho a la intimidad, pues había sido adoptada en atención a la normativa en materia de protección de datos (FJ 6).

Con parejo razonamiento se dictó, previamente, la Sentencia del Tribunal Superior de Justicia (TSJ) de Cantabria, Sala de lo Contencioso-administrativo, de 10 de enero de 2003 (rec. 517/2002). En ella el TSJ reconoció la validez y eficacia de este tipo de tecnologías, señalando el «carácter imperfecto de los sistemas de control más comúnmente usados, tanto el sistema de firma, por su posible manipulación, como el sistema de reloj y ficha, por no impedir la sustituibilidad en su cumplimiento» (FJ 9). Con posterioridad, el TSJ de la Región de Murcia, Sala de lo Social, en su Sentencia 47/2010, de 25 de enero, consideró que el sistema electrónico de captación de huella digital que la empresa aplicaba no revestía «caracteres de intromisión ilegítima en la esfera de la intimidad».

Más adelante, la AN, en su Sentencia de 19 de septiembre de 2019 (rec. 774/2018), aun refiriéndose a un tratamiento de datos biométricos en un contexto ajeno al laboral (acceso de la clientela a un gimnasio vía escáner de huella dactilar), revocó la sanción impuesta por la AEPD a la empresa, reconociendo que la medida superaba el principio de proporcionalidad. La AN argumentó que el sistema de acceso aparte de idóneo era necesario, debido a que evitaba el intercambio de tarjetas –y, por tanto, el intrusismo y el fraude–, y proporcional en sentido estricto, dado que la empresa había incorporado garantías en el tratamiento, consistentes en no almacenar la huella en el sistema (sino el algoritmo) y en no emplear los datos con un fin distinto (FJ 5).

Si bien estas resoluciones consideraron apropiado el tratamiento de datos biométricos, debe ser señalado que fueron promulgadas a la luz de la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal –normativa derogada–, que no incluía los datos biométricos dentro de la categoría de datos especialmente protegidos (art. 7).

En este sentido, cabe remarcar que el poder legislativo europeo en el RGPD vierte una prohibición de tratamiento y, por tanto, una reforzada protección sobre determinadas tipologías de datos porque considera que, por su naturaleza, el uso de estos datos «podría entrañar importantes riesgos para los derechos y las libertades fundamentales» (considerando 51)[29]. Esta naturaleza a la que se alude hace referencia a la estrecha vinculación de los datos sensibles con las características más delicadas o íntimas de las personas, ligadas directamente con su dignidad (Rebollo Delgado, 2021, p. 1016). Es por esta razón por la que la posterior introducción de los datos biométricos en la categoría de datos sen-

[29] Aunque también se encontraba esta prohibición de tratamiento en el artículo 8.1 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 respeta al tratamiento de datos personales y a la libre circulación de estos datos; provisión que, no obstante, no incluía los datos biométricos.

sibles y el reconocimiento legal de su carácter especialmente vulnerable podría conducir a un cambio en el criterio sostenido por los tribunales. Así, aunque no constituye jurisprudencia, la Sentencia del Juzgado de lo Social n.º 2 de Alicante, 190/2023, de 15 de septiembre, avanza en esta línea; al haber estimado la vulneración del derecho a la intimidad de un trabajador, cuya imagen había sido captada, para cumplir con la obligación de registro, sin su consentimiento expreso, sin el ofrecimiento de un sistema alternativo y sin haber efectuado la previa EIPD[30].

Sin embargo, cabe señalar que tampoco puede asegurarse firmemente que esta variación en el juicio vaya a trasladarse a la jurisprudencia y doctrinal judicial, al menos de manera uniforme. Y ello principalmente debido al hecho de que la jurisprudencia de los últimos años tiende a considerar la observancia de la legislación en materia de protección de datos como una cuestión de legalidad ordinaria en algunas materias (Todolí Signes, 2022, p. 238). Además, equipara la exigencia de acreditar la «necesidad» del tratamiento (plasmada tanto en el principio de proporcionalidad como en el propio art. 9.2 b) RGPD) con la conveniencia de la medida empresarial (Todolí Signes, 2022, p. 242). De esta forma, a diferencia del criterio empleado por la AEPD, quien sí que exige que se acredite que el sistema es insustituible por otro menos intrusivo, los tribunales, como realizó la AN en la Sentencia de 19 de septiembre de 2019, se focalizan, más bien, en la eficacia e idoneidad de la tecnología.

Así, el hecho de que la jurisprudencia y la AEPD mantengan posiciones interpretativas –hasta la fecha– dispares genera inseguridad jurídica tanto para las personas trabajadoras que pueden ver lesionados sus derechos fundamentales, como para las empresas que se plantean implantar los sistemas de control biométrico (Rodríguez-Piñero Royo, 2019, p. 104).

En atención a lo expuesto, es importante analizar las implicaciones que tendrá la reforma del artículo 34.9 del ET planteada por el proyecto de Ley para la reducción de la duración máxima de la jornada ordinaria de trabajo y la garantía del registro de jornada y el derecho a la desconexión. Si bien esta reforma podría ser empleada para reforzar la protección de los derechos fundamentales de las personas trabajadoras y zanjar el debate sobre la posibilidad de emplear datos biométricos (p. ej., prohibiendo definitivamente las tecnologías biométricas de registro horario), el texto que se propone, en mi opinión, no contribuye sino a mantener la disparidad de criterios y a reforzar incluso la idea de que el tratamiento de datos biométricos, en estos supuestos, es idóneo, necesario y proporcional.

[30] Además, se encuentra la Sentencia del TS de 15 de enero de 2025 (Sala de lo Social, rec. 136/2023) que, si bien se refiere a los datos relativos al registro salarial, consideró que la empresa no estaba obligada a proporcionar información que permitiese identificar de forma inequívoca la retribución individualizada de una persona trabajadora porque no había norma con rango de ley que lo previese.

6. Las implicaciones de la reforma del registro de jornada planteada por el proyecto de Ley para la reducción de la duración máxima de la jornada ordinaria de trabajo y la garantía del registro de jornada y el derecho a la desconexión

El 4 de febrero de 2025, el Consejo de Ministros, con tramitación por vía de urgencia, aprobó el anteproyecto de Ley para la reducción de la duración máxima de la jornada ordinaria de trabajo, el registro de jornada y el derecho a la desconexión. Posteriormente, el anteproyecto de ley fue aprobado por el Consejo de Ministros, en su segunda vuelta, el 6 de mayo de 2025; iniciando así la propuesta normativa su tramitación parlamentaria. Es por ello por lo que el 16 de mayo de 2025 se publicó en el Boletín Oficial de las Cortes Generales el proyecto de Ley para la reducción de la duración máxima de la jornada ordinaria de trabajo y la garantía del registro de jornada y el derecho a la desconexión.

Se trata de un proyecto de ley que, si bien todavía debe superar los pertinentes trámites parlamentarios, plantea una reforma del ET, en diversos ámbitos, siendo uno de ellos el registro de la jornada diaria.

