Hacia el trabajo del futuro: inteligencia artificial, derechos digitales y potestades empresariales

Yolanda Valdeolivas
Of Counsel
Laboral, Compensación y Beneficios

Belén López
Asesora Jurídica

Índice/

Resumen: Las nuevas tecnologías, potenciadas por la extensión del uso de sistemas de inteligencia artificial, están facilitando una nueva revolución industrial en las empresas, que tienen a su alcance de manera asequible y masiva un sinfín de posibilidades organizativas.

Las herramientas que los sistemas de inteligencia artificial ofrecen se muestran tan interesantes como arriesgadas desde el punto de vista de los límites del poder de dirección de la empresa sobre las personas trabajadoras. El interés por controlar el proceso productivo y el cumplimiento de los deberes contractuales con unos medios altamente sofisticados es susceptible de colisionar, en no pocas ocasiones, con derechos fundamentales, como la intimidad, el secreto de las comunicaciones o la protección de datos personales.

El presente artículo aborda esta cuestión desde la perspectiva europea y española, para analizar la práctica actual de las empresas y el contexto normativo en el que las mismas han de desenvolverse, al objeto de contrastar cómo las posibilidades que la tecnología brinda al funcionamiento empresarial y a la gestión de sus recursos humanos siguen siendo infinitas en un escenario regulador aún limitado.

Abstract: New technologies boosted by the widespread use of artificial intelligence systems are enabling a new industrial revolution within companies, which have endless organisational possibilities at their disposal.

Artificial intelligence systems offer several tools that are both interesting and risky regarding the limits of a company's managerial power over its employees. Controlling the production process and the fulfilment of contractual duties with highly sophisticated technology often clashes with fundamental rights, such as privacy, the confidentiality of communications and data protection.

This paper addresses this issue from a European and Spanish perspective, in order to analyse both the current practices of companies and their regulatory context, and to show that the possibilities offered by technology to business operations and the management of human resources are infinite but are constrained by a limited regulatory framework.

Palabras clave: Derecho del Trabajo; inteligencia artificial; algoritmos; datos personales; derechos digitales; poder de dirección; control biométrico.

Keywords: Employment Law; artificial intelligence; algorithms; personal data; digital rights; management power; biometric control.

Hacia el trabajo del futuro: inteligencia artificial, derechos digitales y potestades empresariales

I. Introducción

Las máquinas han sido, son y seguirán siendo el instrumento que permite a las empresas organizar las estructuras productivas y distribuir a la plantilla desde la perspectiva de la maximización de los rendimientos y, con ello, de los beneficios, en un proceso imparable desde la primera revolución industrial. Ahora, esas máquinas son robots, bots o dispositivos digitales dirigidos no solo a optimizar la producción sino a incrementar el propio control de la actividad laboral, lo que extiende los poderes directivos del empresario y hace más sensibles los derechos laborales, que cobran una nueva dimensión, en un nuevo escenario de búsqueda de equilibrio de intereses que pueden confrontar.

En concreto, de esa imparable irrupción de la digitalización dio cuenta en octubre de 2020 el Foro Económico Mundial, haciendo públicos los datos, verdaderamente esclarecedores, resultantes de la Encuesta sobre el Futuro del Trabajo. Así, ante el impacto de las nuevas tecnologías, las empresas encuestadas indican que buscan transformar la composición de su cadena de valor (55%), introducir una mayor automatización para reducir la fuerza laboral actual (43%) o expandirla como resultado de una integración tecnológica más profunda (34%), así como, en fin, ampliar el número de contratistas para trabajos especializados en determinadas tareas (41%)[1].

