ISSN-e: 2792-8322

Tratamiento y control de datos biométricos de las personas trabajadoras: posibilidades y límites

Susana Rodríguez Escanciano
Catedrática de Derecho del Trabajo y de la Seguridad Social.
Universidad de León (España)
Subdirectora de la Revista de Trabajo y Seguridad Social. CEF
srode@unileon.es | http://orcid.org/0000-0001-5910-2982

1. Teniendo en cuenta que los algoritmos permiten todo tipo de información, sin límite de capacidad y sin sufrir demoras, resulta indiscutible el importante papel que atesoran desde el punto de vista empresarial, pues facilitan extraer conocimientos privilegiados sobre mercados, clientes, *marketing*, ventas, desarrollo de productos, operaciones de servicios, soporte administrativo, oscilaciones de la demanda, requerimientos de consumo, modelado de riesgos o, por lo que aquí interesa, dirección de personal.

Cada vez son más las corporaciones que incorporan inteligencia artificial (IA) como soporte de las decisiones estratégicas en la integridad de las facetas que componen la autonomía organizativa empresarial con proyección en todos los momentos y aspectos de la relación laboral, desde el reclutamiento de las personas trabajadoras, pasando por la vigilancia de las actividades laborales a través de evaluaciones cuantitativas y cualitativas, hasta la extinción del vínculo, sin olvidar aquellos aspectos de gestión ordinaria como, en una lista no exhaustiva, determinación de la jornada, horario, vacaciones, descansos, tareas a realizar, retribuciones, ascensos, modificaciones sustanciales, seguridad y salud, despidos, etc.

A día de hoy, la IA, extramuros del ámbito de la especialización técnica, pivota sobre los tres parámetros siguientes: datos, algoritmos y capacidad matemática para aplicar estos a aquellos. Precisamente, los datos se convierten en la «materia prima capital» o el «nutriente fundamental» de las herramientas inteligentes. Como no podía ser de otra manera, el uso de algoritmos en los centros de trabajo implica el procesamiento por parte de las empresas de datos masivos de las personas trabajadoras hasta el punto de que su extensión ha postergado en el lenguaje el uso de los prefijos habituales del sistema internacional de medidas, ya que tales magnitudes se mueven con soltura en la escala de los cuatrillones (megas, gigas, petas, zetas, yotas), algo difícil de digerir con los cálculos mentales más rudimentarios.

Tal acopio de información no resulta en exceso complicado atendiendo a la singularidad del contrato de trabajo, marcada por varios factores esenciales: la implicación física y mental de la persona, que es inseparable de la actividad encomendada (razón esencial,

intuitu personae, por la que la persona asalariada no es una mera mercancía); la naturaleza vital del vínculo (en el sentido de que la remuneración del trabajo constituye el medio fundamental de vida); la debilidad reivindicativa y negociadora de la parte trabajadora; o la duración normalmente dilatada de la relación laboral, sujeta a múltiples vicisitudes y contingencias; todo ello coronado por la atribución legal a la parte empresarial de un poder muy dominante en la dinámica contractual, cuyo ejercicio cuenta precisamente con el auxilio de las nuevas tecnologías inteligentes.

La gestión digitalizada del personal facilita, además, que todos los extremos concernientes al desarrollo del contrato de trabajo, desde el momento de la selección de personal, pasando por la constitución del nexo contractual hasta su resolución, sean incluidos en los soportes técnicos de la empresa, provocando, en significativa denominación, una «hiperdatificación» de las relaciones laborales, con flujos constantes en la emisión y recepción de noticias, las cuales (de forma simple, descontextualizadas o combinadas entre sí, a través del uso de ficheros y fórmulas matemáticas) pueden contribuir a definir el devenir completo de las personas trabajadoras o candidatas a una ocupación.