Así, el proyecto de ley decide suprimir el contenido del apartado noveno del artículo 34 del ET y crear un nuevo precepto bajo la denominación de artículo 34 bis. Por una parte, el articulado propuesto –si se mantiene en idénticos términos– recoge, en su apartado primero, que: «La empresa mantendrá un registro diario de jornada, realizado por medios digitales, que garantice el cumplimiento efectivo de los requisitos previstos en este artículo. [...]». De esta forma, la obligación legal de efectuar un registro diario de jornada se ve complementada con el deber empresarial de ejecutarlo a través de medios digitales.

Por otra parte, continuando con las modificaciones propuestas, el apartado segundo, introduce el deber de garantizar «la objetividad, la fiabilidad y la accesibilidad del registro de jornada». Y para el cumplimiento de estas garantías, establece cinco premisas concretas, siendo las dos primeras de interés para el presente estudio:

> a) Las personas trabajadoras practicarán los asientos de forma personal y directa, inmediatamente al inicio y finalización de cada jornada, de forma que la empresa no pueda condicionar su contenido [...] [, y]
>
> b) Para garantizar la autenticidad y la trazabilidad de los datos reflejados en el registro, este deberá permitir identificar inequívocamente a la persona trabajadora que lo realiza, así como las eventuales modificaciones de los asientos efectuados.

Por último, debe ser señalado que se remite a la negociación colectiva y al desarrollo reglamentario para la concreción de las especificidades relativas al registro (apdos. 5 y 6).

En este punto, cabe plantearse si los cambios introducidos en el precepto podrían conllevar un cambio en el criterio sostenido por la AEPD. En otras palabras, cabe analizar si la obligación de registro horario en los términos propuestos podría ser suficiente para levantar la prohibición de tratamiento de datos biométricos, sobre la base del artículo 9.2 b) del RGPD. La respuesta a esta pregunta requiere, en primer lugar, considerar si la forma en la que ha sido configurado el deber de registro es lo suficientemente concreta para entender que habilita al tratamiento de datos biométricos, y, en segundo lugar, si, de acuerdo con la redacción propuesta, las tecnologías de biometría superarían el principio de proporcionalidad.

6.1. La concreción de la obligación de registro

Respecto a la primera cuestión planteada, es de interés traer a colación de nuevo la jurisprudencia del TC. En la Sentencia 76/2019, de 22 de mayo, el TC reconoce que las limitaciones de un derecho fundamental establecidas por una ley «pueden vulnerar la Constitución si adolecen de falta de certeza y previsibilidad en los propios límites que imponen y su modo de aplicación»; y añade que la falta de precisión supone que «la ley ya no cumple su función de garantía del propio derecho fundamental que restringe, pues deja que en su lugar opere simplemente la voluntad de quien ha de aplicarla» (FJ 5). En similar sentido se pronuncia también la jurisprudencia del TJUE y del Tribunal Europeo de Derechos Humanos (TEDH), indicando que una norma que posibilite una injerencia en los derechos fundamentales de los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la UE (derecho al respeto de la vida privada y familiar y derecho a la protección de datos de carácter personal):

> [...] debe contener reglas claras y precisas que regulen el alcance y la aplicación de una medida e impongan unas exigencias mínimas, de modo que las personas cuyos datos personales resulten afectados dispongan de garantías suficientes que permitan proteger eficazmente sus datos personales contra los riesgos de abuso [...] (FJ 91 STJUE de 6 de octubre de 2015, asunto C-362/14; FJ 52 STEDH de 4 de julio de 2023, demanda n.º 11519/20)[31].

[31] Así, el TEDH en la Guide on Article 8 of the European Convention on Human Rights (actualizada el 31 de agosto de 2024), donde aborda extensamente las implicaciones del derecho fundamental al respeto a la vida privada y familiar recogido en el artículo 8 del Convenio Europeo de Derechos Humanos, indica que:

> The national law must be clear, foreseeable, and adequately accesible [...] It must be sufficiently foreseeable to enable individuals to act in accordance with the law» (p. 11). Además, respecto a la incorporación de garantías en la norma, establece que: «Lawfulness" also requires that there be adequate safeguards to ensure that an individual's Article 8 rights are respected. Domestic law must provide adequate safeguards to offer the individual adequate protection against arbitrary interference (p. 12).

En este sentido, siendo que la utilización de datos biométricos puede implicar una injerencia en el derecho a la intimidad y/o en el derecho a la protección de datos –teniendo en cuenta además que pertenecen a la categoría de datos especialmente protegidos–[32], la ley que habilite su tratamiento debería ser clara y expresa al respecto. En este contexto, las disposiciones introducidas por el proyecto de ley, de igual forma que el artículo 34.9 del ET, carecen de cualquier tipo de referencia al empleo de tecnologías de biometría y al derecho a la protección de datos de las personas trabajadoras.

Además, aunque podría ser razonado que las concreciones que incorpora el proyecto de ley, es decir, el deber de emplear sistemas digitales y de garantizar inequívocamente la identidad de la persona trabajadora, implican indirectamente una habilitación al tratamiento de datos biométricos, cabe realizar dos matices al respecto. Por una parte, que, de nuevo, estos requisitos no equivalen a un pronunciamiento conciso sobre el uso de esta tipología de datos, y, por otra, que no introducen cambios sustanciales en consideración a la normativa vigente y la jurisprudencia promulgada sobre la materia. Y ello sobre la base de los siguientes argumentos:

1. La obligación de utilizar medios digitales no reduce las posibilidades al empleo de sistemas de reconocimiento facial o de escaneo de huella dactilar. Esta especificación parece responder, más bien, a la necesidad de garantizar el inmediato acceso al registro por parte de las personas trabajadoras, sus representantes legales y la Inspección de Trabajo y Seguridad Social, así como a la necesidad de establecer herramientas que permitan poner a disposición la información en un formato tratable, legible y compatible con los de uso generalizado (art. 34 bis apdos. 2 c) y 2 d). A este respecto, si bien el artículo 34.9 del ET no contempla el deber de emplear sistemas digitales, las exigencias que de él derivan indirectamente postulaban las herramientas digitales como los sistemas idóneos para el cumplimiento de estas. En este sentido, se pronunció la AN, en su Sentencia 22/2022, de 15 de febrero, en la que declaró que el sistema de registro empleado por la empresa, consistente en la firma de la persona trabajadora en un papel no se ajustaba a lo dispuesto en el artículo 34.9 del ET. La AN, aparte de razonar que no se trataba de un sistema fiable que acreditase la jornada diaria, entendió que imponía trabas a una posible puesta a disposición de la información a la persona trabajadora, la representación legal de las personas trabajadoras y la Inspección de Trabajo (FJ 4). De esta forma, la conducción del registro horario mediante medios digitales podría considerarse una concreción efectuada a la luz de la doctrina judicial previa.

[32] En este sentido, el EDPB (2023, p. 5) expone que:

> Las medidas legislativas que sirven de base jurídica para el tratamiento de datos personales interfieren directamente en los derechos garantizados por los artículos 7 y 8 de la Carta. El tratamiento de datos biométricos constituye en sí mismo una grave injerencia en cualquier circunstancia y con independencia del resultado.