Pese a generar *a priori* cierta alarma por el ritmo al que desaparecerán algunos empleos, que se incrementa a causa de las escandalosas cifras de despido que recientemente han acometido las grandes empresas tecnológicas[2], se abren un sinfín de posibilidades que, a no dudar, estriban en el cambio de los modelos de negocio y de la forma de realizar tareas y trabajos[3] , hasta llegar a diluir, en ocasiones, las propias fronteras entre lo laboral y lo extralaboral, porque las tecnologías invaden todos los ámbitos de la vida. En esta línea, recientemente hemos podido comprobar que herramientas como Chat GPT –cuya cesación en el tratamiento de datos personales ha sido recientemente ordenada en Italia[4] - o Dall-E, de la compañía OpenAI, o el chat de Bing se han instalado con naturalidad en nuestro entorno, alterando de paso nuestro modo de relacionarnos con el empleo. Igualmente, una herramienta tan asentada como los sistemas biométricos, que muchas compañías han implantado tanto por razones de seguridad como de registro de la jornada de su personal, es ya el sistema preferido para controlar el acceso de personas a las dependencias de la empresa, por su capacidad de recopilación de datos e identificación y verificación de sujetos[5].

Aunque *grosso modo* hayamos destacado las bondades de estos medios, lo cierto es que también comportan una serie de desafíos, crecientemente complejos, que deben abordarse por los operadores jurídicos teniendo en cuenta, junto a su enorme utilidad, su efectivo funcionamiento y, de manera menos obvia, su alta potencialidad lesiva

1 FORO ECONÓMICO MUNDIAL, *The Future of Jobs Report 2020*, World Economic Forum.

2 CORRALES, R., "Ranking de despidos en las empresas tecnológicas (2022-2023)", *Business Insider España*, 21.01.2023.

3 Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones del Plan coordinado sobre la inteligencia artificial, [COM(2018)795 final], Bruselas, 07.12.2018, apartado 2.4.

4 Garante per la Protezione dei Dati Personali, *Provvedimento del 30 marzo 2023 [9870832]*, Garante Privacy, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9870832.

5 LARSON, T., "What is a Biometric Access Control System?", *Linkedin*, 12.04.2022.

de derechos e intereses[6]. Esta preocupación se refleja claramente en la Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital, de 23 de enero de 2023, que afirma que "[l]a transformación digital no debe implicar un retroceso en los derechos. Lo que es ilegal fuera de línea, es ilegal en línea"[7].

Son cambios recién llegados, pero que exigen una transición justa del sistema laboral a la economía y empleo digitales, apoyada en derechos laborales y un nivel de dignidad individual y socialmente aceptable. Ello exige neutralizar los riesgos sociales que implica la digitalización y sus inherentes disrupciones en el mercado laboral, como son la intensificación y aceleración de los ritmos de trabajo y subsiguiente aparición de riesgos psicosociales asociados a la dislocación del tiempo o lugar de trabajo, la afectación a la conciliación de vida laboral y personal, con crecientes requerimientos en términos de disponibilidad y flexibilidad, así como riesgos sobre la intimidad y privacidad que se ven agudizados por la existencia de recursos digitales asequibles y masivos al servicio del seguimiento y control del trabajo en las empresas.

El presente artículo trata estas poliédricas cuestiones desde una doble perspectiva, práctica y jurídica. Tras una primera aproximación a los conceptos de "algoritmo" e "inteligencia artificial" ("**IA**"), se abordará el cambio de paradigma en las potestades empresariales que está suponiendo la irrupción de estas nuevas herramientas. Cambio que se manifiesta con mayor intensidad en la sofisticación alcanzada por los sistemas digitales de control del trabajo en el contexto empresarial, en el que juegan un papel destacado los dispositivos biométricos, merecedores de un tratamiento singular que justifica su especial atención en lo que sigue, por su mayor capacidad intrusiva en los derechos de las personas trabajadoras. Se abordarán, igualmente, los riesgos y retos que la digitalización supone en el seno de las empresas en su condición de empleadoras, con especial mención a la salud y prevención de riesgos laborales capaz de verse afectados. Por último, se propondrá un mayor papel de la autonomía colectiva, para hacer a su vez un repaso de algunos convenios colectivos, sectoriales y de empresa, que recientemente han abordado el tratamiento de estas tecnologías y de los derechos digitales que pueden servir de referencia en el nuevo tablero.