En efecto, la generalización de sofisticados utillajes técnicos inteligentes en el universo de las organizaciones productivas acarrea una atribución de enormes potencialidades estratégicas en materia de gestión de personal al quedar exponencialmente ampliada la capacidad de obtención, acumulación, retención, elaboración y transmisión de información, permitiendo a la empresa un conocimiento exhaustivo del perfil de las personas empleadas actuales o futuras, en el que se incluyen (cual «teselas de un mosaico») desde aspectos estrictamente profesionales a características individuales pertenecientes al ámbito de su privacidad, consecuencia del mero desarrollo de actividades ordinarias dentro de la empresa y, cómo no, de la multiplicación de las posibilidades conferidas para supervisar la ejecución de la prestación laboral concertada por las personas asalariadas mediante el ejercicio de un poder dotado de mayor intensidad y amplitud respecto de sus modalidades precedentes. Son infinitas las posibilidades de control que proporcionan los instrumentos digitales asistidos por IA (videovigilancia, micrófonos, geolocalización, seguimiento de correos electrónicos, tarjetas electrónicas, contadores de pasos, lectores digitales, interacción del ratón, *cookies*…) que permiten obtener informaciones exhaustivas sobre el rendimiento, la cantidad y calidad de las tareas realizadas, el tiempo empleado, las interrupciones habidas, los patrones de comportamiento y, también, la personalidad de las personas trabajadoras (ejercicio, alimentación, forma física, socialización con compañeros/as…).

Al tiempo, tanta es la información digital que hoy en día se puede obtener (huella digital), de forma rápida y libre a través de las redes sociales, que con mucha frecuencia las empresas recurren a programas informáticos inteligentes para realizar, a través de patrones predeterminados, filtrados y rastreos («*recruiting* 2.0») con el fin de descubrir, entre otros posibles aspectos, la orientación sexual, la situación sentimental, las cargas familiares, la convicción política, las creencias religiosas, los hábitos, el historial de salud, las preferencias para el tiempo de ocio o la tendencia al consumo de sustancias de las personas

trabajadoras. A través de las redes sociales también se pueden descubrir comentarios en contra de la buena imagen de la empresa, su credibilidad, clientela o secretos industriales, fácilmente perceptibles y, por ende, punibles, al igual que se pueden detectar transgresiones de la buena fe contractual en supuestos de incapacidad temporal donde la persona trabajadora lleva a cabo tareas incompatibles con su estado de enfermedad o perjudiciales para su recuperación.

Además, la posibilidad de evaluación por la clientela tiene un objetivo doble en cuanto a la reputación de la persona empleada: por un lado, incrementar la satisfacción de las consumidoras y los consumidores y permitirles establecer sus preferencias hacia el futuro; por otra, obtener información sobre la conducta de la persona trabajadora con un coste ínfimo y utilizar dichos hallazgos para tomar decisiones, máxime cuando algunas empresas deciden publicar esas evaluaciones en la intranet. Ello implica, de un lado, la posibilidad de que la persona consumidora conozca la satisfacción que ha obtenido la anterior clientela con esa persona empleada en concreto; de otro, la persona trabajadora va a ser consciente de que un desempeño insatisfactorio para la clientela no solo será utilizado por la empresa, sino que será conocido por el resto de personas usuarias y potenciales empleadoras en el futuro.

Así pues, la persona trabajadora se ha convertido en un terminal de corrientes de datos, máxime cuando la mayor capacidad de transmisión y de combinación de los mismos de la mano de los algoritmos provoca una total trazabilidad susceptible *a posteriori* de ser valorada, favorable o desfavorablemente, a efectos laborales.

2. El ordenamiento europeo y español de protección de datos, esto es, el Reglamento (UE) 2016/679 (RPD) y la Ley orgánica 3/2018, de 5 de diciembre (LOPDyGDD), distinguen dos niveles de protección en función del bien jurídico tutelado: de un lado, los datos personales que cabría calificar como «ordinarios»; de otro, los datos «sensibles», «especialmente protegidos», «superpersonales» o «pertenecientes a categorías especiales»; esto es, aquellos estrechamente vinculados a la dignidad y personalidad humana (origen étnico o racial, opiniones políticas, convicciones religiosas o filosóficas, afiliación sindical, datos genéticos, datos biométricos, datos relativos a la salud o datos relativos a la vida sexual o la orientación social de las personas), los cuales, aun cuando están ya garantizados por otros derechos fundamentales, reciben una protección cualificada, al establecer la prohibición de su tratamiento, que solo puede ser levantada en supuestos excepcionales variables en función de la naturaleza jurídica de la información en cuestión.

Dentro de este catálogo de datos «privilegiados» en cuanto a sus limitaciones de recopilación y tratamiento se encuentran los datos biométricos, que serán objeto de atención en las páginas siguientes. La identidad biológica es propia de cada sujeto y, por tanto, cualquier instrumento que la utilice permitirá, a quien de él se sirva, adentrarse en el terreno más recóndito que cada ser humano tiene hasta el punto de poder afirmar que, a su través, se puede entrar en la intimidad de la intimidad.