2. Las letras a) y b) del apartado segundo, aun cuando mencionan que el asiento debe ser practicado de forma personal y asegurando la identificación inequívoca de la persona trabajadora, suponen realmente una precisión de las garantías de objetividad, fiabilidad y accesibilidad. Como es indicado en el propio preámbulo del borrador del anteproyecto[33], la observancia de estos tres principios o requisitos ya era previamente requerida para dar cumplimiento a la Directiva 2003/88/CE, de acuerdo con la interpretación efectuada por el TJUE en su Sentencia de 14 de mayo de 2019, y plasmada en el Criterio Técnico 101/2019 de la Inspección de Trabajo (Gómez-Millán Herencia, 2020, p. 243).

Se puede concluir, por todo ello, que el criterio sostenido por la AEPD no tendría por qué variar sobre este punto. En mi opinión, la ausencia de un pronunciamiento preciso sobre el empleo de tecnologías de biometría –y de modificaciones relevantes– impide entender que la normativa alza la prohibición de tratamiento.

6.2. La superación del principio de proporcionalidad

Por otra parte, aunque se alcanzase la conclusión de que sí que puede ser aplicada la excepción del artículo 9.2 b) del RGPD, la persona responsable del tratamiento, es decir, la empresa, debería, en todo caso, demostrar que el sistema biométrico de registro horario es idóneo, necesario y proporcional en sentido estricto.

Así, no puede negarse que la medida es plenamente idónea para el cumplimiento del fin previsto, por cuanto permite no solamente controlar la jornada de las personas trabajadoras, sino también mitigar el fraude en el fichaje (por traspaso de tarjetas o comunicación del PIN de acceso, entre otros) y el robo de las credenciales (Muñoz Ruiz, 2023, p. 36)[34]. Sin embargo, es esta misma característica de los sistemas biométricos la que ocasiona que los juicios de necesidad y de proporcionalidad en sentido estricto presenten una mayor controversia.

Como ha sido anteriormente indicado, la necesidad del tratamiento implica demostrar que no existen otras medidas menos intrusivas que sean eficaces para el cumplimiento del

[33] Véase el borrador publicado inicialmente en el siguiente enlace: https://expinterweb.mites.gob.es/participa/listado/download/58e3800b-9e2c-4ff1-9dd2-316d5792d396

[34] La *European Data Protection Board* también indica, en las Directrices 3/2019 sobre el tratamiento de datos personales mediante dispositivos de vídeo (adoptadas el 29 de enero de 2020), que las tecnologías de biometría pueden ser percibidas como particularmente eficaces. No obstante, expone que ello no excluye que deba ser evaluado su impacto en los derechos y libertades fundamentales y deban ser considerados otros medios menos intrusivos para lograr el fin legítimo del tratamiento (apdo. 73). https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_es.pdf

deber de registro[35]. En este sentido, un factor que asiduamente es empleado por la empresa, en los procedimientos ante la AEPD, para justificar la necesidad de la instalación de sistemas de biometría es su fiabilidad en la identificación de las personas trabajadoras (p. ej., AEPD, PS/00218/2021, PS/00419/2024, PS/00170/2023). Con la introducción de las modificaciones planteadas por el proyecto de ley podría entenderse que la necesidad se encuentra aún más justificada por el deber expreso de la norma de que el sistema identifique inequívocamente a la persona trabajadora y acredite que los asientos sean practicados de forma personal y directa. Ahora bien, la fiabilidad exigida no puede equipararse con una ausencia absoluta de errores o posibilidades de fraude, por cuanto se produciría la paradoja de que ni tan siquiera los sistemas de reconocimiento facial o de escaneo de huella dactilar serían válidos para la observancia de la obligación de registro[36]. Esta tecnología está basada en probabilidades que no garantizan un 100 % de precisión y que, además, podrían permitir una suplantación de la identidad; p. ej., empleando una simulación en silicona del dedo de la persona trabajadora con su huella dactilar (Escajedo San Epifanio, 2017).

Es por ello por lo que para valorar si existen medidas eficaces menos intrusivas resulta recomendable basarse en si los sistemas presentan «niveles adecuados de calidad» (AEPD, 2023, p. 18). Así, el hecho de que una tecnología pueda dar lugar al fraude no tiene por qué ser incompatible con un estándar apropiado de calidad, teniendo en cuenta, en todo caso, que las posibles irregularidades podrían ser mitigadas mediante el uso de medidas disciplinarias (AEPD, PS/00218/2021). A la luz de estas consideraciones, cabe señalar que, en mi opinión, deviene complejo superar el principio de necesidad, atendiendo al criterio sostenido por la AEPD en sus resoluciones –que ya ponderaban el factor de la fiabilidad–, por cuanto, generalmente existirán otros mecanismos digitales de registro adecuados que no impliquen el tratamiento de datos biométricos[37].

[35] Véase el *Manual para la evaluación de la necesidad de las medidas que limiten el derecho fundamental a la protección de datos de carácter personal*, elaborado y publicado el 11 de abril de 2017 por el *European Data Protection Supervisor*. https://www.aepd.es/documento/guia-evaluar-necesidad-tratamientos-en-politicas-y-medidas-legislativas.pdf

[36] Muñoz Ruiz (2023, p. 27) recalca que la huella digitalizada tiene una correspondencia al 96 % con un individuo, «lo que significa que existe una determinada tasa de falsos positivos (da por buena una suplantación) y falsos negativos (rechaza a un individuo autorizado)».

[37] A este respecto, resulta interesante traer a colación la normativa de otros países. En este sentido, Escajedo San Epifanio (2015, p. 178) indica que:

> Noruega, en su normativa de protección de datos, ha establecido con claridad que los números de identidad nacional y otros medios «claramente identificativos», como considera su Inspector Nacional de protección de datos que lo son algunos tipos de datos biométricos, solo deben emplearse cuando existe una «necesidad objetiva de identificación» y sobre esta base prohibió algunos usos, como el control horario de los empleados.

Una conclusión pareja se obtiene del juicio de proporcionalidad en sentido estricto[38]. Un incremento de la eficacia del sistema no compensa aparentemente la injerencia en el derecho a la protección de datos y en el derecho a la intimidad; a causa de las consecuencias de una hipotética brecha de seguridad[39], y a la posibilidad de afectar a otros derechos fundamentales, debido a la facultad de las tecnologías de biometría de obtener información personal adicional –como datos relativos a la salud de la persona trabajadora– (Muñoz Ruiz, 2023, p. 31)[40].

Por todo lo expuesto, desde mi punto de vista, las modificaciones planteadas por el proyecto de ley no deberían conducir *a priori* a un cambio del criterio de la AEPD ni, por tanto, a un levantamiento de la prohibición de tratamiento de datos biométricos del artículo 9.2 b) del RGPD.

No obstante, sí que cabe contemplar que podría, por el contrario, respaldar la línea jurisprudencial tendente a reforzar la legitimidad de las facultades empresariales de control. El hecho de que el articulado propuesto prevea expresamente que se debe garantizar inequívocamente la identidad de la persona trabajadora, puede derivar en que la jurisprudencia considere que los sistemas de biometría son necesarios para el fin de control horario; especialmente si se tiene en cuenta que –como ha sido remarcado con anterioridad– los tribunales emplean, más bien, un criterio de conveniencia de la medida adoptada (Todolí Signes, 2022).