II. Inteligencia artificial y algoritmos

Un algoritmo es un "conjunto ordenado y finito de operaciones o reglas que permite hallar la solución de un problema, que puede implementarse o no a través de programas informáticos"[8]. La doctrina caracteriza comúnmente los algoritmos como funciones matemáticas[9], que constan de tres partes: (i) la entrada de datos (*inputs*); (ii) el procesamiento de estos datos gracias a patrones de conducta que el sistema ha adquirido a partir del análisis de experiencias pasadas; y (iii) la salida u obtención de resultados (*outputs*). Por su parte, el Grupo Independiente de Expertos de Alto Nivel sobre Inteligencia Artificial define los sistemas de IA, cuya existencia y caracterización no se entiende sin la presencia de algoritmos, como aquellos programas o equipos informáticos "diseñados por seres humanos que,

6 MERINO SEGOVIA, A., "Tecnologías y tratamiento de datos en los procesos de selección y contratación laboral (1)", en Revista Trabajo y Derecho, núm. 87/2022, [LA LEY 1444/2022], pg. 2.

7 PARLAMENTO EUROPEO, CONSEJO y COMISIÓN EUROPEA, *Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital* (2023/C 23/01).

8 *Guía práctica y herramienta sobre la obligación empresarial de información sobre el uso de algoritmos en el ámbito laboral: Información algorítmica en el ámbito laboral* (2022), pg. 6.

9 MERCADER UGUINA, J.R., *Algoritmos e inteligencia artificial en el derecho digital del trabajo*, Tirant lo Blanch, Valencia, 2022, pg. 18; PAREJA FLORES, C. et al., *Algoritmos y Programación en Pascal*, Madrid, Openlibra, 2011, pgs. 6-7.

dado un objetivo complejo, actúan en la dimensión física o digital mediante la percepción de su entorno a través de la adquisición de datos, la interpretación de los datos estructurados o no estructurados, el razonamiento sobre el conocimiento o el tratamiento de la información fruto de estos datos y la decisión de las mejores acciones que se llevarán a cabo para alcanzar el objetivo fijado"[10].

Los datos son la materia prima que alimenta los sistemas de IA, tanto para su proceso de aprendizaje como para llevar a cabo su "razonamiento" de manera adecuada y obtener finalmente los *outputs* pretendidos. En este sentido, la cantidad y variedad de datos requerido por los sistemas de IA para arrojar resultados útiles en un muy reducido periodo de tiempo es ingente, lo que lleva a la doctrina a caracterizar estos sistemas, respecto de los datos, por la "triple V": volumen, variedad y velocidad[11], como demuestra, por ejemplo, el superordenador *MareNostrum* del Centro Nacional de Supercomputación, con una capacidad de 11,1 *petaflops* y capaz de realizar aproximadamente 11.100 billones de transacciones por segundo. De ahí que la IA sea posiblemente el aspecto más ambicioso de las nuevas formas de gestión del entorno de trabajo, los recursos materiales y la plantilla. Dado su potencial y la tendencia favorable a la implantación de sistemas *agile* de gestión en las empresas, hoy en día ni estamos en condiciones de renunciar a su uso[12], ni puede negarse su decisiva influencia sobre la relación de trabajo que, en una interesante paradoja respecto de la constante evolución de la nota de la dependencia característica de la relación laboral por cuenta ajena, representa un espaldarazo a la capacidad de control de la empresa en su vertiente de empleadora y fortalece la dependencia, permitiendo a las empresas desplegar sus poderes de organización, dirección y control de manera indirecta o implícita[13].

