

Implicaciones de los sistemas de inteligencia artificial en la relación laboral

Aida Fonseca Díaz (autora de contacto)

Doctora en Derecho y profesora en el Departamento de Ciencias Jurídicas de la Facultad de Ciencias Jurídicas, Educación y Humanidades.

Universidad Europea de Madrid (España)

aida.fonseca@universidadeuropea.es | <https://orcid.org/0000-0001-7858-311X>

Maria Petronela Popiuc

Doctora en Derecho acreditada ANECA y profesora en Derecho.

Universidad Camilo José Cela (España)

mpopiuc@ucjc.edu | <https://orcid.org/0000-0002-6599-0848>

Extracto

La creciente disponibilidad de datos masivos plantea desafíos inéditos en el ámbito jurídico, ya que su procesamiento mediante sistemas de inteligencia artificial impacta directamente en la protección de los derechos y en la configuración del Estado constitucional. Este artículo examina cómo la actual «fiebre del *Big Data*» puede afectar la tutela de los datos personales de los trabajadores y trabajadoras y en qué medida el marco legislativo vigente ofrece garantías suficientes. Partiendo del *Knowledge Discovery in Data Bases* y de las cinco dimensiones del *Big Data*, se analiza cómo la acumulación masiva de información exige un marco regulador capaz de garantizar la transparencia, la rendición de cuentas y el respeto a los derechos fundamentales. A través de una revisión crítica de la normativa laboral y del Reglamento de inteligencia artificial, se abordan los riesgos asociados a la gestión algorítmica de las relaciones laborales y se reflexiona sobre la necesidad de equilibrar la innovación tecnológica con la salvaguarda de los principios constitucionales. Se proponen, además, vías para reforzar la intervención humana y los mecanismos de control en el ámbito empresarial, dada su incidencia directa y creciente en los derechos de las personas trabajadoras.

Palabras clave: *Big Data*; inteligencia artificial; derecho del trabajo; gestión laboral algorítmica; protección de datos; capitalismo de la vigilancia; Reglamento de inteligencia artificial.

Recibido: 03-09-2025 / Revisado: 05-10-2025 / Aceptado: 21-11-2025 / Publicado: 06-03-2026

Cómo citar: Fonseca Díaz, A. y Popiuc, M. P. (2026). Implicaciones de los sistemas de inteligencia artificial en la relación laboral. *Revista de Trabajo y Seguridad Social. CEF*, 491, 172-196. <https://doi.org/10.51302/rts.2026.24791>

Implications of Artificial Intelligence Systems in Labour Relations

Aida Fonseca Díaz (corresponding author)

PhD in Law; Lecturer, Department of Legal Sciences, Faculty of Legal Sciences, Education and Humanities.

University Europea of Madrid (Spain)

aida.fonseca@universidadeuropea.es | <https://orcid.org/0000-0001-7858-311X>

Maria Petronela Popiuc

PhD in Law (ANECA-accredited); Lecturer in Law.

University Camilo José Cela (Spain)

mpopiuc@ucjc.edu | <https://orcid.org/0000-0002-6599-0848>

Abstract

The growing availability of massive datasets presents unprecedented challenges in the legal field, as their processing through artificial intelligence systems directly impacts the protection of rights and the very structure of the constitutional state. This article examines how the current “Big Data fever” may affect the protection of workers’ personal data and to what extent the existing legal framework offers sufficient safeguards. Starting from Knowledge Discovery in Data Bases and the five dimensions of Big Data, the analysis explores how the massive accumulation of information demands a regulatory framework that ensures transparency, accountability, and respect for fundamental rights. Through a critical review of labor regulations and the Artificial Intelligence Regulation, the article addresses the risks associated with algorithmic management of labor relations and reflects on the need to balance technological innovation with the safeguarding of constitutional principles. It also proposes ways to strengthen human oversight and control mechanisms within the business sphere, given their direct and growing impact on workers’ rights.

Keywords: Big Data; artificial intelligence; labor law; algorithmic management; data protection; surveillance capitalism; EU AI act.

Received: 03-09-2025 / Revised: 05-10-2025 / Accepted: 21-11-2025 / Published: 06-03-2026

Citation: Fonseca Díaz, A. y Popiuc, M. P. (2026). Implications of Artificial Intelligence Systems in Labour Relations. *Revista de Trabajo y Seguridad Social. CEF*, 491, 172-196. <https://doi.org/10.51302/rtss.2026.24791>

Sumario

- 1. Introducción: la fiebre del *Big Data*
 - 2. El proceso de tecnologización y la gestión laboral algorítmica (*algorithmic management*)
 - 3. Protección de datos en el capitalismo de la vigilancia
 - 4. Consecuencias de la dependencia algorítmica en las relaciones laborales
 - 4.1. Protección de las personas trabajadoras en la toma de decisiones automatizadas
 - 4.2. Alfabetización de las personas intervinientes en la cadena de valor de los sistemas de IA
 - 5. Conclusiones
- Referencias bibliográficas

1. Introducción: la fiebre del *Big Data*

La inteligencia artificial (IA) se refiere al conjunto de sistemas capaces de realizar tareas que, hasta ahora, requerían inteligencia humana: analizar información, razonar, tomar decisiones o resolver problemas. Estos sistemas pueden ser puramente digitales (como asistentes virtuales o motores de recomendación) o tener componentes físicos (robots, sensores inteligentes, etc.). Su aplicación abarca desde la medicina hasta la banca, la educación o el mercado laboral.

En el centro de muchos de estos sistemas se encuentra el llamado *machine learning* o aprendizaje automático, una rama de la IA que permite a las máquinas aprender de los datos sin haber sido programadas de forma explícita para cada tarea. A través de algoritmos específicos, estos sistemas son capaces de identificar patrones, extraer conclusiones y mejorar su rendimiento conforme procesan más información. Ahora bien, para que estos algoritmos funcionen y evolucionen, necesitan grandes volúmenes de datos. De ahí que conceptos como el *Big Data* y la minería de datos se hayan convertido en pilares imprescindibles de esta nueva era tecnológica.

En este sentido, el denominado KDD (*Knowledge Discovery in Data Bases*) es un proceso no trivial de extracción de información a partir de datos potencialmente útiles para el usuario que consta de varias etapas: una de estas es la denominada «minería de datos» o *data mining*. La minería de datos permite transformar todos estos datos en conocimiento, mediante un proceso complejo que se desarrolla desde el filtrado de los datos hasta su validación final y sirve para descubrir patrones, relaciones y tendencias, lo que puede ser beneficioso para la toma de decisiones estratégicas y para la propia generación del conocimiento (Fayyad *et al.*, 1996).

Por tanto, el proceso de minería de datos es lo que sustenta los algoritmos del *machine learning* o aprendizaje automático que alimentan los sistemas de IA (Molina Félix, 2002). Por lo que podríamos afirmar que el *Big Data* es el punto de unión de todos estos conceptos.

El concepto de *Big Data* no solo abarca la cantidad de datos, sino también una serie de características muy específicas denominadas las 5V's: volumen, velocidad, variedad, veracidad y valor. A fin de aproximarnos a la importancia del *Big Data* en el tejido empresarial, nos detendremos solo en el volumen de los datos. Esta característica hace referencia al tamaño: el *byte* es la unidad de información de base utilizada en computación. En la actualidad, es tal la cantidad de datos, que, en tan solo unos años, hemos pasado del *megabyte*

al *zettabyte*, e incluso lo hemos sobrepasado, pues hay quienes se refieren al *brontobyte* para hacer referencia a esta ingente cantidad de información¹.

En términos gráficos, en el año 2022 se consumieron en total 79 *zettabytes*, esto es, 79.000.000.000.000.000.000.000.000 de *bytes*, la cifra es tan difícil de asimilar que, haciendo una analogía, podríamos guardar el equivalente a 17.200 millones de iPhones de 64 GB o grabar una película HD a 1080p con una duración de 36 millones de años (Díaz Bonet, 2023). Y vamos en aumento: la edición 10.0 de *Data Never Sleeps* prevé que se generen y consuman a nivel mundial 181 *zettabytes* para 2025, es decir, 181 sextillones de *bytes*. El impacto de la IA en todas las facetas de la vida y los recursos necesarios para abastecer todo su potencial se reflejan en los datos. De acuerdo con el último informe «*Data Never Sleeps: AI Edition*» de julio de 2024, cada minuto, Dall-E 2 genera 1.389 imágenes, 19.028 imágenes son creadas por otras plataformas de conversión de texto a imagen y 7.431 minutos de vídeo son generados por herramientas IA².

Con esta aproximación teórica podemos percatarnos fácilmente de esta nueva «fiebre del *Big Data*»³, es decir, del valor que tienen estos datos en el ámbito empresarial y geopolítico, y consecuentemente también en el legal y su impacto en las relaciones laborales. Como se puede deducir, nada de todo esto es gratis, especialmente si se trata de tecnología: cada minuto se gastan 293.000 dólares en IA⁴.