Precisamente, la métrica de las personas, la biometría, es uno de los terrenos en los que de forma más evidente se puede apreciar el desarrollo presente y futuro de los sistemas algorítmicos como instrumentos de control laboral con manifestaciones particularmente interesantes en el reclutamiento de personal, en el acceso a las distintas dependencias empresariales, en la valoración del rendimiento y en los apuntes de la jornada laboral (inicio, terminación e interrupciones, esto es, tiempo improductivo e improductivo), máxime cuando los datos biométricos presentan unas características comunes, a saber: son útiles a efectos de autenticación o identificación, son universales (todas las personas los poseen), son únicos (deben ser capaces de discernir a una persona de otra) y son permanentes (tienen una presencia continua en el tiempo).

Constituyen, asimismo, una solución idónea para garantizar la entrada de persona autorizada a los equipos técnicos y máquinas, a través de lectores o detectores como alternativa más segura que las claves personales, pues anillos, pulseras, gafas, cascos o tarjetas identificativas que incorporan huellas u otros hallazgos permiten a la persona empleada, tras conectarlas o acercarlas a un lector, acceder a ciertas salas, operar con el ordenador, poner en marcha utensilios de trabajo…, volcando con detalle el trazo de los movimientos realizados y su emplazamiento concreto en cada momento. Sin descartar tampoco su ayuda a la hora de prevenir riesgos laborales, permitiendo una adecuada planificación de la actividad preventiva a través de variados sistemas *wereables* que aportan información sobre las constantes vitales de una persona, cansancio, sueño y fatiga.

Como es fácil adivinar, la principal ventaja del tratamiento de datos biométricos radica en que no permiten la suplantación del sujeto sometido a seguimiento o vigilancia, a diferencia de los soportes de identificación tradicionales, que admitían la transferibilidad.

3. En un afán de simplificación, tales controles pueden ser de tres tipos:

a) Los que permiten, con muy pocos márgenes de error, el análisis de aspectos físicos, fisiológicos y morfológicos de la persona (biometría estática), a través de la verificación de las huellas dactilares, los patrones de la mano, el reconocimiento facial, las características de la retina, la geometría del iris, el olor corporal, los rasgos de la voz, las estructuras venosas, las pulsaciones, las ondas cerebrales, el ritmo cardiaco, la frecuencia respiratoria, el sudor o el ADN.

b) Los que facilitan la valoración de los comportamientos, actuaciones o forma de realizar ciertas conductas (biometría dinámica), mediante la comprobación de su escritura, su firma, la fuerza en la presión de las teclas del ordenador, las mediciones de respuesta a situaciones concretas, las destrezas al conducir, la manera de andar o de moverse y la rapidez de la marcha.

c) Los que posibilitan conocer los rasgos psicológicos (biometría psíquica), esto es, la manera de reaccionar frente a ciertas situaciones o pruebas, que pueden dar información sobre el estado de ánimo (seguro, deprimido, ansioso, conten-

to, aburrido, tímido, extravertido…), así como sobre el funcionamiento del cerebro distinguiendo por partes (creativo, atento…) o sobre los niveles de felicidad o tristeza, sin olvidar aquellos que habilitan para llevar a cabo predicciones sobre la personalidad futura e influencia interpersonal.

Además, los principales componentes del sistema biométrico son los tres siguientes: 1) el sensor, que captura los rasgos o características concretas; 2) el repositorio, que es la base de datos donde se almacenan las plantillas biométricas inscritas para su comparación; y 3) los algoritmos, utilizados para la extracción de características (procesamiento) y comparación.

4. Tales tipologías y entramados no dejan de presentar un carácter invasivo, pues habilitan para descubrir estados de ánimo, niveles de energía, rasgos de la personalidad, trastornos psicóticos, influencia interpersonal en el trabajo en equipo (liderazgo, sumisión…) o propensión a padecer enfermedades degenerativas o crónicas. Los *softwares* de evaluación de personas realizan test de personalidad, inteligencia o salud mental mediante el reconocimiento facial, pueden perjudicar a personas transgénero, a quienes están pasando por un momento personal adverso (fallecimiento de un familiar, divorcio…) o a determinadas culturas, pues los movimientos faciales generalmente asociados a las principales emociones (enfado, asco, miedo, felicidad, tristeza o sorpresa) varían en función de la personalidad individual, situaciones o convicciones.