De hecho, los datos de la ya citada Encuesta del Foro Económico Mundial de 2020 no sorprenden: las empresas, especialmente las tecnológicas, aunque no solo estas, están rediseñando sus estructuras con ayuda de los sistemas de IA para integrar con mayor eficiencia la información obtenida, tanto de las opiniones de las personas trabajadoras como de las reacciones de la tecnología[14]. No obstante, deben extremarse las cautelas en su utilización en lo relativo a los riesgos que provoca sobre la persona. De acuerdo con el *Chartered Institute for Personnel Development*, tales riesgos pueden manifestarse en muy variadas dimensiones, como la gestión del talento, la salud y seguridad en el trabajo, la continuidad laboral e incluso la reputación de la propia empresa[15]. Valga recordar que *Tay, el chatbot* que la compañía Microsoft lanzó a Twitter el 23 de marzo de 2016 en fase experimental y sin ningún filtro sobre la información procesable, obligó a la empresa a cerrar la cuenta creada en menos de veinticuatro horas, debido a que *Tay* comenzó a proferir comentarios racistas y loas al nazismo[16]. No extrañará, pues, que el suministro de datos sometido a la regla de la "triple V", con límites pendientes de definición, preocupe tanto a los desarrolladores de los sistemas de IA como a sus operadores, al menos desde dos perspectivas:

(i) Desde el punto de vista formal, el enorme volumen de datos, mayoritariamente personales en la relación empresa-persona trabajadora, exige ser especialmente cauteloso en su obtención y tratamiento, lo que impone observar las

10 COMISIÓN EUROPEA, Libro Blanco sobre Inteligencia Artificial. Un enfoque europeo de la excelencia y la confianza [COM(2020) 65 final], Bruselas, 19.02.2020.

11 Como señala MERCADER UGUINA, J.R., *Algoritmos e inteligencia artificial en el derecho digital del trabajo*, cit., pg. 22.

12 BELTRÁN DE HEREDIA RUÍZ, I., "Algoritmos, psicometría y derechos del yo inconsciente de la persona (o «neuroderechos») en el ámbito socio-laboral", en la *ponencia Presentada al Congreso «La tecnología y la digitalización en las relaciones laborales: personas y competitividad»*, Valencia 17 y 18 de noviembre 2022.

13 PÉREZ DEL PRADO, D., "Los tradicionales conceptos de trabajador y empresario en un mundo digital", en MERCADER UGUINA, J.R., DE LA PUEBLA PINILLA, A., GIMENO DÍAZ DE ATAURI, P. y GORDO GONZÁLEZ, L. (Coords.), *Cambio tecnológico y transformación de las fuentes laborales. Ley y convenio colectivo ante la disrupción digital,* por. Valencia, Tirant lo Blanch, 2023, pgs. 100-101.

14 BETTERWORKS, "How AI is Transforming HR: The Future of People Analytics", 19.10.2021.

15 HOUGHTON, E. y GREEN, M., *People Analytics: Driving Business Performance with People Data*, Chartered Institute for Personnel Development, 2018.

16 JUÁREZ, D., "La inteligencia artificial de Microsoft se vuelve nazi y racista en un día", en *La Vanguardia*, 25.03.2016.

normas existentes en materia de protección de datos en la Unión Europea, el Reglamento (UE) 2016/679 General de Protección de Datos ("**RGPD**") y, en España, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales ("**LOPDGDD**"). En este sentido, el principal problema, como se verá repetidamente en este artículo, es que la normativa actual carece de límites claros, sin perjuicio de las alusiones a los deberes genéricos de "preservar la dignidad humana de los interesados, así como sus intereses legítimos y sus derechos fundamentales" (artículo 88.2 RGPD).

(ii) Desde el punto de vista material, es evidente que, en presencia de modelos precisos, pero también rígidos y limitados[17] su "razonamiento" es por definición formalmente válido cuando las condiciones en que el sistema ha sido instruido se replican en situaciones concretas, el riesgo de que el *output* sea inútil es elevado, mostrando estos programas una enorme vulnerabilidad a la confusión "por ruido"[18]; con el añadido peligro subyacente de que el sistema procese datos en sí mismos discriminatorios o sesgados[19], voluntaria y/o involuntariamente, provocando que los resultados también lo sean, en un efecto que la doctrina coincide en llamar "discriminación algorítmica"[20]. Este riesgo se intensifica cuando dos o más causas de discriminación prohibidas interactúan, creando una situación de discriminación por interseccionalidad[21]. En este sentido, el Parlamento Europeo advierte uno de los mayores riesgos del uso de la IA en su impacto sobre los derechos fundamentales a la intimidad, protección de datos y no discriminación[22], no siempre fácilmente identificable y conducente a una casi inevitable casuística.