La alta inversión en activos de datos tiene una razón de ser: los beneficios y ventajas que las organizaciones pueden obtener de ellos, como innovaciones, servicios, medidas de seguridad, mejora en el proceso de toma de decisiones, mejores experiencias para los clientes (lo que se traduce en un aumento de las ventas), mayor eficiencia operativa y nuevas fuentes de ingresos. En consecuencia, la inversión en sistemas de IA y en *machine learning* es imprescindible para poder procesar y analizar estos grandes volúmenes de datos (Coyle y Manley, 2022).

Teniendo en cuenta que esta inversión en *machine learning* impactará en el posicionamiento de unas empresas frente a otras, en la productividad y, en consecuencia, en los beneficios, no es despreciable considerar que estas emplearán muchos recursos y esfuerzos en proteger la confidencialidad de sus algoritmos⁵.

¹ No está claro el origen del concepto «brontobyte». El término «byte» fue acuñado por Werner Buchholz ingeniero de IBM en 1956, para hacer referencia al conjunto más pequeño de datos, compuesto por 8 bits.

² No obstante, el informe también refleja aspectos no tan positivos como que cada minuto, los empleados ahorran 467.882 horas de trabajo utilizando ChatGPT y son 52 los trabajos universitarios marcados por plagio de IA en Turnitin cada minuto (DOMO, 2024).

³ De ahí que empleemos la expresión «la fiebre del *Big Data*» para referirnos a una nueva fiebre del oro, como sucedió en California (Estados Unidos) entre 1848 y 1855.

⁴ Como también concluye el referido informe y la infografía recuperada de DOMO (2024).

⁵ Se hace referencia a los potenciales beneficios del tejido empresarial, sin perjuicio de otros intereses institucionales o gubernamentales, en los que no incidiremos en este artículo.

2. El proceso de tecnologización y la gestión laboral algorítmica (*algorithmic management*)

La utilización del *Big Data* por parte del tejido empresarial en el desarrollo e implementación de sistemas de IA se ha venido denominando *algorithmic management* o gestión laboral algorítmica. Esta expresión hace referencia al proceso mediante el cual, a partir de los datos proporcionados a los algoritmos, estos son empleados con fines estratégicos para la empresa y también para la selección, dirección, monitorización, vigilancia e incluso la imposición de medidas disciplinarias a los empleados y las empleadas (Todolí Signes, 2023).

Con ello, se refuerza el poder de control y dirección de la empresa prevenido en el artículo 20 del Estatuto de los Trabajadores (ET), ya que los resultados obtenidos permitirán establecer patrones y predicciones que faciliten las acciones descritas (Rivas Vallejo, 2020). De hecho, parte de la doctrina sostiene que, a corto plazo, con el fin de optimizar costes y aumentar los beneficios empresariales, la tecnologización de los procesos productivos implicará ir mucho más allá de la inversión en tecnología, logrando una reducción radical de las plantillas en las empresas (Selma Penalva, 2021).

Ante los cambios producidos como consecuencia de la tecnologización, y en particular frente a la eliminación de puestos de trabajo, se han identificado movimientos como el «neoludismo», definido en el Segundo Congreso Ludita celebrado en 1996 como «un movimiento sin líderes, de resistencia pasiva al consumismo y a las tecnologías cada vez más extrañas y amenazadoras de la Edad Informática». Con ello, no cabría una confrontación directa con el desarrollo tecnológico sino un uso erróneo o malintencionado que perjudique a los seres humanos⁶.

A pesar de las resistencias, se está invirtiendo mucho en IA. En España, durante el primer trimestre de 2024, el 19,79 % de las empresas de 50 a 249 empleados utilizó tecnologías de IA, un porcentaje que asciende al 40,64 % en empresas de 250 o más empleados, mientras que en las empresas de menos de 10 empleados el porcentaje apenas alcanza el 6,60 %. Además, podemos destacar otros datos relevantes que anuncian cambios en la relación laboral (si es que no se están produciendo ya⁷):

⁶ Tal y como desarrolla García García (2023), el neoludismo se sostiene en tres principios: 1) no se rechaza la tecnología, sino el mal uso que se hace de ella y que perjudica a la humanidad; 2) la tecnología es política: está al servicio del poder; 3) la visión personal de la tecnología es peligrosamente limitada: la tecnología tiene repercusiones sociales y ambientales. Este ideario también es defendido por otros laboristas.

⁷ Aunque también es significativo que las pequeñas empresas ya estén utilizando sistemas de IA, por lo que tímidamente van aumentando la confianza y/o la disponibilidad de recursos empresariales en estas tecnologías. INE, Encuesta sobre el uso de TIC y del comercio electrónico en las empresas. Año 2023, primer trimestre 2024. (Datos definitivos actualizados en enero de 2025). Vid. <https://www.ine.es/jaxi/Datos.htm?tpx=59891>. Pueden consultarse los datos anteriores en https://www.ine.es/dyngs/INEbase/es/operacion.htm?c=estadistica_C&cid=1254736176743&menu=ultiDatos&idp=1254735576799

Tabla 1. La IA en las empresas (primer trimestre de 2023) por agrupación de actividad económica

Empresas	De 10-49	50-249	Más de 250
Empresas que no utilizan ninguna de las tecnologías de IA porque: faltan conocimientos especializados relevantes en la empresa	78,76	77,52	78,28
Empresas con tecnología IA de aprendizaje automático o <i>machine learning</i> para el análisis de datos	26,02	39,09	52,72
Empresas con tecnología IA de automatización de flujos de trabajo o ayuda en la toma de decisiones	30,83	41,08	55,79
Empresas que emplean tecnologías de IA para procesos de producción	25,71	32,21	42,53
Empresas que emplean tecnologías de IA para organización de procesos de administración o gestión empresarial	24,10	23,65	31,37

Fuente: elaboración propia a partir de los datos del INE.

Como se deduce de la tabla, existe un alto interés por parte del tejido empresarial de implementar y utilizar sistemas de IA para el análisis de datos (un porcentaje que oscila entre el 26 % y el 52 %, según el tamaño de la empresa), para la toma de decisiones (entre un 30 % y un 55 %), para los procesos de producción (entre un 25 % y un 42 %) y para la organización de procesos de administración y la gestión empresarial (entre un 24 % y un 31 %). Sin embargo, una de las dificultades para utilizarlas es la falta de conocimientos especializados relevantes para la materia cuyo porcentaje supera el 75 % sea cual sea el tamaño de la empresa, cuestión sobre la que incidiremos más adelante.

De acuerdo con estos datos, podríamos afirmar que la tecnologización del tejido empresarial en los procesos con el fin de aumentar en productividad y competitividad está creciendo exponencialmente en los últimos años, fundamentalmente a partir de la pandemia provocada por el COVID-19⁸, por lo que la gobernanza de los sistemas de IA está planteando problemas de diversa naturaleza, esencialmente jurídica⁹.

⁸ Incluso parte de la doctrina sostiene que la informatización de los procesos productivos alcanza hoy su punto máximo (Selma Penalva, 2021).

⁹ En particular, de naturaleza conceptual (qué entendemos por sistemas y modelos de IA), funcional y de orden práctico (en cuanto a su implementación) y, especialmente, de naturaleza jurídica (Fernández Villarino, 2021).

En este sentido, Mercader Uguina (2022, p. 28) se refiere al dato como «la materia prima capital de la sociedad de la información y del conocimiento». En la película *Justicia artificial* estrenada en 2024 en España, se introduce la posibilidad de desarrollar un algoritmo que priorice la vida de determinadas personas (VIP para el algoritmo) en caso de accidente. ¿Podría existir esta posibilidad en un futuro?, ¿hasta dónde se extendería la protección industrial del algoritmo como secreto profesional frente a su colisión con otros derechos fundamentales como la vida de las personas?

Garantizar el secreto de los algoritmos generará un valor en ocasiones incalculable para el tejido empresarial. Por ello, no nos deberían sorprender noticias como que la multinacional estadounidense Meta Platforms, Inc (dueña de un conglomerado de empresas como Facebook, Instagram, WhatsApp y Threads, entre otros) haya decidido eliminar a los verificadores de contenidos, sustituyéndoles por «notas comunitarias», como ya lo hiciera X (en su día, Twitter) propiedad de Elon Musk¹⁰.