En consecuencia, para evitar de nuevo una disparidad de criterios y adoptar una posición garantista de los derechos fundamentales de las personas trabajadoras, en mi opinión, la reforma propuesta podría haber sido empleada para incluir: directamente una prohibición al tratamiento de datos biométricos con fines de control horario, o al menos unas reglas claras para que, vía negociación colectiva, se habilite su tratamiento exclusivamente en aquellos supuestos en los que sea necesario su uso por las circunstancias de la actividad[41]. Y, en todo caso, con unas garantías concretas de carácter técnico que podrían consistir o partir de: que el sistema no guarde el dato biométrico, que el mismo no sea almacenado en in-

38 Véanse las *Directrices del SEPD para la evaluación de la proporcionalidad de las medidas que limitan los derechos fundamentales a la intimidad y a la protección de los datos personales*, elaboradas y publicadas el 19 de diciembre de 2019 por el *European Data Protection Supervisor* (SEPD, 2019). https://www.edps.europa.eu/system/files/2021-12/19_12_19_edps_proportionality_guidelines_es.pdf

39 Además, sobre este punto se ha pronunciado el Comité Económico y Social en el Dictamen 1/2025 (sobre el anteproyecto de ley) indicando que: «debieran contemplarse cuantas medidas y salvaguardas sean necesarias en materia de ciberseguridad para minimizar el elevado riesgo de ataques informáticos que *a priori* comporta la interoperabilidad del registro y la accesibilidad remota desde diferentes organizaciones y servidores informáticos» (p. 15).

40 Por ejemplo, la Magistratura laboral austriaca considera que este uso de los datos biométricos supone un control de alta intensidad para un objetivo relativamente «trivial» (Escajedo San Epifanio, 2015, p. 231).

41 En este sentido, se entiende que es especialmente eficaz para aquellas empresas cuya actividad se desarrolle con horarios flexibles, jornadas irregulares o teletrabajo (Poquet Catalá, 2020).

ternet, que se conserven los datos de manera cifrada y que se implementen medidas técnicas para impedir el uso de las plantillas biométricas con un fin distinto (Fernández Orrico, 2020; AEPD, 2023, p. 28). No obstante, dado que la norma no se pronuncia al respecto, cabe acudir a la negociación colectiva.

7. El papel de la negociación colectiva

En este contexto, ante la ausencia de pronunciamiento por parte de la normativa laboral –tanto en lo referente a la habilitación de tratamiento de los datos biométricos como a la inclusión de garantías–, la negociación colectiva es dispuesta como la herramienta para completar estas lagunas; por cuanto el articulado se remite a ella. No obstante, no parece proporcionado, o es al menos cuestionable, que la norma delegue en la negociación colectiva la misión de corregir la «desregulación» existente en la materia (Todolí Signes, 2022, p. 247). Esta remisión, desprovista de cualquier indicación, en ocasiones, puede resultar asimismo perjudicial para los derechos fundamentales de las personas trabajadoras (Cruz Villalón, 2020)[42].

En principio, el RGPD contempla la negociación colectiva como un mecanismo a través del cual los Estados miembros pueden introducir «normas más específicas para garantizar la protección de los derechos y libertades en relación con el tratamiento de datos personales de los trabajadores en el ámbito laboral» (art. 88.1 RGPD y Considerando 155). Así, la normativa europea reconoce a los convenios colectivos la capacidad de legislar garantías adicionales para la tutela del derecho a la protección de datos (Garrigues Giménez, 2022). Por ejemplo, el Convenio colectivo del Sector Comercio del Mueble 2022-2026 (Resolución 4 de agosto de 2023[43]), en su artículo 71, recoge que:

> La instalación de elementos de controles biométricos en el centro o puesto de trabajo requerirá la aceptación del trabajador y deberá ser consultado a la representación de los trabajadores. En todo caso, en el tratamiento de datos la empresa se regirá por el principio de intervención mínima y proporcionalidad al fin pretendido, así como por las disposiciones comunes contenidas en este título, debiendo llevar a cabo, antes del mismo, una evaluación de impacto […].

[42] Así, Cruz Villalón (2020) indica que:

> A estos efectos, la intervención del legislador estatal ha podido presentarse igualmente como contradictoria: de un lado, con una lógica de fomento de la intervención de actuación complementaria por parte del convenio colectivo enriquecedora de las potencialidades de este como instrumento de profundización del disfrute de los derechos fundamentales; de otro lado, siendo el legislador estatal el que ofrece las posibilidades, incluso las propicia, de que el convenio colectivo se convierta en instrumento lesivo de los derechos fundamentales en lo laboral.

[43] Publicado en el Boletín Oficial de la Comunidad de Madrid el 23 de agosto de 2023.

Se trata, pues, de una disposición que añade el deber de consulta a los órganos de representación de las personas trabajadoras.

Sin embargo, adicionalmente a esta habilidad de la negociación colectiva, el RGPD, en el artículo 9.2 b), prevé expresamente que la obligación que permite levantar la prohibición de tratamiento de datos biométricos pueda estar contemplada en un convenio colectivo (Mercader Uguina, 2023, p. 40). A este respecto, es relevante señalar que el propio RGPD reconoce a los Estados miembros un «margen de maniobra» para especificar las normas que versan sobre el tratamiento de datos sensibles –en él incluidas– (considerando 10). Trasladada esta facultad al ámbito laboral, el considerando 52 recuerda igualmente que cuando así lo establezcan los Estados miembros se podrán autorizar «excepciones a la prohibición de tratar categorías especiales de datos personales». De una primera lectura del preámbulo del reglamento, se puede razonar, por tanto, que la legislación europea otorga cierta capacidad de creación normativa a los Estados miembros, la cual puede ser extendida en el ámbito laboral a la negociación colectiva –por cuanto así también lo reconoce el art. 9.2 b) al mencionar los convenios colectivos–[44,45].

En relación con esta capacidad, no resulta extraño, no obstante, encontrar que la misma es empleada de nuevo contraviniendo la normativa en materia de protección de datos[46]. En este sentido, el propio artículo 9.2 b) del RGPD establece dos requisitos concretos para observar: la aportación de garantías y la justificación de la necesidad del tratamiento (Garrigues Giménez, 2022).

7.1. El deber de recoger garantías adecuadas

El artículo 9.2 b) del RGPD recuerda que el convenio colectivo –o derecho de los Estados miembros– que autorice el tratamiento de datos biométricos debe establecer «garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado» (Sierra Hernáiz, 2021).

[44] Afirmativamente se pronuncia también la Autoridad Catalana de Protección de Datos en su Dictamen CNS 2/2022: https://apdcat.gencat.cat/web/.content/Resolucio/Resolucions_Cercador/Dictamens/2022/Documents/es_cns_2022_002.pdf

[45] Además, Rodríguez-Piñero Royo (2019) recuerda que la regulación sobre el empleo de tecnologías biométricas entraría dentro del ámbito material de los convenios colectivos de acuerdo con el artículo 85.1 del ET; por cuanto respondería al cumplimiento de la obligación legal de registro, tratándose esta de una materia de índole laboral.

[46] A este respecto, cabe señalar que la autorización al tratamiento de datos biométricos podrá estar incluida, en todo caso, en convenios colectivos estatutarios, regulados en el título III del ET (Mercader Uguina, 2023, p. 41).