A nuestro juicio, este problema se agrava por la opacidad que caracteriza estos sistemas de IA, llevando a su oportuna calificación por parte de algunos autores como "caja negra"[23], en la medida en que es muy difícil traducir al lenguaje humano, incluso reconocer, el criterio que conduce a la máquina al resultado finalmente elegido. Precisamente, fruto de tales riesgos, la UE se ha mostrado tajante en lo concerniente a la toma de decisiones íntegramente automatizadas cuando estas puedan producir efectos jurídicos en la persona o "le afecte significativamente de modo similar" (artículo 22 RGPD), otorgando al interesado un mayor poder de decisión sobre el tratamiento de sus datos. Con ello, *a priori*, se corrigen en el territorio de los Estados Miembros posibles actuaciones como las de las tecnológicas estadounidenses, que monitorizan la productividad de las personas trabajadoras, midiendo el número de tareas acometidas y la velocidad con que se realizan, generando avisos automáticos incluso de despido a quienes no alcanzan la mínima productividad exigida[24]. Ahora bien, al margen de las dudas interpretativas que la referencia a que la decisión automatizada "afecte significativamente de modo similar" (artículo 22 RGPD)[25], hay que considerar que estas cautelas tienen excepciones, muy relevantes desde el punto de vista del Derecho del Trabajo, cuando la decisión automatizada: (i) sea necesaria para la ejecución de un contrato; (ii) esté autorizada conforme a la normativa de la UE o de un Estado Miembro; o (iii) se haya dado el consentimiento explícito de la persona afectada.

17 PAREJA FLORES, C. et al., *Algoritmos y Programación en Pascal*, cit., pg. 16.

18 PARRA, V.D., "*Inteligencia Artificial para la toma de decisiones*", en My Tips, 24.03.2020.

19 DU SAUTOY, M., *Programados para crear*, Barcelona, Acantilado, 2020, pg. 119.

20 ZUIDERVEEN BORGESIUS, F., *Discrimination, artificial intelligence, and algorithmic decision-making*, Estrasburgo, Consejo de Europa, 2018.

21 GINÈS i FABRELLAS, A., "La gestión algorítmica del trabajo: nuevos retos jurídicos, tecnológicos y éticos", en *Digitalización, recuperación y reformas laborales, XXXII Congreso Anual de la Asociación Española de Derecho del Trabajo y de la Seguridad Social*. Madrid (MITES),2022, pg. 307.

22 Resolución del Parlamento Europeo de 14 de marzo de 2017 sobre las implicaciones de los macrodatos en los Derechos fundamentales: privacidad, protección de datos, no discriminación, Seguridad y aplicación de la ley [2016/2225(INI)].

23 PASQUALE, F.A., The Black Box Society: *The Secret Algorithms That Control Money and Information*, Cambridge, Harvard University Press, 2015; MERCADER UGUINA, J.R., Algoritmos e inteligencia artificial en el derecho digital del trabajo, cit., pg. 20; BELTRÁN DE HEREDIA RUÍZ, I., "Algoritmos, psicometría y derechos del yo inconsciente de la persona (o «neuroderechos») en el ámbito socio-laboral", cit., pg. 10.

24 LECHER, C., "How Amazon automatically tracks and fires warehouse workers for `productivity´", *The Verge*, 25.04.2019.

No obstante lo anterior, lo cierto es que aplicar las disposiciones generales del RGPD y la LOPDGDD de manera indiferenciada en el tratamiento por parte de la empresa de datos personales de las personas trabajadoras arroja resultados insuficientes e incoherentes[26]. Como se abordará con más detalle a continuación, las reglas que la empresa debe observar al respecto se circunscriben a respetar el principio de obligación legal en el tratamiento y de exactitud de los datos, así como los deberes de confidencialidad y transparencia e información a la persona trabajadora afectada[27], mientras que esta última prácticamente se limita a prestar su consentimiento informado para que sus datos personales, sin identificarse legalmente cuáles necesita conocer y tratar la empresa[28], se empleen con fines relacionados con el mantenimiento, desarrollo y control de la relación contractual[29].