De acuerdo con el artículo 1 de la Ley 1/2019, de 20 de febrero, de secretos empresariales, se considera secreto empresarial cualquier información o conocimiento (incluido el tecnológico, científico, industrial, comercial, organizativo o financiero) que reúna tres condiciones: que sea secreto, que tenga un valor empresarial (real o potencial) debido a su carácter secreto y que haya sido objeto de medidas razonables por parte de su titular para mantenerlo en secreto. La protección proporcionada por el precepto cubre a cualquier persona física o jurídica como titular del secreto empresarial, que legítimamente ejerza el control sobre el mismo, extendiéndose a cualquier modalidad de obtención, utilización o revelación de la información constitutiva de aquel que resulte ilícita o tenga un origen ilícito conforme a esta ley. De acuerdo con parte de la doctrina, los algoritmos y los sistemas de IA se encontrarían dentro de la protección que proporciona dicho precepto. ¿Estamos, por tanto, desprotegidos frente a los efectos nocivos de los algoritmos?

3. Protección de datos en el capitalismo de la vigilancia

Para Zuboff, el capitalismo de la vigilancia se fundamenta en la recolección y el análisis intensivo de datos de comportamiento humano mediante dispositivos inteligentes, transfor-

¹⁰ Aunque aún no sabemos de qué forma desarrollará Meta las notas a la comunidad, en la red social X, las notas de la comunidad permiten que los propios usuarios moderen el contenido de las publicaciones sin que la empresa supervise directamente el proceso (como Meta lo hacía antes a través de los verificadores de contenidos). Un grupo de usuarios se puede registrar como colaboradores para añadir una nota en la que se informe de una información errónea o engañosa contenida en una publicación. Después, otros usuarios colaboradores califican dicha nota como útil o no útil. Cuando se alcanza un número suficiente de puntuaciones útiles, la empresa añade una nota pública debajo de la publicación en cuestión. La red social X implementó esta posibilidad en 2019 (Twitter) cuando un equipo de desarrolladores planteó la posibilidad de incorporar un modelo de *crowdsourcing* para resolver los problemas que tenía la red social para moderar los contenidos (Armero y Goodwin, 2025).

mándolos en predicciones y acciones que sirven a los intereses comerciales de las grandes tecnológicas. Mediante esta arquitectura automatizada, las empresas moldean la conducta de los usuarios y las usuarias para maximizar beneficios, reduciéndolos a meros «usuarios» y «usuarias» y socavando las regulaciones que protegen sus derechos, lo cual, según la autora, pone en peligro la democracia.

Son muchas sus manifestaciones en el ámbito laboral, abarcando desde el registro, los sistemas de videovigilancia, microfónicos y telefónicos, el acceso a los archivos del ordenador o a los programas informáticos instalados (incluso en remoto), el rastreo por geolocalización, los controles biométricos, el seguimiento por correo electrónico, por redes sociales o el control de las páginas web que ha visitado la persona trabajadora y el control informático de la productividad en tiempo real (Mercader Uguina, 2001).

El artículo 4.14 del Reglamento general de protección de datos (RGPD) define los datos biométricos como aquellos datos personales obtenidos mediante tratamientos técnicos específicos sobre características físicas, fisiológicas o conductuales que permiten la identificación única de una persona (p. ej., imágenes faciales, huellas dactilares). Esta definición coincide literalmente con el artículo 3 de la Directiva 2016/680 y el artículo 3 del Reglamento de inteligencia artificial (RIA) 2024. Incluye tanto sistemas de reconocimiento de emociones e identificación biométrica como de categorización (edad, color de ojos, orientación sexual o política)¹¹.

En concreto, conforme al WP80 del Grupo de Trabajo sobre protección de datos del artículo 29 (GT29), los sistemas de control biométrico permiten su registro o codificación en dos categorías: las físicas o fisiológicas y las comportamentales. Las físicas miden las características físicas de una persona entre las que se encuentran: la comprobación de las huellas digitales, análisis de la imagen del dedo, reconocimiento del iris, análisis de la retina, reconocimiento facial, reconocimiento de muestras de las manos, reconocimiento de la forma de la oreja, detección del olor corporal, reconocimiento de la voz, análisis de muestras de ADN y análisis de los poros de la piel, etc.¹². En cuanto a los comportamentales, miden el comportamiento de una persona e incluyen la comprobación de la firma manuscrita, el análisis de la pulsación sobre las teclas, el análisis de la forma de caminar, etc. Posteriormente, el Dictamen 3/2012 del GT29 sobre la evolución de las tecnologías biométrica adoptado el 27 de abril de 2012, añade las psicológicas, como la medición de la respuesta a situaciones concretas o pruebas específicas que se ajusten a un perfil psicológico (GT29, 2012, p. 4).

¹¹ El considerando 8 distingue los sistemas de identificación biométrica remota en «tiempo real» —donde captura, comparación e identificación se realizan instantánea o casi instantáneamente con material de vídeo en directo— de los sistemas «en diferido», en los que los datos se recogen previamente y la comparación e identificación se efectúan tras una demora significativa usando grabaciones o imágenes almacenadas.

¹² Aunque el uso del ADN para la identificación biométrica plantea cuestiones específicas, el presente documento no va a ocuparse de ellas. Se puede señalar que la generación de un perfil de ADN en tiempo real como instrumento de autenticación no parece posible actualmente (GT29, 2023, pp. 3 y 4).

De acuerdo con los riesgos que puede producir el tratamiento de estos datos, el RIA prevé la existencia de sistemas de IA que considera de alto riesgo por tener la capacidad de afectar a la salud y la seguridad de los derechos fundamentales de las personas. En particular, y de acuerdo con la remisión al anexo III que realiza el artículo 6 del RIA, se considerarán sistemas de IA de alto riesgo aquellos que afecten a una pluralidad de ámbitos¹³, entre los cuales se encuentran: la identificación biométrica y categorización de personas físicas, es decir, sistemas de IA destinados a utilizarse en la identificación biométrica remota «en tiempo real» o «en diferido» de personas físicas y el empleo, la gestión de los trabajadores y el acceso al autoempleo, tales como la contratación o selección de personas físicas o los sistemas de IA empleados para tomar decisiones relativas a la promoción y resolución de relaciones contractuales de índole laboral.

Para estos sistemas, el RIA determina establecer, implantar, documentar y mantener un sistema de gestión de riesgos asociado específicamente a los mismos, entendiendo por tal un proceso iterativo continuo que se llevará a cabo durante todo el ciclo de vida de un sistema de IA de alto riesgo, mediante el requerimiento de actualizaciones sistemáticas periódicas. Por ello, el reglamento consiente autorizar una extensa variedad de sistemas de IA con riesgo alto, aunque supeditándolos a una serie de requisitos horizontales de protección y obligaciones para acceder al mercado de la Unión Europea¹⁴.

En el ámbito laboral, el empleador podría utilizar los sistemas de reconocimiento facial no solo para el control de la asistencia, sino también para predecir patrones de movimientos durante su actividad laboral. Por ello, el Dictamen 2/2017 sobre el tratamiento de datos del GT29 advierte que las empresas deben abstenerse de utilizar estas tecnologías, con algunas excepciones marginales¹⁵, pero tales escenarios no

¹³ El anexo III incluye ocho ámbitos: identificación biométrica; infraestructuras críticas; educación y formación profesional; empleo, gestión de los trabajadores y acceso al autoempleo; acceso a servicios privados esenciales y a servicios y prestaciones públicas esenciales, y disfrute de estos; garantía del cumplimiento del derecho; migración, asilo y gestión del control fronterizo; y Administración de Justicia y procesos democráticos.

¹⁴ Los legisladores han aclarado y precisado dichos requisitos de manera que sean más viables desde el punto de vista técnico y supongan una carga menor para las partes interesadas, por ejemplo, en lo que respecta a la calidad de los datos o a la documentación técnica que deben elaborar las pymes para demostrar que sus sistemas de IA de alto riesgo cumplen los requisitos establecidos. Dado que los sistemas de IA se desarrollan y distribuyen mediante cadenas de valor complejas, el texto transaccional incluye cambios que aclaran la asignación de responsabilidades y las funciones de los distintos agentes de dichas cadenas, en particular los proveedores y los usuarios de sistemas de IA (Consejo de la Unión Europea, 2023). Las condiciones concretas para entender que un sistema es de alto riesgo, vienen recogidas en el artículo 6.1 del RIA.

¹⁵ De acuerdo con el RGPD, el tratamiento de datos biométricos con fines de identificación debe basarse en una de las excepciones previstas en el artículo 9, apartado 2: que el interesado haya dado su consentimiento explícito, 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

pueden utilizarse para invocar una legitimación general del uso de tecnologías de reconocimiento facial¹⁶.

El control de la conducta de la persona trabajadora mediante estos sistemas se denomina *software in accounting*. Estos sistemas permiten, previa identificación del operador, memorizar el número de operaciones efectuadas por el mismo, el número de errores cometidos al efectuarlas, el tiempo empleado para cada una, el tiempo total de trabajo, la memoria utilizada, el número de frecuencia y la duración de las interrupciones. De acuerdo con el análisis realizado con anterioridad, el tratamiento de estos datos por parte del empleador será lícito siempre que exista interés legítimo y se cumplan principios de proporcionalidad y subsidiaridad, estableciéndose como límites la dignidad humana sus intereses legítimos y los derechos fundamentales¹⁷.