Este deber de aportar garantías adecuadas se plasma, en primer lugar, en el considerando 52 del RGPD. En él se recoge una exigencia: los Estados miembros ostentan la facultad de configurar excepciones a la prohibición de tratar datos sensibles, siempre que «se den las garantías apropiadas, a fin de proteger datos personales y otros derechos fundamentales». El «deber» de asegurar la protección de los derechos de las personas interesadas a través de la introducción de garantías adicionales no es exclusivo del apartado b) del artículo 9.2 del RGPD, sino que se reitera a lo largo de dicho precepto. Así, se puede observar que en los apartados g), i) y j) se recoge una similar exigencia empleando, no obstante, una expresión distinta: «establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado».

En este contexto, es imprescindible traer a colación la Sentencia del TC 76/2019, de 22 de mayo, que, aun refiriéndose a otra tipología especial de datos personales –datos relativos a las opiniones políticas–[47], crea un importante precedente en cuanto a la configuración legal de las garantías exigidas a lo largo del artículo 9 del RGPD. El TC se centra en el apartado g) del artículo 9.2 del RGPD, no obstante, los razonamientos que aporta podrían ser aplicables al artículo 9.2 b) del RGPD, por cuanto ambos preceptos se refieren a la necesidad de aportar garantías adecuadas.

En primer lugar, el TC aclara que el «margen de maniobra» que se reconoce a los Estados miembros en el considerando 10 no solamente se extiende a la configuración de la causa habilitante que excepciona la prohibición de tratamiento de datos especialmente sensibles, sino que igualmente se refiere al establecimiento de las garantías adecuadas (FJ 4). Se razona que estas son mencionadas en el reglamento como una «obligación concreta de los Estados miembros»; es decir, como un condicionante a la habilitación normativa (FJ 4), que puede entenderse cumplido cuando la norma interna prevé las garantías adecuadas de manera expresa y no cuando «se remite implícitamente a las garantías generales contenidas en el Reglamento general de protección de datos» (FJ 8).

A mayor abundamiento, el TC especifica que la exigencia de incluir dichas garantías no viene únicamente impuesta por la normativa europea, sino, asimismo, por su jurisprudencia. Una norma potencialmente intrusiva de derechos fundamentales –en este caso del derecho a la protección de datos del art. 18.4 CE– debe incluir «garantías adecuadas de tipo técnico, organizativo y procedimental, que prevengan los riesgos de distinta probabilidad

[47] La Sentencia 76/2019 declaró inconstitucional el artículo 58.1 bis de la Ley orgánica del régimen electoral general por considerar que vulneraba los artículos 18.4 y 53.1 de la CE. La norma que se pretendía incluir abría la puerta a que los partidos políticos pudiesen emplear datos relativos a las opiniones políticas de las personas, bajo el pretexto de la existencia de un «interés público» (reflejado en el considerando 56 y en el art. 9.2 g) RGPD). No obstante, el precepto no preveía las garantías adicionales que el artículo 9.2 g) y la jurisprudencia constitucional anterior exigían al respecto (previsibilidad y certeza de las medidas restrictivas, y cumplimiento del principio de proporcionalidad).

y gravedad y mitiguen sus efectos, pues solo así se puede procurar el respeto del contenido esencial del propio derecho fundamental» (FJ 6). Además, dichas garantías han de estar previstas en la propia ley o convenio colectivo, por cuanto no pueden «deferirse a un momento posterior a la regulación legal del tratamiento de datos personales de que se trate» (FJ 8). La inclusión en el convenio colectivo de garantías adecuadas para la salvaguarda del derecho fundamental a la protección de datos se configura, así, como una exigencia constitucional y legal.

En adición, el TC recalca que las garantías deben adaptarse al tipo de tratamiento, la naturaleza de los datos y «la probabilidad y gravedad de los riesgos de abuso»; siendo su finalidad ulterior proteger el contenido esencial del derecho fundamental (FJ 6). En este punto, es importante recordar que el contenido esencial del derecho a la protección de datos se desgrana en el poder de disposición sobre los datos personales, y, en concreto, en: el derecho de la persona interesada a consentir sobre la recogida de sus datos personales y el derecho a ser informada de la persona responsable y finalidad del tratamiento (FJ 7 Sentencia TC 292/2000). No obstante, como indica el TC, las garantías deben adecuarse al tipo de tratamiento, y considerando la naturaleza de las relaciones laborales[48], deviene insuficiente, en mi opinión, asegurar exclusivamente el contenido esencial del derecho fundamental. Por una parte, el consentimiento rara vez es libre en el ámbito laboral (Cruz Villalón, 2020) y, por otra parte, el deber de información individual –así como los principios de tratamiento: minimización, licitud, etc.– viene exigido por la normativa europea. Cabría, por tanto, centrarse en garantías de carácter técnico y de reconocimiento del ejercicio de derechos colectivos –como la exigencia de un consentimiento colectivo–[49].

7.2. La observancia del criterio de necesidad

En segundo lugar, el artículo 9.2 b) del RGPD reconoce que se alzará la prohibición cuando el tratamiento sea «necesario para el cumplimiento de obligaciones [...]».

[48] En este sentido, cabe señalar que la digitalización aumenta aún más el desequilibrio de poderes entre el empresario y el trabajador, por cuanto otorga más herramientas de poder a la empresa (Pérez del Prado, 2023, pp. 116-117).

[49] A este respecto, se debe resaltar que la adecuación del RGPD al ámbito laboral es cuestionable. Todolí Signes (2024, p. 231) apunta que:

> El RGPD (y el Reglamento de Inteligencia artificial) no es una normativa laboral y no está pensada ni adaptada a los principios de funcionamiento de las relaciones industriales. Así, la regulación en materia de protección de datos funciona en una lógica de garantías decididas unilateralmente por el responsable del tratamiento; de relevancia determinante del consentimiento; de derechos de ejercicio individual, etc. Reglas de funcionamiento muy alejadas de los principios básicos del ordenamiento laboral, cimentado en limitaciones a la autonomía de la voluntad; reconocimiento de la autonomía colectiva; intervenciones legislativas con garantías de derechos claras; normas de derecho mínimo necesario, etc.

A este respecto, se ha pronunciado recientemente el TJUE en su Sentencia de 19 de diciembre de 2024 (asunto C-65/23), en respuesta a una cuestión prejudicial planteada por el *Bundesarbeitsgericht* (TS de lo Laboral alemán)[50]. El tribunal alemán se cuestionaba si un órgano judicial nacional podía entrar a revisar el «carácter necesario» que el convenio colectivo había determinado en virtud de los artículos 5, 6 y 9.

En respuesta a esta cuestión prejudicial, el Tribunal de Justicia argumentó que cabe entender que los órganos jurisdiccionales nacionales tienen la facultad de controlar lo dispuesto en el convenio colectivo y de valorar si efectivamente «las justificaciones alegadas por las partes en dicho convenio acreditan el carácter necesario del tratamiento de datos personales que se deriva de él» (FJ 58).