En definitiva, la falta de una regulación específica en el ámbito laboral evidencia la necesidad de una adaptación de la normativa que, por el momento, trata de suplirse con interpretaciones jurisprudenciales, administrativas y convencionales, incapaces, con todo, de eludir la urgencia de un tratamiento integral de la digitalización y la protección de datos en el entorno laboral dentro de su normativa natural, esto es, el Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores ("**ET**") y normas concordantes, más apta para contemplar garantías suficientes y adecuadas para la interdicción de una desproporcionada intromisión en la privacidad y derechos fundamentales de las personas trabajadoras[30].

III. Poder de dirección y vigilancia en la empresa

Sin perjuicio de las normas contenidas en la LOPDGDD sobre la protección de datos personales, cuya gestión debe preservar los derechos de las personas, lo cierto es que el tratamiento de los de la persona trabajadora por su empresa carece de regulación específica, en una omisión del entorno laboral más destacable por dos razones. De una parte, porque las garantías generales aplicables a cualquier persona, con independencia de su cualidad de trabajadora, obvian las particulares exigencias de su posición de debilidad negociadora respecto de la empresa, así como el entorno colectivo de la relación de trabajo que equilibra aquella, relegando relevantes derechos de participación y control de las instancias representativas de los trabajadores en este contexto, más allá de la genérica llamada a la negociación colectiva contenida en el artículo 91 LOPDGDD, que rellena ese hueco indirectamente y allí donde se prevea la actual redacción del artículo 64.4.1.d) ET viene a salvar este clamoroso silencio extendiendo el derecho colectivo de información a los parámetros, reglas e instrucciones en que se basan los algoritmos o sistemas de IA que afectan a la toma de decisiones relativas a las condiciones de trabajo, acceso y mantenimiento del empleo, incluida la elaboración de perfiles. De otra, porque la propia LOPDGDD no ignora la especial incidencia de esta materia en el ámbito empresarial, con preceptos específicos en el entorno laboral que hubieran debido completarse con esta otra ordenación, desdibujándose la necesidad de garantías especiales de la obtención y tratamiento empresarial de datos personales

25 De manera muy sucinta, esta última expresión del artículo 22.1 RGPD ha sido estudiada por el Grupo de Trabajo del Artículo 29 (actual Comité Europeo de Protección de Datos) en su informe *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*. En este sentido, una decisión tiene efectos jurídicos cuando afecta a la situación legal de una persona o a sus derechos *v.gr.* cancelación de un contrato o denegación de una prestación social (pg. 23) y tiene efectos significantes cuando dicha decisión: (i) impacta en las circunstancias, comportamiento u opciones de las personas; (ii) puede tener un efecto permanente o prolongado; y/o (iii) causa la exclusión o discriminación de dicha persona (pg. 24).

26 VALDEOLIVAS GARCÍA, Y., "Derechos de información, transparencia y digitalización", en AEDTSS, *Digitalización, recuperación y reformas laborales, XXXII Congreso Anual de la Asociación Española de Derecho del Trabajo y de la Seguridad Social*, cit., pg. 200.

27 Cfr. los artículos 4, 5, 8 y 11 LOPDGDD, respectivamente.

28 Ante este vacío, sirve como referencia a efectos informativos la Guía para la protección de datos en las relaciones laborales, de la Agencia Española de Protección de Datos ("**AEPD**"), publicada en mayo de 2021.

29 Cfr. los artículos 6.1 b) RGPD y 6 LOPDGDD.

30 VALDEOLIVAS GARCÍA, Y., op. ult. cit., pgs. 197 y ss.

del trabajador, poniéndose el acento, por contraste, en el mero uso de los dispositivos digitales en el medio laboral, ya como herramientas para el desempeño de las tareas profesionales, ya para la vigilancia de su adecuada ejecución.