Una muestra de tales peligros aplicada al marco de la seguridad fronteriza puede encontrarse en la Sentencia del Tribunal General de la Unión Europea de 7 de septiembre de 2023 (ECLI:EU:C:2023:640), referida a una petición de transparencia formulada por un representante político en relación con la tecnología de reconocimiento de emociones ensayada en el proyecto *iBorderCtrl*, financiado por la Unión Europea. En su desarrollo se pone en práctica tecnología de reconocimiento de emociones que utiliza IA para detectar mentiras en los controles fronterizos a través del reconocimiento facial (datos biométricos) con el propósito de agilizar la seguridad en las fronteras y el control de pasaportes. Para ello, el *software* es capaz de detectar numerosas microexpresiones (hasta 38) en el rostro en función de cada respuesta. Las personas que viajan, cuando superen el test, reciben un código QR que les permite pasar la frontera. En caso contrario aparecerá un agente físico de seguridad para realizar un control adicional. El tribunal distingue entre los documentos que contienen información relativa a las herramientas y tecnologías desarrolladas y a la evaluación ética y jurídica de los sistemas, llegando a la conclusión de que el deber de transparencia de las instituciones comunitarias se aplica solo sobre el segundo grupo de documentos, pero no respecto del primero.

Igualmente ilustrativa es la resolución de la Agencia de Protección de Datos húngara en la que se revisaba la práctica llevada a cabo por un banco durante 45 días consistente en utilizar un *software* de procesamiento de señales de voz basado en IA. El mencionado *soft-*

ware analizaba y evaluaba los estados emocionales de la clientela y las palabras clave utilizadas en las llamadas. La finalidad de esta tecnología era gestionar las quejas, controlar la calidad de las conexiones y del trabajo y, además, aumentar la eficiencia de las personas empleadas. A continuación, los resultados de este análisis se almacenaban junto con las grabaciones de las llamadas y estos datos se usaban para clasificar las conversaciones en orden de prioridad. La justificación del banco para el procesamiento de datos se basó en su interés legítimo de garantizar buenos niveles de retención de la clientela y eficiencia, pero la agencia concluyó que el banco no había considerado adecuadamente los intereses en juego, mereciendo la imposición de una cuantiosa multa y quedando obligado a suspender el uso del sistema de análisis de emociones descrito.

Recientemente, la Agencia de Protección de Datos Española (AEPD) ha bloqueado (y la Audiencia Nacional lo ha ratificado) el tratamiento de datos biométricos (iris) realizado por una empresa (Worldcoin) con afectación a numerosas personas, incluidas personas menores, sin constar acreditados ni el consentimiento ni la información pertinente de dicho tratamiento.

5. La regla general, a la luz del artículo 9 del RPD de aplicación directa en el sistema español, es la prohibición del tratamiento de datos biométricos, que solo puede enervarse por algunos motivos, como puede ser cuando sea

> […] necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho Laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión, el de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado [art. 9.2 b) RPD].

La doctrina judicial y la AEPD venían entendiendo que el segundo condicionante (autorización por norma legal) quedaba amparado por los artículos 34.9 (registro horario), 20.3 y 20 bis del Estatuto de los Trabajadores (ET) (ejercicio del poder de control empresarial) o por la Ley 31/1995, de 8 de noviembre, de prevención de riesgos laborales, sin necesidad de consentimiento de la persona trabajadora, siempre y cuando estuviera debidamente informada y no hubiera otra alternativa menos lesiva de la intimidad para los mismos fines de control, esto es, se tratase de un cauce imprescindible. En el mismo sentido se había manifestado el principio 18 de la Recomendación CM/ Rec. (2015) del Comité de Ministros del Consejo de Europa sobre el tratamiento de datos personales en el contexto laboral.

Entre los pronunciamientos judiciales españoles más llamativos de esta etapa se encuentran los referidos al citado control biométrico de la mano que permite identificar a la persona trabajadora mediante un reconocimiento tridimensional: largo, ancho y espesor. Cuestionada la licitud de semejante método utilizado en una Administración regional como

fichaje del horario del personal, el Tribunal Supremo consideró que resulta idóneo para conseguir el objetivo propuesto, cual es «lograr un mayor nivel de eficacia en la Administración pública (empleador, *in casu*) controlando el efectivo cumplimiento de sus obligaciones por parte de los empleados públicos». Reconoció el órgano judicial que la medida se entiende necesaria debido al «notorio carácter imperfecto de los sistemas de control más comúnmente usados», que no impiden «la sustituibilidad en su cumplimiento».