Este razonamiento, en mi opinión, matiza una cuestión relevante: el momento de justificación de la «necesidad», mencionada tanto en el artículo 6.1 b) como en el artículo 9.2 b) del RGPD. El deber de justificación no solamente vendría impuesto a las empresas a la hora de efectuar la EIPD, sino que se exigiría igualmente a los agentes sociales en el momento de la negociación. Por tanto, se entiende que aquellas disposiciones de convenios colectivos que carezcan de una explicación razonable de la necesidad del tratamiento de datos biométricos podrán ser objeto de examen por los órganos jurisdiccionales; lo que podría tener como consecuencia que los tribunales declarasen que el articulado pactado es ineficaz.

En este sentido, un ejemplo –si bien controvertido[51]– en el que se refleja la facultad de juicio sobre las disposiciones de los convenios colectivos, ejercida por los tribunales del orden jurisdiccional laboral, es el supuesto enjuiciado en la Sentencia del TSJ de Aragón 379/2016, de 27 de mayo[52]. Se trata de una resolución que parte de los siguientes hechos.

El demandante y posterior recurrente, que trabajaba como asesor comercial para una empresa de atención telefónica a la clientela, fue despedido por proceder reiteradamente

[50] El *Bundesarbeitsgericht* planteó una segunda cuestión prejudicial: si el artículo 88 del RGPD exigía el cumplimiento de las obligaciones derivadas de los artículos 5, 6, apartado 1 y 9, apartados 1 y 2. Ante este planteamiento, el Tribunal de Justicia respondió afirmativamente, entendiendo que las normas adoptadas en virtud de dicho artículo no pueden «tener por objeto o como efecto eludir las obligaciones del responsable o del encargado del tratamiento que resultan de otras disposiciones de dicho Reglamento» (FJ 42).

[51] Véase el comentario realizado por Todolí Signes (2021b).

[52] Frente a esta sentencia se presentó recurso de casación para la unificación de doctrina, que fue inadmitido mediante Auto de la Sala de lo Social del TS de 18 de mayo de 2017. Y, posteriormente, frente al Auto del TS fue presentado recurso de amparo ante el TC, quien resolvió, en la Sentencia 160/2021, de 4 de octubre, que no había habido vulneración del derecho a la protección de datos y que la determinación de la cuestión correspondía a los órganos judiciales (FJ 4). Consideró, por tanto, que se trataba de una cuestión de legalidad ordinaria. Para profundizar en las implicaciones jurídicas de esta Sentencia del TC, es interesante acudir al análisis crítico que efectúa Molina Navarrete (2021).

de manera incorrecta en el ejercicio de sus funciones. Como medio de prueba de los incumplimientos, la empresa aportó grabaciones de las conversaciones telefónicas que había mantenido el trabajador con las personas usuarias; grabaciones de las que si bien el trabajador tenía constancia de que eran efectuadas, fueron empleadas contraviniendo un compromiso alcanzado con la representación de las personas trabajadoras. Así, previo despido, la empresa y la representación de las personas trabajadoras habían firmado un documento de desarrollo de compromisos en el que la dirección asumió el compromiso de que la monitorización de las llamadas no tendría en ningún caso como objetivo su utilización como mecanismo disciplinario. Atendiendo a dicho acuerdo, el trabajador alegó vulneración del artículo 18.4 de la CE y solicitó la nulidad del despido.

El supuesto es interesante porque, tanto en instancia como en suplicación, se declaró que no había lesión del derecho fundamental –ni nulidad de la prueba–, aunque se hubiera contravenido el pacto colectivo. El TSJ argumentó que de cumplirse lo acordado, se estaría permitiendo «la inmunidad de los asesores frente al control empresarial de la actividad laboral que desempeñan» (FJ 4). De esta forma, el tribunal realizó un examen del acuerdo colectivo adoptado, declarándolo, en cierta manera, ineficaz, bajo el pretexto de que el poder disciplinario es irrenunciable (Todolí Signes, 2021b).

De todo lo expuesto se deduce que, si se recoge, vía convenio colectivo, el tratamiento de datos biométricos para el registro horario, deberán ser tenidas en cuenta las especificidades técnicas del artículo 9.2 b) del RGPD: previsión de garantías adecuadas y determinación del carácter necesario del tratamiento.

Dicho esto, si bien la normativa europea pretende ser garantista aun cuando se trata de excepcionar la prohibición que versa sobre el tratamiento de datos biométricos, es común hallar convenios colectivos cuya articulación no se adecúa a las exigencias plasmadas.

7.3. La inobservancia de la normativa en los convenios colectivos

En ocasiones, la negociación colectiva se limita a la reiteración de las provisiones ya previstas en las normas de protección de datos, absteniéndose de regular garantías adicionales. Así, por ejemplo, el Convenio colectivo de la industria del calzado (Resolución de 24 de marzo de 2023[53]) y el Convenio colectivo estatal para las industrias de curtido, correas y cueros industriales y curtición de pieles para peletería (Resolución de 9 de marzo de 2023[54]) prevén en sus artículos 73 y 85, respectivamente, que: «El tratamiento de datos biométricos

[53] Publicado en el Boletín Oficial del Estado (BOE) el 10 de abril de 2023.

[54] Publicado en el BOE el 22 de marzo de 2023.

dirigidos a identificar de manera unívoca a una persona requerirá el consentimiento de esta, salvo que ese tratamiento sea necesario para cumplir con la obligación del control diario de jornada». Estas provisiones aplican la excepción del artículo 9.2 b) del RGPD y la concretan en la obligación de registro horario del artículo 34.9 del ET. Sin embargo, su redacción obvia la justificación del «carácter necesario» y la configuración de garantías para la protección de los derechos fundamentales de las personas trabajadoras afectadas.

En esta línea, el III Convenio colectivo de residencias para personas con problemas de salud mental, cuya titularidad y gestión se lleven a cabo de forma privada (Resolución de 2 de febrero de 2024[55]), contempla, que:

> Las empresas podrán establecer un sistema de control de asistencia sin que el tiempo reflejado en el registro de asistencia signifique, por sí solo, horas efectivas de trabajo. A tales efectos, se permite el uso de sistemas de control de asistencia que impliquen el tratamiento de datos biométricos siempre que se garantice su seudonimización (art. 12).

Se trata de un supuesto en el que se observa igualmente una carencia en el razonamiento de la necesidad de la medida. Además, si bien se aporta una garantía adicional –la seudonimización– esta puede devenir insuficiente, por cuanto el sistema de registro en sí mismo exige que se pueda identificar al sujeto, de lo contrario pierde su utilidad. Podría ser una garantía más adecuada para este fin la exigencia de emplear tecnologías que no almacenen los datos biométricos directamente (Garrigues Giménez, 2022).

De la lectura de algunos convenios colectivos, se puede observar que el empleo de estos para alzar la prohibición de tratamiento inobservando el RGPD provoca que la negociación colectiva se distancie de su «tradicional» propósito: tener como principal objeto mejorar lo establecido en la normativa y no agravar la intromisión a los derechos fundamentales de las personas trabajadoras (Muñoz Ruiz, 2022, p. 398). Esta problemática refleja, en cierta manera, la carencia de conocimiento de los órganos de representación de las personas trabajadoras de los retos digitales que se plantean y la normativa en materia de protección de datos (Rodríguez-Piñero Royo, 2019, p. 102). Y viene provocada, asimismo, desde mi punto de vista, por la ausencia de directrices en la normativa laboral[56].