Singularidades de la gestión empresarial de los datos personales de las personas trabajadoras justificadas por permitir a la empresa conocer y procesar gran cantidad de información que, con ocasión del vínculo laboral, es capaz de desbordar tal funcionalidad hasta penetrar en al ámbito de la privacidad e intimidad de la persona trabajadora de forma mucho más aflictiva que la deducible de cualquier otro responsable o gestor de datos, fruto de la posición de dominio. Dicho sujeto posee, junto a facultades directivas de la relación laboral, capacidad sancionadora en la ejecución de la prestación, participadas por las instancias colectivas, sin atisbarse en la normativa aplicable una regulación concreta tendente a reforzar los derechos fundamentales de las personas trabajadoras, cuya garantía debe ser efectiva en todas las fases de la relación laboral[31].

La tensión de intereses y derechos subyacentes reside en que a los datos personales recabados con finalidades en apariencia estrictamente profesionales se asocian otros, como consecuencia de su análisis masivo, también determinantes de efectos laborales, sin descartarse la falta de neutralidad y objetividad del resultado, ni la existencia de discriminación directa o indirecta, ni la eventual lesión de la intimidad y privacidad[32], faltando controles y cautelas que aseguren una recepción y uso transparentes y proporcionados. La utilización de la IA y de los algoritmos en la toma de decisiones empresariales no excluye, así, la ausencia de intromisiones en la vida privada con consecuencias profesionales, haciendo imprescindibles las garantías tanto en la fase de obtención de datos, frente a intrusiones ilegítimas o desproporcionadas en la información recabada, como en la de utilización de la información seleccionada.

Por lo que afecta a la empresa, las reglas se concretan, básicamente, en el principio de exactitud de los datos y los deberes de confidencialidad, transparencia e información al trabajador afectado (artículos 4, 5 y 11 LOPDGDD, respectivamente). Del lado de la persona trabajadora, quedan reducidas principalmente a su consentimiento informado (artículos 6 y 11 LOPDGDD), en unos términos genéricos que admiten, además, relevantes excepciones[33], pues la regla para el tratamiento de los datos de las personas trabajadoras es la relación contractual, siendo el consentimiento una excepción en caso de que deba realizarse un tratamiento específico. Así, conforme a la legislación, el tratamiento de datos

31 Al margen del despido, la adopción empresarial de medidas organizativas, en especial las de carácter colectivo, presumen el manejo de datos personales de los trabajadores que son premisa de los criterios de identificación de los afectados -nombre y apellidos, edad, antigüedad, puesto, salario, rendimiento y otros-, con conocimiento, además, de la representación legal de los trabajadores en fase de consultas, lo que implica, a efectos de oposición de la persona trabajadora, informar también a esta sobre tales criterios y su baremo. Porque si este tratamiento refleja las características del individuo, valorando su rendimiento laboral, conducta, posibilidad de confianza en sus actuaciones y otros aspectos, debe existir derecho a impugnar dichas resoluciones y a ser informado sobre los criterios de evaluación y programa utilizado en el tratamiento que sirvió para adoptar la decisión sobre apreciaciones de conducta [cfr. la Resolución AEPD R/01656/2013].

32 Sobre estos efectos, más ampliamente, TODOLÍ SIGNES, A. "La gobernanza colectiva de la protección de datos en las relaciones laborales: big data, creación de perfiles, decisiones empresariales automatizadas y los derechos colectivos", Revista de Derecho Social, 2018, núm. 84, pgs. 5 y ss., para quien, cuando el algoritmo manda, las minorías están en desventaja, reproduciendo sesgos sociales de género y otros; también, VALDEOLIVAS GARCÍA, Y., op. cit., pg.198.