Conforme al artículo 88 del RGPD los convenios colectivos deben establecer normas específicas para garantizar la protección de los derechos y libertades en relación con el tratamiento de datos personales de los trabajadores en el ámbito de la relación laboral. En España, la Ley 12/2021, de 28 de septiembre, por la que se modifica el ET (conocida como Ley *riders* mediante la inclusión de la presunción de laboralidad en el ámbito de las plataformas digitales de reparto) prevé que los convenios colectivos establezcan límites a la vigilancia ejercida mediante IA a los trabajadores y las trabajadoras¹⁸.

Finalmente, el RIA recoge un amplio número de prácticas de IA prohibidas, con la posibilidad de utilizar la identificación biométrica remota por parte de las autoridades policiales. A fin de facilitar la comprensión de todas las recogidas en el artículo 5, proporcionamos a continuación una tabla de aquellas que afectarían al ámbito laboral:

protección social, para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento, que el tratamiento sea necesario para fines de medicina preventiva laboral, por razones de interés público en el ámbito de la salud pública o que el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos, entre otros.

¹⁶ Dictamen 2/2017 sobre el tratamiento de datos en el trabajo. Adoptado el 8 de junio de 2017. WP249.

¹⁷ Así lo dispone el artículo 88 del RGPD conforme al cual:

Dichas normas incluirán medidas adecuadas y específicas para preservar la dignidad humana de los interesados, así como sus intereses legítimos y sus derechos fundamentales, prestando especial atención a la transparencia del tratamiento, a la transferencia de los datos personales dentro de un grupo empresarial o de una unión de empresas dedicadas a una actividad económica conjunta y a los sistemas de supervisión en el lugar de trabajo.

¹⁸ En concreto, se introduce una nueva letra d) en el artículo 64.4, en virtud de la cual la persona trabajadora tiene derecho a ser informada por la empresa de los parámetros, reglas e instrucciones en los que se basan los algoritmos o sistemas de IA que afectan a la toma de decisiones que pueden incidir en las condiciones de trabajo, el acceso y mantenimiento del empleo, incluida la elaboración de perfiles.

Tabla. 2. Prácticas de IA prohibidas

Sistema prohibido	Técnicas y prácticas incluidas
Sistemas de IA que trasciendan la conciencia de una persona.	• Técnicas subliminales que trasciendan la conciencia de una persona. • Técnicas deliberadamente manipuladoras o engañosas con el objetivo o efecto de alterar sustancialmente el comportamiento de una persona o colectivo mermando de manera apreciable su capacidad para tomar una decisión informada y haciendo que tomen una decisión que de otro modo no habrían tomado, de un modo que provoque, o sea razonablemente probable que provoque, perjuicios considerables a esa persona, a otra o a un colectivo¹⁹.
Sistemas de IA que aprovechen las vulnerabilidades de algunas personas.	• Sistema que aproveche alguna de las vulnerabilidades de una persona física o un determinado colectivo derivadas de su edad o discapacidad, o de una situación social o económica específica, con la finalidad o el efecto de alterar de manera sustancial el comportamiento de dicha persona o de una persona que pertenezca a dicho colectivo de un modo que provoque, o sea razonablemente probable que provoque, perjuicios considerables a esa persona o a otra.
Sistemas de IA que permitan evaluar o clasificar la fiabilidad de las personas físicas o colectivos.	• Evaluar o clasificar a personas físicas o a colectivos de personas durante un periodo determinado de tiempo atendiendo a su comportamiento social o a características personales o de su personalidad conocidas, inferidas o predichas, de forma que la puntuación ciudadana resultante provoque una o varias de las situaciones siguientes: 1) un trato perjudicial o desfavorable hacia determinadas personas físicas o colectivos de personas en contextos sociales que no guarden relación con los contextos donde se generaron o recabaron los datos originalmente; 2) un trato perjudicial o desfavorable hacia determinadas personas físicas o colectivos de personas que sea injustificado o desproporcionado con respecto a su comportamiento social o la gravedad de este.



¹⁹ Son varios los términos y adjetivos incluidos en esta definición que necesitarán una mayor aclaración a efectos de categorizar un sistema de IA como prohibido o permitir, por el contrario, su entrada y desarrollo: qué se debe entender por una alteración «sustancial» frente a una alteración no sustancial de la conciencia humana, cómo lo «apreciarán» las personas responsables y qué debemos entender como «razonable» o «considerable» a estos efectos.

Sistema prohibido	Técnicas y prácticas incluidas
Sistemas de IA que permitan realizar evaluaciones de riesgos de personas físicas con el fin de valorar o predecir el riesgo de cometer un delito.	Realizar evaluaciones de riesgos de personas físicas con el fin de valorar o predecir el riesgo de que una persona física cometa un delito basándose únicamente en la elaboración del perfil de una persona física o en la evaluación de los rasgos y características de su personalidad. * Esta prohibición no se aplicará a los sistemas de IA utilizados para apoyar la valoración humana de la implicación de una persona en una actividad delictiva que ya se base en hechos objetivos y verificables directamente relacionados con una actividad delictiva.
Sistemas de IA que permitan realizar el reconocimiento facial mediante la extracción no selectiva de imágenes.	- El fin específico establecido en la definición. - El uso de un sistema de IA que cree o amplíe bases de datos de reconocimiento facial mediante la extracción no selectiva de imágenes faciales de internet o de circuitos cerrados de televisión.
Sistemas de IA para inferir las emociones de una persona física en los lugares de trabajo y en los centros educativos.	El fin específico establecido en la definición. * Excepto cuando el sistema de IA esté destinado a ser instalado o introducido en el mercado por motivos médicos o de seguridad.
Sistemas de IA para la categorización biométrica y clasificación individual de las personas físicas.	- El fin específico establecido en la definición. - Para deducir o inferir su raza, opiniones políticas, afiliación sindical, convicciones religiosas o filosóficas, vida sexual u orientación sexual. * Esta prohibición no incluye el etiquetado o filtrado de conjuntos de datos biométricos adquiridos lícitamente, como imágenes, basado en datos biométricos ni la categorización de datos biométricos en el ámbito de la garantía del cumplimiento del derecho.
Sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público.	- Se prohíbe el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía del cumplimiento del derecho, salvo y en la medida en que dicho uso sea estrictamente necesario para alcanzar uno o varios de los objetivos siguientes: a) La búsqueda selectiva de víctimas concretas de secuestro, trata de seres humanos, explotación sexual de seres humanos o búsqueda de personas desaparecidas.

Sistema prohibido	Técnicas y prácticas incluidas
Sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público. (cont.)	b) La prevención de una amenaza específica, importante e inminente para la vida o la seguridad física de las personas físicas o de una amenaza real y actual o real y previsible de un atentado terrorista. c) La localización o identificación de una persona sospechosa de haber cometido un delito a fin de llevar a cabo una investigación o un enjuiciamiento penales o de ejecutar una sanción penal por alguno de los delitos mencionados en el anexo II (RIA) que en el Estado miembro de que se trate se castigue con una pena o una medida de seguridad privativas de libertad cuya duración máxima sea de al menos cuatro años.

Fuente: elaboración propia, 2025.

Teniendo en cuenta el rápido avance de la tecnología y la necesidad de adquirir unos conocimientos técnicos necesarios para la aplicación efectiva del RIA, el mismo prevé la necesidad de que la comisión evalúe y revise el Reglamento antes del 2 de agosto de 2029, y posteriormente cada cuatro años²⁰.

4. Consecuencias de la dependencia algorítmica en las relaciones laborales

Como se advirtió con anterioridad al tratar la «fiebre del *Big Data*», los intereses comerciales, productivos o estratégicos en preservar la confidencialidad de los algoritmos, pueden dificultar la persecución de responsabilidades. En este sentido, hay quienes defienden que, para evitar el monopolio de algunas multinacionales, los sistemas de IA se organicen utilizando

²⁰ Asimismo, antes del 2 de agosto de 2028 y posteriormente cada cuatro años, la comisión debe evaluar y comunicar al Parlamento Europeo y al Consejo la necesidad de modificar la lista de ámbitos de alto riesgo que figura en el anexo del reglamento, los sistemas de IA incluidos en el ámbito de aplicación de las obligaciones de transparencia, la eficacia del sistema de supervisión y gobernanza y los avances en el desarrollo de documentos de normalización sobre el desarrollo eficiente desde el punto de vista energético de modelos de IA de uso general, incluida la necesidad de medidas o acciones adicionales. Por último, antes del 2 de agosto de 2028 y posteriormente cada tres años, la comisión debe evaluar la repercusión y la eficacia de los códigos de conducta voluntarios para fomentar la aplicación de los requisitos establecidos para los sistemas de IA de alto riesgo a los sistemas de IA que no sean sistemas de IA de alto riesgo y, posiblemente, otros requisitos adicionales para dichos sistemas de IA.