6. Ahora bien, recientemente, en noviembre de 2023, la AEPD, en línea con el criterio renovado del Comité Europeo de Protección de Datos Personales, ha publicado una *Guía sobre tratamientos de control de presencia mediante sistemas biométricos*, en la que termina por declarar que tales sistemas (incluida la huella dactilar o el reconocimiento facial, del iris, de la voz…) vulneran, en el actual marco normativo, la protección de datos personales de la persona trabajadora, pues suponen un tratamiento de alto riesgo, tanto si se utilizan para la identificación como para la autenticación, partiendo de la base de categoría especial de estos datos. Entiende la AEPD que tales mecanismos no se pueden admitir con carácter general, indiscriminado o masivo, para llevar a cabo un control horario o de presencia, atendiendo a las tres circunstancias siguientes:

1) La normativa española vigente no contiene autorización legal expresa para utilizar datos biométricos con la finalidad de controlar la presencia o la dedicación horaria. Los antes expuestos artículos 34.9 y 20.3 del ET no dan cobertura legal expresa a estas herramientas, como tampoco lo hace la LOPDyGDD.

2) El consentimiento de la persona trabajadora no puede levantar la prohibición de tratamiento de una categoría especial de datos personales, al haber un desequilibrio entre las partes del contrato de trabajo y no existir cobertura legal de uso de esta herramienta.

3) En el hipotético supuesto de existir cobertura legal de uso, el respeto al principio de minimización de las categorías especiales de datos, como los biométricos, hace muy difícil su aceptación, exigiendo un pertinente análisis de impacto, previamente al inicio del tratamiento, donde se valorará la idoneidad, necesidad y proporcionalidad. Asimismo, ha de cumplir determinadas garantías y obligaciones de transparencia y seguridad, ya que dependiendo de los datos recogidos se pueden derivar informaciones «sobre enfermedades, taras, características genéticas, consumos de sustancias…».

En suma, teniendo en cuenta el carácter intrusivo de los mecanismos utilizados y la naturaleza de los datos obtenidos, parece claro que el recurso a esta tecnología biométrica, cuando hipotéticamente estuviera habilitada por una disposición legal, debe ir acompañado no solo de la obligación de informar a las personas trabajadoras afectadas, de la conse-

cución de una finalidad legítima y del cumplimiento de los principios de proporcionalidad e intervención mínima, sino también de la realización de una evaluación de impacto por parte de quien sea responsable del tratamiento.

Como último hito en este excurso, cabe señalar que el Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial (REIA), define los datos biométricos como «los datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física, como imágenes faciales o datos dactiloscópicos» (art. 3.34) y la «verificación biométrica» como «la verificación automatizada y uno-a-uno, incluida la autenticación, de la identidad de las personas físicas mediante la comparación de sus datos biométricos con los datos biométricos facilitados previamente» (art. 3.36).

En la medida en que «los datos biométricos pueden permitir la autenticación, la identificación o la categorización de las personas físicas y el reconocimiento de las emociones de las personas físicas» (Considerando 14), esta norma europea veta ambas modalidades: la utilización de los sistemas de «categorización biométrica» o de «reconocimiento de emociones» (art. 5). Con mayor detalle, indica el Considerando (30) que:

> Deben prohibirse los sistemas de categorización biométrica basados en datos biométricos de las personas físicas, como la cara o las impresiones dactilares de una persona física, para deducir o inferir las opiniones políticas, la afiliación sindical, las convicciones religiosas o filosóficas, la raza, la vida sexual o la orientación sexual de una persona física.

Por su parte, el Considerando (18) entiende prohibidos los sistemas que permiten inferir «emociones o intenciones como la felicidad, la tristeza, la indignación, la sorpresa, el asco, el apuro, el entusiasmo, la vergüenza, el desprecio, la satisfacción y la diversión».

Se entienden prohibidos, por tanto, aquellos artilugios que permiten a la empresa realizar perfilados sobre la biometría de las personas trabajadoras capaces de provocar limitaciones, segregaciones o exclusiones atendiendo al índice cuantitativo de la productividad de la persona trabajadora o aquellos algoritmos psicogénicos que facilitan interpretar emociones (psicogenia), permitiendo anticipar conductas, predecir el estado anímico y emocional, detectar rasgos psicológicos o enfermedades o manipular la capacidad cerebral para conformar opiniones, convicciones o pensamientos.