[55] Publicado en el Diari Oficial de la Generalitat Valenciana el 5 de marzo de 2024.

[56] La ley, en un contexto en el que la negociación colectiva permite un mayor grado de adecuación a las circunstancias concretas de la actividad empresarial, tiene «la responsabilidad de garantizar unos resultados mínimos, así como de estructurar las posibilidades de actuación de los sujetos, reequilibrando las relaciones de poder y facilitando la autorregulación» (Álvarez del Cuvillo, 2023, p. 389).

8. Conclusiones

Las empresas que instalan sistemas de control horario que implican el tratamiento de datos biométricos deben observar asimismo la normativa en materia de protección de datos. En este sentido, la AEPD sostiene que, atendiendo a lo dispuesto en el RGPD, la obligación legal de registro del artículo 34.9 del ET no es lo suficientemente expresa para levantar la prohibición de tratamiento que recae sobre esta categoría especial de datos personales. No obstante, esta interpretación se contrapone, en cierta manera, con la jurisprudencia y doctrina judicial dictada al respecto; que, a falta de un pronunciamiento a la luz de la vigente normativa, valida el empleo de sistemas de biometría con fines de registro horario. Así, la disparidad de criterios y la inseguridad jurídica que los acompaña se debe, en parte, a la ausencia de concreción en la normativa laboral, cuya redacción encarga la elección del sistema de registro a la negociación colectiva y/o a la decisión empresarial.

En este contexto, el proyecto de ley, careciendo de cualquier pronunciamiento sobre la materia, mantendrá posiblemente la incertidumbre jurídica. El articulado propuesto, siguiendo el criterio de la AEPD, no es lo suficientemente expreso para entender levantada la prohibición de tratamiento del artículo 9.2 b) del RGPD. No obstante, las concreciones que incorpora –deber de emplear sistemas digitales y de garantizar la identificación inequívoca de la persona trabajadora– podrían reforzar la idea jurisprudencial de que las tecnologías biométricas de registro son necesarias.

Además, la reforma planteada delega de nuevo en la negociación colectiva la tarea de concretar la forma del registro y, por tanto, de tutelar la privacidad de las personas trabajadoras. Sin embargo, la «naturaleza» garantista de la negociación colectiva puede verse afectada cuando la norma configura la remisión, absteniéndose de proveer una regulación subsidiaria aplicable en ausencia del ejercicio de la autonomía colectiva[57].

Consecuentemente, en mi opinión, debería plantearse la opción de incluir en la normativa laboral una prohibición definitiva del tratamiento de datos biométricos con fines de registro horario, o, alternativamente, una posible habilitación de su tratamiento vía negociación colectiva, reservada, no obstante, al cumplimiento del carácter necesario recogido en el RGPD. Si bien esta segunda opción permitiría emplear los sistemas de biometría cuando las circunstancias de la actividad lo requiriesen, cabría plantearse igualmente si solucionaría el conflicto. En qué medida existe un supuesto en el que la instalación de un sistema de reconocimiento facial o de huella dactilar no pueda ser sustituido por otro que reporte una menor injerencia en los derechos fundamentales de las personas trabajadoras. Es por ello

[57] Como señala Todolí Signes (2020, p. 1502), esta circunstancia ocurre también en la normativa sobre el teletrabajo. Al no regular un plan B, se «corre el peligro de que en defecto de convenio colectivo lo que se imponga sea la voluntad individual empresarial».

por lo que, desde mi punto de vista, la forma más garantista sería impedir el tratamiento de datos biométricos para el control horario de forma expresa en la normativa laboral, y, en su ausencia, a través de la negociación colectiva.

Referencias bibliográficas

AEPD. (2023). *Guía sobre tratamientos de control de presencia mediante sistemas biométricos*. https://www.aepd.es/guias/guia-control-presencia-biometrico.pdf

Alfonso Mellado, C. L. (2019). Problemas aplicativos concretos en el cumplimiento de la obligación de registro de jornada. En C. L. Alfonso Mellado y G. E. Rodríguez Pastor, *El registro de jornada* (pp. 57-108). Tirant lo Blanch.

Álvarez del Cuvillo, A. (2023). El papel de la negociación colectiva en la regulación del uso de los dispositivos digitales puestos a disposición de los trabajadores. En J. R. Mercader Uguina y A. de la Puebla Pinila (Dirs.), *Cambio tecnológico y transformación de las fuentes laborales: Ley y convenio colectivo ante la disrupción digital* (pp. 383-408). Tirant lo Blanch.

Castillo Vázquez, I. del. (2021). Requisitos del consentimiento utilizado como fundamento jurídico para el tratamiento de los datos de carácter personal (comentario al artículo 7 RGPD y al artículo 6 LOPDGSS). En A. Troncoso Reigada (Dir.), *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales* (pp. 945-956). Thomson Reuters-Aranzadi.

Cristóbal Roncero, R. (2020). Nuevas tecnologías y tiempo de trabajo. En E. Monreal Bringsvaerd, J. Thibault Aranda y A. Jurado Segovia (Coords.), *Derecho del trabajo y nuevas tecnologías: estudios en homenaje al profesor Francisco Pérez de los Cobos Orihuel (en su 25.º Aniversario como Catedrático de Derecho del Trabajo)* (pp. 595-614). Tirant lo Blanch.

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.

EDPB. (2020). *Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679*. https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_es.pdf

EDPB. (2023). *Directrices 5/2022 sobre el uso de la tecnología de reconocimiento facial en el ámbito de la aplicación de la ley.* https://www.edpb.europa.eu/system/files/2024-05/edpb_guidelines_202304_frtlawenforcement_v2_es.pdf

Escajedo San Epifanio, L. (2015). *Reconocimiento e Identificación de las personas mediante Biometrías estáticas y dinámicas*. [Tesis doctoral, Universidad de Alicante]. http://hdl.handle.net/10045/53043

Escajedo San Epifanio, L. (2017). *Tecnologías biométricas, identidad y derechos fundamentales.* Aranzadi.

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.

García Coca, O. (2020). El registro de la jornada laboral y la privacidad de los trabajadores. En M. Rodríguez-Piñero Royo y A. Todolí Signes (Coords.), *Vigilancia y control en el Derecho del Trabajo Digital* (pp. 327-352). Thomson Reuters Aranzadi.

Garriga Domínguez, A. (2023). La especial posición de los datos biométricos en el RGPD: peculiaridades derivadas de su naturaleza y riesgos asociados a su tratamiento. En J. A. Viguri Cordero (Coord.), *La implementación del Reglamento general de protección de datos en España y el impacto de sus cláusulas abiertas* (pp. 115-144). Tirant lo Blanch.

Garrigues Giménez, A. (2022). La respuesta negocial al uso de algoritmos en la relación de trabajo: bases, previsiones, presencias y ausencias. En P. Rivas Vallejo, P. (Dir.ª), *Discriminación algorítmica en el ámbito laboral: perspectiva de género e intervención* (pp. 635-668). Thomson Reuters Aranzadi.