DAOs en *blockchains* públicas como Ethereum, esto significaría, sin entrar en detalles técnicos, que los sistemas de IA se organicen en estructuras de gestión digital descentralizadas, es decir, sin una estructura jerárquica central definida y sin un líder o conjunto de líderes, regidas por contratos inteligentes con decisiones registradas en cadenas de bloques públicos –esto es el *blockchain* (libros contables digitales y transparentes)– como lo es Ethereum²¹.

Estos contratos especifican cómo se tomarán decisiones y cómo se asignarán los recursos dentro de la DAO. Ahora bien, parece poco probable que los intereses de las *Big Tech* como Meta, Nvidia, Apple, OpenAI, Microsoft, Alphabet (Google), Amazon o el conglomerado empresarial propiedad de Elon Musk (Tesla, SpaceX, XAI o X.com) coincidan con esta visión.

¿Qué queremos decir con todo ello? Al fin y al cabo, la ética algorítmica puede conducir (y conducirá) a un permanente desencuentro entre los intereses productivos de las empresas con la dignidad y el respeto de los derechos de los trabajadores y las trabajadoras (y de las personas en general, clientes, proveedores, etc.), fundamentalmente derivados del derecho a la intimidad, a la protección de datos, al secreto de las comunicaciones y otros, como su salud e integridad. Por ello, ante la incertidumbre que genera este conflicto, debemos plantearnos en qué medida las decisiones estratégicas que se desarrollen dentro de una empresa deben seguir dependiendo exclusivamente del ser humano, y en este sentido, cómo podemos garantizar la protección de trabajadores y trabajadoras ante determinadas decisiones estratégicas.

Como se ha venido advirtiendo, los algoritmos aprenden extrayendo patrones de datos, por lo que las personas con capacidad de decisión en una empresa podrían confiar en los resultados (predicciones) sin ni siquiera verse atraídas a conocer las razones que motivan dicha decisión o la posible responsabilidad de los profesionales y trabajadores que han intervenido durante la cadena de valor. A este nivel de confianza que se puede llegar a alcanzar en los sistemas de IA se le denomina «dependencia algorítmica», e incluso podría llegar a desarrollarse tanto en las empresas hasta el nivel de dirigirla (Faliero, 2021). Y aunque aún parezca un escenario utópico²², es una posibilidad que plantea el propio RIA, al incluir un amplio catálogo de prácticas prohibidas y de sistemas de alto riesgo, como vimos²³.

²¹ Una organización descentralizada autónoma (Decentralized Autonomous Organization, DAO, por sus siglas en inglés) es una entidad sin una estructura jerárquica central definida y sin un líder o conjunto de líderes. En su lugar, se basa en un conjunto de contratos inteligentes que se ejecutan en una red blockchain. Estos contratos especifican cómo se tomarán decisiones y cómo se asignarán los recursos dentro de la DAO. Las DAO son una forma de llevar a cabo actividades comunitarias y empresariales sin tener que depender de una autoridad centralizada. Al utilizar una blockchain para almacenar y validar las transacciones, se pueden garantizar la transparencia y la descentralización.

²² En realidad, utópico no es, como ya sucedió con una compañía de entrega a domicilio cuya base de datos ya estaba sometida a la gestión algorítmica (Sentencia del Tribunal Supremo 805/2020, de 25 de septiembre).

²³ Existen antecedentes a nivel europeo, como Tribunale Ordinario di Bologna (31 de diciembre de 2020). Sentenza (Caso Deliveroo: algoritmo FERank declarado discriminatorio), <https://abogadosenleonmv>.

4.1. Protección de las personas trabajadoras en la toma de decisiones automatizadas

El temor, cada vez más extendido, a la dependencia algorítmica, es decir, a que la toma de decisiones se realice a través de procesos automatizados ha venido explicándose por la doctrina más especializada con el lema *human in command* o «persona al mando»²⁴.

El artículo 22 del RGPD reconoce el derecho de toda persona a no quedar sometida a decisiones basadas únicamente en procesos automatizados con efectos jurídicos o similares, salvo tres excepciones: que sea necesario para un contrato, que la ley lo autorice con salvaguardias adecuadas, o que exista consentimiento explícito del interesado.

De acuerdo con Todolí Signes (2023) esto implica que la plataforma, para demostrar que hay intervención humana significativa, debería acreditar que, de forma estadísticamente relevante, se aparta de la toma de decisiones del algoritmo o, alternativamente, que el ser humano realiza un proceso de toma de decisiones independiente y que posteriormente es comparado con el tomado por el sistema de manera automatizada.

En esta línea, el artículo 14 del RIA exige que los sistemas de IA de alto riesgo incorporen mecanismos de supervisión humana efectiva –con interfaces adecuadas– para vigilar su uso y minimizar riesgos a la salud, la seguridad y los derechos fundamentales. Combinado con el artículo 22 del RGPD, impide que estos sistemas adopten decisiones con efectos jurídicos sobre personas físicas, salvo en los supuestos excepcionados por el propio RGPD.

Además, el «derecho a explicación» del artículo 22.3 del RGPD y el artículo 11 de la Directiva general de protección de datos exige que, tras una decisión algorítmica con efectos significativos, se informen al interesado los motivos y elementos principales de dicha resolución, sin necesidad de revelar el funcionamiento interno del algoritmo. El artículo 86 del RIA refuerza esta obligación para IA de alto riesgo, garantizando explicaciones «claras y significativas», y la Ley 12/2021 (art. 64.4 ET) exige además que el comité de empresa conozca los parámetros y reglas algorítmicos que afectan a la toma de decisiones.

En consecuencia, aunque entendamos que el derecho a una explicación no pueda aplicarse con carácter individual a conocer información del algoritmo concreto que tomó la

com/2021/02/05/sentencia-tribunal-ordinario-bolonia-31-diciembre-2020-caso-deliveroo-discriminacion-algoritmica-o-discriminacion-a-traves-de-un-algoritmo/ y Rechtbank Den Haag (5 de febrero de 2020). Vonnis (Caso SyRI: declarado ilegal por vulnerar el derecho a la privacidad y la transparencia), <https://fundacionhermes.org/primer-sentencia-europea-declara-ilegal-un-algoritmo-de-evaluacion-de-caracteristicas-personales-de-los-ciudadanos-2/>

²⁴ También conocido como *human-in command* (Hendricx, 2019) Organización Internacional del Trabajo (2019).

decisión, ello no implica que el comité de empresa sí pudiera solicitar el acceso a dicha información, aunque el algoritmo o el sistema de IA pudiera estar sometido a confidencialidad. Además de todas aquellas garantías y responsabilidades establecidas en el RIA en cuanto a los sistemas de gobernanza, de transparencia y no discriminación²⁵.

4.2. Alfabetización de las personas intervinientes en la cadena de valor de los sistemas de IA

En las distintas etapas del KDD o descubrimiento de conocimiento en bases de datos²⁶ que explicamos con anterioridad, intervienen numerosos profesionales expertos en *Big Data*, fundamentalmente desde el ámbito de la ingeniería, como son el *data architect*, el *data engineer*, el *data analyst*, el *data scientist* y el *chief data officer (CDO)*. Cada uno de ellos está especializado en una fase del proceso.

Sin incidir en las funciones concretas de cada uno de ellos, conviene aproximarnos a su perfil profesional para comprender la importancia que tienen todos ellos en los resultados que ofrecen los sistemas de IA:

1. *Data architect*: se encarga de inspeccionar y analizar la infraestructura de datos en una organización, planifica futuras bases de datos e implementa soluciones para el almacenamiento y manejo de datos.
2. *Data engineer*: es responsable de toda la infraestructura de datos de una empresa. En términos prácticos, construye, prepara y mantiene los datos para que sean aptos para el análisis y la toma de decisiones.
3. *Data analyst*: es quien se encarga de estar en una constante búsqueda de necesidades de información que tengan las distintas áreas del negocio, para poder investigarlas y dar respuestas que sean útiles para la resolución de problemas y mejora de procesos.

²⁵ El responsable del despliegue también es el responsable de realizar la evaluación de impacto de derechos fundamentales del artículo 27 del RIA. Además, resultarían de aplicación las obligaciones de los responsables del despliegue de sistemas de IA de alto riesgo concretadas en el artículo 26 del RIA y el considerando 58 del RGPD que establece los fundamentos del principio de transparencia. Este exige que toda la información que se dirija, bien al interesado o al público en general, debe ser precisa, concisa, fácilmente accesible y comprensible, y que se utilice un lenguaje claro y sencillo (visualizándose, en su caso). En consonancia con el artículo 12 del RGPD, que impone la obligación al responsable del tratamiento de adoptar las medidas oportunas para facilitar al interesado la información establecida en los artículos 13 y 14 del RGPD.