Otra cosa sucede con la posible utilización de datos biométricos a los efectos de prevenir accidentes o enfermedades profesionales, pues el Considerando (18) del REIA considera excluidos de la prohibición de tratamiento «los estados físicos, como el dolor o el cansancio, como, por ejemplo, los sistemas utilizados para detectar el cansancio de los pilotos o

conductores profesionales». Estos usos permitidos, no obstante, deben ir acompañados de la observancia de todos los principios recogidos en el RPD (transparencia e información –individual y colectiva–, minimización, finalidad y evaluación de impacto), así como de todas las garantías que establece el REIA a observar por los fabricantes, proveedores o comercializadores (art. 16) y, por lo que aquí interesa, por el empresario usuario: 1) arbitrar medidas de vigilancia humana durante su tiempo de funcionamiento de acuerdo con la información que le haya facilitado el proveedor; 2) vigilar el funcionamiento del sistema e informar de posibles incidentes; 3) interrumpir si fuera necesario su funcionamiento e informar a las autoridades; 4) conservar los archivos de registro que se generan automáticamente y utilizar la información facilitada para cumplir la obligación de evaluación de impacto relativa a la protección de datos (art. 27).

Más discutible es la exclusión de la prohibición de aquellos sistemas destinados a

> la mera detección de expresiones, gestos o movimientos que resulten obvios… esas expresiones pueden ser expresiones faciales básicas, como un ceño fruncido o una sonrisa; gestos como el movimiento de las manos, los brazos o la cabeza, o características de la voz de una persona, como una voz alzada o un susurro (Considerando 18 REIA *in fine*),

pues abre la puerta a zonas de penumbra entre la licitud y el veto.

***

Sirvan estas líneas como pórtico de este nuevo número de la *Revista de Trabajo y Seguridad Social*. *CEF*, donde autorizadas voces disertan, en la sección de estudios, sobre temas de máxima actualidad e interés, como «La extinción del contrato por falta de pago o retrasos continuados en el abono del salario tras la aprobación de la Ley orgánica 1/2025, de 2 de enero», del Dr. Eduardo Enrique Taléns Visconti; «"Garantías multinivel" y "perspectiva de diversidad (género, discapacidad, infancia)" en el enjuiciamiento de los asuntos sociolaborales: avances y resistencias… y algún exceso», a cargo del Dr. Cristóbal Molina Navarrete; «Cobertura de déficits preventivos a través de la negociación colectiva: organización preventiva y representación especializada», cuya autora es la Dra. Josefa Romeral Hernández; «Las enfermedades profesionales en sectores feminizados: un sistema pendiente de reforma con perspectiva de género», del Dr. Matthieu Chabannes; y «La toxicidad de los nanomateriales en el contexto laboral: principio de precaución y control de exposición», de D.ª Rosa María Rodríguez Casáis.

De gran enjundia son, igualmente, los diálogos con la jurisprudencia, centrados en pronunciamientos de tanta trascendencia como los siguientes: «Absentismo y remuneración: los incentivos antiabsentismo en el punto de mira. Comentario a la Sentencia del Tribunal

Supremo 40/2025, de 20 de enero», a cargo de D.ª Ana Matorras Díaz-Caneja; «Trabajo a distancia: ¿ha cambiado algo después de la Ley 10/2021 para algunas empresas? Comentario a la Sentencia de la Audiencia Nacional 62/2024, de 3 de junio», de D. Francisco Trillo Párraga; «Irrelevancia del origen de la pensión de incapacidad permanente –enfermedad común o accidente no laboral– en el acceso al derecho del complemento por mínimos. Comentario a la Sentencia del Tribunal Supremo 1007/2024, de 10 julio», de D. Francisco Javier Fernández Orrico, y «Cosas de casa que (algunos) "hombres-jueces" se empeñan en enseñar a las mujeres: *¿mansplaining* para conciliar corresponsablemente? A propósito de la Sentencia del Tribunal Superior de Justicia de Canarias/Las Palmas 359/2025, de 27 de febrero», a cargo de D. Cristóbal Molina Navarrete.

Para concluir, no menos sugerente es el Foro de debate, que incluye la reflexión «De la escuela al foro: ¿sigue vivo el legado del graduado social? La visión anticipada del derecho del trabajo de José Gascón y Marín», de D. José Blas Fernández Sánchez.

Cómo citar: Rodríguez Escanciano, S. (2025). Tratamiento y control de datos biométricos de las personas trabajadoras: posibilidades y límites. *Revista de Trabajo y Seguridad Social. CEF*, *486*, 7-16. https://doi.org/10.51302/rtss.2025.24487