Gómez-Millán Herencia, M. J. (2020). Registro de jornada y control horario. En S. González Ortega (Coord.), *El nuevo escenario en materia de tiempo de trabajo, XXXVIII Jornadas Universitarias Andaluzas de Derecho del Trabajo y Relaciones Laborales* (pp. 215-260). Junta de Andalucía, Consejo Andaluz de Relaciones Laborales.

Gómez Sánchez, Y. (2021). Categorías especiales de datos personales: los datos de origen étnico o racial, los datos genéticos, los datos biométricos, los datos relativos a la salud, los datos relativos a la vida sexual y la orientación sexual (comentario al artículo 9.1 RGPD). En A. Troncoso Reigada (Dir.), *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales* (pp. 1041-1065). Thomson Reuters-Aranzadi.

González Moreno, M. (2019). RGPD: uso de huella dactilar biométrica en el ámbito laboral. *Actualidad Jurídica Aranzadi*, *951*, 7.

Mercader Uguina, J. R. (2023). Disrupción digital y sistema de fuentes: una visión general. En J. R. Mercader Uguina, y A. de la Puebla Pinilla (Dirs.), *Cambio tecnológico y transformación de las fuentes laborales: ley y convenio colectivo ante la disrupción digital* (pp. 23-44). Tirant lo Blanch.

Miralles López, R. (2021). La evaluación de impacto relativa a la protección de datos (comentario al artículo 35 RGPD). En A. Troncoso Reigada (Dir.), *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales* (pp. 2137-2162). Thomson Reuters-Aranzadi.

Molina Navarrete, C. (2021). Eficacia de gestión versus protección de datos: ¿reactividad jurisdiccional a la «inflación de derechos humanos» (en el trabajo)? Comentario a la Sentencia del Tribunal Constitucional 160/2021, de 4 de octubre. *Revista de Trabajo y Seguridad Social*. *CEF*, *465*, 109-122. https://doi.org/10.51302/rtss.2021.2564

Montesdeoca Suárez, A. (2022). La imprescindible compatibilidad entre los sistemas de registro horario laboral y el derecho a la protección de datos del trabajador. *Iuslabor*, *1*, 168-212. https://doi.org/10.31009/IUSLabor.2022.i01.07

Muñoz Ruiz, A. B. (2022). La integración del pacto colectivo en el contenido del derecho fundamental de protección de datos de carácter personal: comentario a la STC 160/2021, de 4 de octubre. En *Liber amicorum en homenaje a Aurelio Desdentado Bonete* (pp. 393-412). Tirant lo Blanch.

Muñoz Ruiz, A. B. (2023). *Biometría y sistemas automatizados de reconocimiento de emociones: implicaciones jurídico-laborales*. Tirant lo Blanch.

Pérez del Prado, D. (2023). Los tradicionales conceptos de trabajador y empresario en un mundo digital. En J. R. Mercader Uguina y A. de la Puebla Pinilla (Dirs.), *Cambio tecnológico y transformación de las fuentes laborales: ley y convenio colectivo ante la disrupción digital* (pp. 91-123). Tirant lo Blanch.

Poquet Catalá, R. (2020). *El teletrabajo: análisis del nuevo marco jurídico*. Thomson Reuters Aranzadi.

Rebollo Delgado, L. (2021). Las condiciones de tratamiento de categorías especiales de datos (comentario al artículo 9 RGPD y artículo 9 LOPDGDD). En A. Troncoso Reigada (Dir.). *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales* (pp. 1013-1039). Thomson Reuters-Aranzadi.

Rodríguez Martín-Retortillo, R. M. (2022). El registro obligatorio de la jornada diaria de trabajo: impacto, efectos y estado de la cuestión tras tres años de vigencia. *Revista española de derecho del trabajo*, *257*, 61-92.

Rodríguez Pastor, G. E. (2019). El registro diario de jornada: la normativa y su interpretación. En C. L. Alfonso Mellado y G. E. Rodríguez Pastor, *El registro de jornada* (pp. 11-56). Tirant lo Blanch.

Rodríguez-Piñero Royo, M. (2019). El registro diario de jornada: la normativa y su interpretación. *Temas Laborales: Revista andaluza de trabajo y bienestar social*, *150*, 91-109.

Rodríguez-Piñero Royo, M. (2020). Registro de jornada mediante controles biométricos: un caso de incoherencia en el Derecho del Trabajo Digital. En M. Rodríguez-Piñero Royo y A. Todolí Signes (Coords.), *Vigilancia y control en el Derecho del Trabajo Digital* (pp. 273-300). Thomson Reuters Aranzadi.

Selma Penalva, A. (2010). El control de accesos por medio de huella dactilar y sus repercusiones prácticas sobre el derecho a la intimidad. *Aranzadi Social: Revista Doctrinal*, *3*(3), 27-36.

SEPD. (2019). *Directrices del SEPD para la evaluación de la proporcionalidad de las medidas que limitan los derechos fundamentales a la intimidad y a la protección de los datos personales*. https://www.edps.europa.eu/system/files/2021-12/19_12_19_edps_proportionality_guidelines_es.pdf

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.

Todolí Signes, A. (2020). La regulación del trabajo a distancia. *Derecho de las relaciones laborales*, *11*, 1493-1504.

Todolí Signes, A. (2021a). Derecho a la intimidad y a la desconexión digital en el teletrabajo. En M. Rodríguez-Piñero Royo y A. Todolí Signes (Coords.), *Trabajo a distancia y teletrabajo: análisis del marco normativo vigente* (pp. 229-245). Thomson Reuters Aranzadi.

Todolí Signes, A. (11 de noviembre de 2021 –2021b–). Los Tribunales niegan la eficacia de la negociación colectiva en materia de Protección de Datos. Comentario a la STC de 160/2021, de 4 de octubre. *Argumentos en Derecho Laboral*. https://adriantodoli.com/2021/11/11/los-tribunales-niegan-la-eficacia-de-la-negociacion-colectiva-en-materia-de-proteccion-de-datos-comentario-a-la-stc-de-160-2021-de-4-de-octubre/

Todolí Signes, A. (2022). Control tecnológico: una propuesta de aplicación del triple juicio de proporcionalidad conforme a la normativa europea de protección de datos. En *Digitalización, recuperación y reformas laborales. XXXII Congreso Anual de la Asociación Española de Derecho del Trabajo y de la Seguridad Social. Ponencias*. Alicante, 26 y 27 de mayo de 2022 (pp. 223-252). Ministerio de Trabajo y Economía Social. Subdirección General de Informes, Recursos y Publicaciones.

Todolí Signes, A. (2024). Democracia en el trabajo y codeterminación ante el uso de la IA en la empresa: algo más que negociar el algoritmo. *Revista Crítica de Relaciones de Trabajo, Laborum*. *N.º Extra 2*, 229-250.

Troncoso Reigada, A. (2021). Los principios relativos al tratamiento (comentario al artículo 5 RGPD y al artículo 4 LOPDGDD). En A. Troncoso Reigad (Dir.), *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales* (pp. 847-907). Thomson Reuters-Aranzadi.

Alba Navalón Arnal. Personal investigador no doctor del Departamento de Derecho del Trabajo y de la Seguridad Social de la Universitat de València. https://orcid.org/0009-0004-6582-5326