²⁶ O simplemente de la *data mining* o minería de datos, al tratarse de la etapa del KDD centrada en el desarrollo de los métodos y técnicas para hacer que todos los datos tengan sentido.

4. *Data scientist*: desarrolla procesos de análisis de datos de alta complejidad, mediante el diseño y desarrollo de algoritmos que permitan encontrar hallazgos relevantes en la información, interpretar resultados y obtener conclusiones relevantes.
5. El *CDO* o director de datos es el responsable de analizar, clasificar y convertir todos los datos en bruto en estadísticas exactas, modelos prescriptivos y predictivos que marquen las estrategias de la empresa.

Descritas las funciones de estos profesionales, ¿de qué forma influye la formación no estrictamente técnica de las personas intervinientes en la cadena de valor de los sistemas de IA en las relaciones laborales? Es decir, ¿están formados todos estos trabajadores y trabajadoras en una ética profesional compartida?, ¿están sujetos a códigos deontológico al igual que otros colectivos?, ¿quién desarrolla y supervisa la ética de los algoritmos?

La principal consecuencia (y riesgo) de todo ello es que estos profesionales (enseñantes de la IA) carezcan de la formación ética y jurídica necesarias para comprender los límites, las consecuencias, y, en definitiva, el alcance que pueden tener los resultados que ofrezcan estos sistemas. Sobre esta cuestión, el RIA no contempla ninguna figura específica que realice las tareas de supervisión o vigilancia de los sistemas de IA, sino que se refiere a todas aquellas personas físicas que intervengan en el proceso. Así, el considerando 73 y el artículo 26.2 del RIA (referido a las obligaciones de los responsables de despliegue de los sistemas de IA de alto riesgo) prevén que los responsables de despliegue²⁷ encarguen la supervisión humana a personas físicas con formación, competencia y autoridad necesarias.

A estos efectos, resultarían de aplicación los considerandos 20 y 91, junto con el artículo 4 del RIA, ya que obligan a garantizar que todos los agentes de la cadena de valor (desde ingenieros de datos hasta supervisores humanos) cuenten con la formación, competencias y autoridad necesarias en IA. El considerando 20 exige capacitarles en las obligaciones de transparencia y no discriminación del reglamento; el 91, verificar sus competencias para aplicar y supervisar correctamente los sistemas, y el artículo 4 impone a proveedores y responsables del despliegue adoptar medidas que aseguren un nivel adecuado de alfabetización en IA, atendiendo a su experiencia, educación y al contexto de uso.

En este punto, sería interesante incidir en la responsabilidad de todas las personas intervinientes en la cadena de valor de los sistemas de IA, pudiendo llegar a ser sancionadas si, de haber recibido la formación a la que se prevé la normativa, cometieran algún tipo de negligencia o de transgresión de la buena fe. Del mismo modo, convendrá examinar en un futuro, tras la implementación del RIA, las obligaciones del delegado de protección de datos

²⁷ En este contexto, el «responsable del despliegue» (*deployment provider*, según la terminología del RIA) es definido como la persona física o jurídica, autoridad, agencia u otro organismo que utilice un sistema de IA bajo su autoridad, salvo que dicho sistema se utilice en el transcurso de una actividad personal o doméstica. Esta figura es clave en la fase de implementación práctica del sistema.

en la aplicación del RIA más allá de las funciones que ya asume en todos los sistemas que traten datos personales, así como la creación de una nueva figura en el organigrama corporativo o la adaptación de las propias funciones del delegado de protección de datos que asuma las funciones conferidas por el RIA (lo que ya recibe el nombre en foros tecnológicos de *RAI Champion* (*Responsible AI Champion*) o *AICO* (*AI Compliance Officer*).

5. Conclusiones

Todos los factores analizados a lo largo de este estudio implícitos a la propia tecnologización unidos al deterioro medioambiental y la transición energética, el envejecimiento de la población y el descenso de la natalidad (fundamentalmente en España), la competitividad en mercados nacionales e internacionales, los conflictos armados y la geopolítica, así como la gestión de futuras pandemias (y las consecuencias que perviven derivadas de la COVID-19) esbozan un escenario laboral complejo y disruptivo, marcado por la incertidumbre y la vertiginosa velocidad en su transformación (Selma Penalva, 2021). Además, también hemos de sumar los problemas actuales derivados de las pensiones, la temporalidad (y, en consecuencia, las elevadas tasas de desempleo juvenil) y la (des) protección del trabajador o trabajadora autónoma, y ha de añadirse la posibilidad de que en un futuro el trabajador-ser humano sea reemplazado por la trabajadora o el trabajador-maquinizado, por lo que estos problemas podrían acrecentarse. En cuanto a las pensiones, cabría preguntarse ¿cotizarán las trabajadoras o los trabajadores maquinizados? En consecuencia, ¿contribuirán al pago de las pensiones de los trabajadores-seres humanos? En caso contrario, ¿perderá la oportunidad el Estado de tomarse su pedacito de tarta?

Quizá pueda resultar complicado –al menos a corto plazo– extender el deber de cotización a las trabajadoras o los trabajadores-maquinizados, para ello tendríamos que entender que la IA general puede llegar a alcanzarse y ser real: por lo que parece razonable la hipótesis de una cotización especial por solidaridad debido a la reducción de las plantillas humanas²⁸.

En todo caso, el desempleo juvenil aumentaría, por lo que en sí misma la temporalidad no sería el problema, lo ocuparía todo el desempleo de larga duración derivado de la contratación a los nuevos empleados-robots o maquinizados. En consecuencia, se plantearía un escenario paradójico en el empleo juvenil pues concurrirían la sobreeducación y el exceso de competencias con la posible obsolescencia de sus conocimientos como consecuencia del paro de larga duración (Mercader Uguina, 2019, p. 177).

²⁸ Así lo plantea Selma Penalva (2021). Es razonable sostener esta hipótesis, pues ya se encuentran en vigor el Mecanismo de Equidad Intergeneracional (MEI) al igual que la reciente «cuota de solidaridad», que grava solo el exceso de salario sobre la base máxima de cotización mediante tipos por tramos, que se incrementan gradualmente desde alrededor del 1 % en 2025 hasta alcanzar en 2045 tipos del 5,5 %, 6 % y 7 % según el tramo del exceso.

Finalmente, y en cuanto a la desigualdad de género, podría presentarse un futuro desalentador: la feminización de determinados sectores de actividad precarizada (cuidado, educación y trabajo en el hogar) no solo correría el riesgo de acrecentarse sino de ser sustituido por el progreso de la tecnologización²⁹ unido a los sesgos y estereotipos sexistas derivados de los sistemas de contratación y de promoción profesional de las personas trabajadoras³⁰.

Podríamos considerar que parte de la solución a esta grave problemática la ofrecerían los nuevos yacimientos de empleo emergidos tras la previa destrucción de otros muchos mediante la tecnologización de los procesos productivos, pero ¿serán estos suficientes para compensar dicha pérdida?³¹

Entre los nuevos yacimientos de empleo o profesiones que pueden generarse durante el proceso de tecnologización, entre ellas, podríamos considerar: experto en *blockchain*, ingeniería artificial (más allá de los expertos en *Big Data* enumerados), especialistas en impresiones 3D, arquitecto e ingeniero de *smart cities* y casas inteligentes, ciberabogados (y similares), desarrolladores de aplicaciones de realidad virtual, *cloud engineer* o ingeniero *cloud* (supervisa los datos y la gestión en la nube), ciberseguridad, hiperautomatización de marketing con IA, *fintech* (finanzas y tecnología), *agile coach* y *scrum master* (es un facilitador de proyectos, encargados de liderar la gestión de proyectos en una organización entre los distintos equipos de trabajo), especialistas en *software* por voz y lingüistas (ya que en futuro la mayoría de instrucciones se introducirán por voz y no a través

²⁹ «Por cada siete hombres que trabajan en ocupaciones que están más amenazadas por el cambio tecnológico, es decir, que tienen una probabilidad del 90 por ciento o más de ser eliminadas por la tecnología, hay 10 mujeres en esos trabajos» (*Women, Automation, and the Future of Work (Executive Summary) - IWPR*). A título ilustrativo, conforme a los datos del Sindicato Español de Pilotos de Líneas Aérea (SEPLA), en España, apenas un 4 % de las mujeres son pilotos de avión (SEPLA, 2025). Y aunque ya hay más de un 50 % de juezas, abogadas y fiscales, hay un momento en el que el crecimiento en la carrera profesional se detiene. Tomando como ejemplo el caso de la judicatura, aunque hace 10 años, la cifra de mujeres en órganos judiciales colegiados en España era de 492 (de un total de 1.503 miembros de la Carrera Judicial destinados en esos tribunales) y hoy ya son 676 mujeres (de los 1.597 jueces/zas y magistrados/as en activo), la cifra va disminuyendo a medida que subimos en jerarquía: 433 se encuentran en audiencias provinciales, 203 en tribunales superiores de justicia, 28 en la Audiencia Nacional y solo 10 en el Tribunal Supremo, lo que supone un 12,34 % del total de magistrados/as en el máximo órgano judicial de España en la jurisdicción ordinaria, según el último informe sobre «Estructura demográfica de la Carrera Judicial» publicado por el Servicio de Estadística del Consejo General del Poder Judicial (CGPJ) <https://www.poderjudicial.es/cgpj/es/Temas/Estadistica-Judicial/Estudios-e-Informes/Estructura-demografica-de-la-Carrera-Judicial/>

³⁰ Ejemplo de todo ello fue el sistema desarrollado por Amazon para el reclutamiento de profesionales, cuyo algoritmo penalizaba el término «mujer» en los currículums (BBC News Mundo, 2018). Pero no solo debemos considerar la discriminación por razón de sexo, otros colectivos podrían verse afectados. Por ejemplo: si el algoritmo mide el tiempo de realización de una prueba, podría dejar fuera a personas con discapacidad.

³¹ Por lo que muchos autores han venido defendiendo la desaparición del derecho del trabajo y el retorno a la plena autonomía de la voluntad que permite el derecho civil. Así, Alemán (2002) y Durán López (2004).

de *prompts*), energías renovables y sostenibilidad, biotecnología y salud digital (nanomédicos, biomedicina y telemedicina debido al envejecimiento poblacional), entre otras (Schumpeter, 1985, pp. 117-124).

Además, debemos tener presente que la evanescencia de la empresa como espacio físico también podrá generar nuevos puestos de empleo en el metaverso (por ejemplo, dependientes, hosteleros digitales con representación de su avatar), si bien frente a las oportunidades internas que puede ofrecer el metaverso, también son mayores los riesgos de precariedad y *dumping* social (Nogueira Guastavino, 2022, p. 25). Más allá de su impacto en términos de destrucción o creación de empleo, el proceso de digitalización no solo reconfigura el mercado laboral, sino que también plantea riesgos para nuestras capacidades cognitivas y creativas. Este fenómeno ha sido descrito como «descarga cognitiva», esto es, la externalización progresiva de funciones mentales hacia dispositivos y sistemas tecnológicos, y se vincula doctrinalmente con el retroceso del denominado «efecto Flynn», relativo al estancamiento o disminución de determinados indicadores de capacidad intelectual en las últimas décadas.

Tal como advierte Gerlich (2025) la descarga cognitiva consiste en cómo el uso frecuente de herramientas de IA está cambiando nuestras habilidades cognitivas, llevándonos a tomar caminos más fáciles en la realización de algunas tareas. Según el estudio, utilizar los motores de búsqueda para acceder a los datos en lugar de profundizar en los datos y en la información estaría reduciendo nuestro pensamiento crítico y nuestra inferencia.

Este estudio es coincidente con el denominado «efecto Flynn», llamado así por el investigador neozelandés James R. Flynn. Se trata de un fenómeno observado en el campo de la inteligencia humana donde se ha identificado un aumento sostenido y significativo en las puntuaciones de los test de coeficiente intelectual a lo largo de varias décadas en muchas partes del mundo. Pues bien, desde 1930 estas puntuaciones de cociente intelectual habían estado aumentando de forma constante, pero la tendencia parece haber cambiado según el estudio de la Universidad de Northwestern, en virtud del cual el «efecto Flynn» parece haberse detenido e incluso estar revirtiéndose en tres categorías clave de inteligencia (Dworak *et al.*, 2023).

El estudio emplea una prueba de personalidad *online* denominada «Proyecto de Evaluación de Personalidad de Apertura Sintética» para analizar a casi 400.000 estadounidenses. Los investigadores registraron las respuestas de 2006 y de 2018 para comprobar si existían cambios en las puntuaciones relativas a la capacidad cognitiva. Los resultados mostraron caídas en razonamiento verbal (lógica y vocabulario), razonamiento matricial (resolución de problemas digitales y analogías) y habilidades matemáticas y computacionales (conocidas como series de letras y números). Sin embargo, las puntuaciones en razonamiento espacial siguieron el patrón opuesto. ¿Significa ello entonces que ahora somos menos inteligentes?

Recuerda Larson que existen tres tipos de inferencia: la IA clásica exploró las deducciones, la IA moderna explora las inducciones, pero sobre el tercer tipo –las abducciones– no

está trabajando nadie. Para Peirce, en su origen, la abducción es una reacción a la sorpresa. El pensamiento inteligente implica un conocimiento capaz de ir más allá de la observación directa, pero la forma en que adquirimos este conocimiento es un misterio, igual que la manera en que aplicamos el conocimiento adecuado en el momento oportuno a un problema. Por ello, ni la deducción ni la inducción sirven para arrojar luz sobre el misterio de la inteligencia humana.

De ahí que, por el momento, solo la inteligencia humana es capaz de desarrollar un pensamiento crítico y recurrimos a la imaginación, a la curiosidad y a la creatividad para generar soluciones a los problemas planteados. Conforme a estos estudios, el motivo de destrucción de muchos empleos no será tanto el proceso de tecnologización o incluso la llegada de la IA generativa, sino la pérdida de nuestra inferencia, de nuestra capacidad para conectar los puntos críticos y obtener conclusiones a partir de ellos. Los sistemas de IA pueden ofrecer respuestas rápidas e incluso aparentemente correctas, pero son respuestas matemáticas generadas a partir de una caja negra (*dark box*). Nunca deberíamos aceptarlas sin cuestionarlas previamente.

Tal y como afirman Robinson y Aronica (2024, pp. 83-119), unos de los mayores expertos en creatividad y muy críticos con los sistemas educativos actuales, el milagro de la especie humana no es cuánto nos hemos hundido, sino cómo magníficamente nos hemos levantado. Para Robinson y Aronica, tenemos un extraordinario poder humano: el poder de la imaginación. Damos por sentado esta capacidad de traer a la mente cosas que aún no están presentes, y con base en ello obtenemos hipótesis acerca de las cosas que nunca han sido, pero que podrían ser. Robinson y Aronica sostienen que la imaginación y la creatividad son rasgos exclusivos del ser humano, ausentes en el resto de las especies. Advierten que, sin quererlo, las prácticas cotidianas y la obsesión por la eficiencia industrial van adormeciendo esa capacidad innata en nosotros y en nuestros hijos e hijas. Propone recuperar la «experiencia anestésica» —estar plenamente conscientes y vivos— y apostar por modelos que valoren la creatividad más allá de su utilidad práctica.

Tanto el «efecto Flinn» como la descarga cognitiva están revelando lo que Robinson y Aronica y otros expertos llevan años vaticinando: vivimos en sociedades dominadas por la frivolidad (Lipovetsky, 2006, p. 13) dirigidos en una única dirección marcada por la industrialización y la suplantación del propio individuo. De ahí su acepción como sociedades posmodernas, ávidas de identidad y de realización personal inmediata en la que se disuelve la confianza en el propio individuo en pro del aquí y el ahora y en la promesa de la eterna juventud (Lipovetsky, 2004). Seducidos por los avances de los sistemas de IA no estamos siendo conscientes de que seremos nosotros mismos, y no una superinteligencia, los que decidamos perder aquello que nos hace realmente únicos en el mundo: nuestra imaginación, nuestra curiosidad y nuestra creatividad.

En definitiva, y como valoración del análisis desarrollado, puede afirmarse que el impacto de la IA en el ámbito laboral no debe interpretarse como un desenlace prefijado o un destino

inevitable, sino como un fenómeno en construcción, condicionado en gran medida por las decisiones sociales, políticas y jurídicas que adoptemos en el presente y en los próximos años. La clave no reside únicamente en anticipar si la IA sustituirá o no a la trabajadora o al trabajador (ser humano), sino en reflexionar colectivamente sobre qué modelo de relación laboral y de sociedad aspiramos a construir en esta nueva era de transformación tecnológica.

En nuestra opinión, el verdadero desafío consiste en encontrar un equilibrio entre el potencial innovador de estos sistemas y la necesidad de preservar los principios que han sostenido históricamente el Estado social y democrático de derecho, entre ellos, la protección de los derechos de las personas trabajadoras. Dicho de otro modo: el progreso tecnológico no puede concebirse al margen de los valores, principios y derechos que garantizan la cohesión social. Resulta imprescindible, por tanto, el respeto a los cambios integrados en el ordenamiento jurídico que afectan al derecho del trabajo y –muy especialmente– el fomento de la negociación colectiva como principal garante de las condiciones laborales ante los desafíos expuestos. Además, ante la magnitud de las consecuencias (aumento del desempleo –especialmente juvenil–, de la desigualdad de género, de la brecha salarial y de la exclusión social) es imprescindible que se fomente el desarrollo de políticas públicas acordes con esta nueva realidad laboral y la necesaria vigilancia por parte de la Administración laboral asegurando el cumplimiento de la normativa. Todo ello con un claro objetivo: que la IA no se convierta en un factor de precarización laboral y en un riesgo para la protección laboral de los trabajadores y trabajadoras, sino en un vector de desarrollo inclusivo.

Es innegable que la evolución tecnológica, lejos de erosionar los derechos fundamentales, puede convertirse en un instrumento para reforzar la justicia social, garantizar la sostenibilidad del sistema y consolidar la dignidad del trabajo humano en un contexto globalizado. Solo de este modo podremos transformar la incertidumbre que acompaña al cambio en una oportunidad real de modernización, capaz de cohesionar la eficiencia económica con el respeto a la persona trabajadora como eje central de cualquier orden jurídico-laboral.

Referencias bibliográficas

- Alemán, C. (2002). ¿Hacia la desaparición del Derecho del Trabajo? *Revista de Derecho Social*, (17).
- Armero, R. y Goodwin, G. E. (9 de enero de 2025). Mark Zuckerberg dice que Meta se inspirará en X: así funcionan las Notas de Comunidad. Business Insider. <https://www.businessinsider.es/tecnologia/mark-zuckerberg-dice-meta-inspirara-x-funcionan-notas-comunidad-1434505>
- BBC News Mundo (11 de octubre de 2018). *El algoritmo de Amazon al que no le gustan las mujeres*. <https://www.bbc.com/mundo/noticias-45823470>
- Coyle, D. y Manley, A. (2022). *What is the value of data? A review of empirical methods* (Policy Brief). Cambridge: Bennett Institute for Public Policy, University of Cambridge. <https://www.bennettinstitute.cam.ac.uk/publications/what-value-data-review-empirical-methods/>

- Consejo de la Unión Europea. (9 de diciembre de 2023). Artificial Intelligence Act: Council and Parliament strike a deal on the first worldwide rules for AI. <https://www.consilium.europa.eu/es/press/press-releases/2023/12/09/artificial-intelligence-act-council-and-parliament-strike-a-deal-on-the-first-worldwide-rules-for-ai>
- Consejo General del Poder Judicial. *Estructura demográfica de la Carrera Judicial*. <https://www.poderjudicial.es/cgpj/es/Temas/Estadistica-Judicial/Estudios-e-Informes/Estructura-demografica-de-la-Carrera-Judicial/>
- Díaz Bonet, G. (6 de julio de 2023). Los 8 data centers más bellos y sorprendentes del planeta. Escudo Digital. https://www.escudodigital.com/tecnologia/8-data-centers-mas-bellos-sorprendentes-planeta_53249_102.html
- DOMO. (6 de junio de 2024). *Domo releases "Data Never Sleeps: AI Edition" infographic*. Domo. <https://www.domo.com/es/news/press/domo-releases-data-never-sleeps-ai-edition-infographic>
- Dworak, E. M., Revelle, W. y Condon, D. M. (2023). Looking for Flynn effects in a recent online U.S. adult sample: Examining shifts within the SAPA Project. *Intelligence*, 98. <https://doi.org/10.1016/j.intell.2023.101734>
- Durán López, M. A. (2004). El fin del Derecho del Trabajo. *Relaciones Laborales*, 1.
- Faliero, J. C. (2021). Limitar la dependencia algorítmica. Impactos de la inteligencia artificial y sesgos algorítmicos. *Nueva Sociedad*, 294, 120-129. <https://nuso.org/articulo/limitar-la-dependencia-algoritmica/>
- Fayyad, U., Piatetsky-Shapiro, G. y Smyth, P. (1996). From data mining to knowledge discovery in databases. *AI Magazine*, 17(3), 37-54. <https://doi.org/10.1609/aimag.v17i3.1230>
- Fernández Villarino, R. (2021). El derecho ante la inteligencia artificial. A propósito de lo dispuesto en el art. 80.5 del Convenio Colectivo Nacional de la Banca. *Trabajo, Persona, Derecho, Mercado*, 4, 141-163. <https://doi.org/10.12795/TPDM.2021.i4.08>
- García García, A. (2023). La dignidad de la persona trabajadora en el centro del Derecho del Trabajo de la era digital. *Revista Jurídica de la Universidad de León*, 11, 3-18. <https://doi.org/10.18002/rjule.i11.8160>
- Gerlich, M. (2025). AI tools in society: Impacts on cognitive offloading and the future of critical thinking. *Societies*, 15(1), 6. <https://doi.org/10.3390/soc15010006>
- GT29. (1 de agosto de 2003). *Documento de trabajo sobre biometría* (Documento n.º 12168/02/ES WP 80). Bruselas. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp80_es.pdf
- GT29. (27 de abril de 2012). *Dictamen 3/2012 sobre la evolución de las tecnologías biométricas* (Documento n.º 00720/12/ES WP 193). Bruselas. https://www.aepd.es/documento/wp193_es.pdf
- Hendricx, F. (2019). Privacy 4.0 at work: Regulating employment, technology, and automation. *Comparative Labor Law & Policy Journal*, 41, pp. 166 y ss.
- Lipovetsky, G. (2004). *La era del vacío*. Anagrama.
- Lipovetsky, G. (2006). *El imperio de lo efímero. La moda y su destino en las sociedades modernas*. Anagrama.

- Mercader Uguina, J. R. (2001). Derechos fundamentales de los trabajadores y nuevas tecnologías: ¿Hacia una empresa panóptica? *Relaciones Laborales*, 10, 11-1.
- Mercader Uguina, J. R. (2019). *Reformas laborales en tiempos de digitalización y cambio tecnológico*. En *Anuario de la Facultad de Derecho de la Universidad Autónoma de Madrid* (Fasc. 1, pp. 163-182). Agencia Estatal Boletín Oficial del Estado. https://www.boe.es/biblioteca_juridica/anuarios_derecho/articulo.php?id=ANU-A-2019-10016300182
- Mercader Uguina, J. R. (2022). *Algoritmos e inteligencia artificial en el derecho digital del trabajo*. Tirant lo Blanch.
- Molina Félix, L. C. (2002). *Torturando a los datos hasta que confiesen*. UOC.
- Nogueira Guastavino, M. (2022). Metaverso y legislación aplicable al contrato de trabajo. *Revista de Trabajo y Seguridad Social. CEF*, 471, 17-53. <https://doi.org/10.51302/rtss.2022.3337>
- Organización Internacional del Trabajo. (2019). *Trabajar para un futuro más prometedor: Informe de la Comisión Mundial sobre el Futuro del Trabajo*. Ginebra: OIT. https://www.ilo.org/global/publications/books/WCMS_662410/lang-es/index.htm
- Selma Penalva, A. (2021). Inteligencia artificial y Derecho del Trabajo. *Ius et Scientia*, 7(2), 29-40. <https://doi.org/10.12795/IETSCIENTIA.2021.i02.03>
- SEPLA. (2025). *Aviadoras*. *Revista SEPLA*, 191. <https://sepla.es/revista/no191-aviadoras/>
- Rivas Vallejo, P. (2020). *La aplicación de la inteligencia artificial al trabajo y su impacto discriminatorio*. Thomson Reuters Aranzadi.
- Robinson, K. y Aronica, L. (2024). *El elemento: Descubrir tu pasión lo cambia todo* (2.ª ed.). Debolsillo.
- Schumpeter, J. A. (1985). *Capitalismo, socialismo y democracia*. TECSA.
- Todolí Signes, A. (2023). *Algoritmos productivos y extractivos: Cómo regular la digitalización para mejorar el empleo e incentivar la innovación*. Aranzadi.

Aida Fonseca Díaz. Doctora en Derecho con sobresaliente *cum laude* por la UAM. Es investigadora colaboradora en el GCIPS en la Universidad Europea. Ha participado en varias monografías, artículos y congresos relativos al ámbito del derecho procesal. Es abogada colegiada en el ICAM desde el año 2006 y ha sido letrada del SOJ Social. Ha realizado la revisión crítica de la normativa laboral examinando cómo la actual fiebre del *Big Data* afecta a la protección de los datos personales en el marco de la relación laboral y la jurisdicción social. <https://orcid.org/0000-0001-7858-311X>

Maria Petronela Popiuc. Doctora en Derecho acreditada por ANECA y profesora en Derecho en la Universidad Camilo José Cela. Ha participado como ponente en diversos congresos y seminarios de especialización en la disciplina. En el ámbito de la investigación, destaca su vinculación al grupo TECSEC y COMIDER de la UCJC. Ha realizado el análisis jurídico de los conceptos técnicos desarrollados en la investigación, contribuyendo a la proposición de vías para reforzar la tutela de los derechos de los trabajadores. <https://orcid.org/0000-0002-6599-0848>

Contribución de autorías. Las autoras han contribuido en un mismo porcentaje a la realización de este trabajo.