33 Exactitud y confidencialidad de los datos personales y condiciones del consentimiento que, a modo de principios, preceden en la LOPDGDD a los derechos de transparencia e información, acceso, rectificación, supresión, limitación y oposición del tratamiento, así como de portabilidad de los datos, a los que se suman luego tratamientos concretos diversos y heterogéneos por razón de la finalidad de su manejo, con especial interés en lo relativo al sistema de denuncias internas de especial incidencia en el ámbito laboral, en tanto presupuesto de medidas disciplinarias en la empresa. Más ampliamente sobre aquellos derechos en general, PRECIADO DOMÈNECH, C.H., *Los derechos digitales de las personas trabajadoras. Aspectos laborales de la LO 3/2018, de 5 de diciembre de Protección de Datos y Garantía de los Derechos Digitales*. Pamplona (Aranzadi), 2019, pgs. 27 y ss.; MOLINA NAVARRETE, C., *Datos digitales de las personas trabajadoras en tiempos de (pos)covid19: Entre eficiencia de gestión y garantías*. Albacete (Bomarzo), 2021, pgs. 83 y ss.; TODOLÍ, A. "The evaluation of workers by customers as a method of control and monitoring in firms: Digital reputation and the European Union's General Data Protection Regulation", *International Labour Review*, 2021, Vol. 160, núm. 1, pgs. 77 y ss. También, AEPD, *La protección de datos en las relaciones laborales*, 2021.

prescinde del consentimiento si es necesario para la ejecución de un contrato en el que el interesado es parte o para aplicar a petición de este medidas precontractuales, que cabe supeditar, leída la norma a contrario, a que la persona afectada consienta el tratamiento para finalidades relacionadas con el mantenimiento, desarrollo y control de la relación contractual (artículos 6.1.b) RGPD y 6.3 LOPDGDD, respectivamente), sin perjuicio de la transparencia de tales datos y el derecho de la persona trabajadora a ser informada, sin excepciones ahora a tenor del citado artículo 11 LOPDGDD, que incluye su accesibilidad e inteligibilidad, así como el derecho al olvido y portabilidad, que incrementan su capacidad decisoria[34]. Resulta esencial, pues, establecer parámetros de identificación de los datos personales que son necesarios y adecuados para el conocimiento y análisis empresarial, por servir para mantener, desarrollar o controlar la relación laboral, incluso al margen del consentimiento de la persona trabajadora. Con todo, recuérdese que el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos reservados, aquellos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico, salvo que sea necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento en el ámbito del derecho laboral (artículo 9.1 LOPDGDD); lo que parece tener nula cabida en el mismo, pues su conocimiento empresarial, lejos de responder a informaciones necesarias para el ejercicio de las facultades directivas y sancionadoras, solo serviría como fuente de discriminación[35].

Parece defendible entonces una interpretación restrictiva del poder empresarial, atemperada por principios como los de necesidad, idoneidad y proporcionalidad, pautas interpretativas imprescindibles que, ausentes en buena medida de nuestra normativa interna[36], llaman a su mejor determinación vía negociación colectiva.

34 Artículos 17 y 20 RGPD, que la LOPDGDD parece limitar exclusivamente a los datos recogidos en búsquedas de internet, redes sociales y servicios equivalentes (artículos 93 a 95).

35 Salvo el caso excepcional de empresas de tendencia, como advierte CRUZ VILLALÓN, J., *Protección de datos personales del trabajador en el proceso de contratación: facultades y límites de la actuación del empleador*, Albacete (Bomarzo), 2019, pgs. 33-35.

36 No así el RGPD, cuyo Considerando 4, tras señalar que el derecho a la protección de los datos personales no es un derecho absoluto, por su función social obliga a considerarlo en equilibrio con otros derechos fundamentales, conforme al principio de proporcionalidad. Importante doctrina constitucional que cabe extender a esta sede, que ya ha aplicado este principio en relación con los poderes empresariales, entendiendo que las limitaciones a los derechos de las personas trabajadoras deben satisfacer una acreditada necesidad o interés legítimo de la empleadora y ser lo menos invasivas posible, priorizando el uso menos aflictivo para aquellos derechos -entre otras, las Sentencias del Tribunal Constitucional ("**TC**") 98, 186 y 292/2000, 196/2004, 29 y 170/2013, 39/2016 y 160/2021; igualmente, las SSTS 21 sep. 2016, (4353/2015) y 8 feb. 2021 (84/2019).

37 No obstante, la negociación colectiva es poco activa en la previsión de garantías adicionales, con casi total ausencia de referencias al tratamiento de datos. Así, SERRANO GARCÍA, J.Mª., La protección de datos y la regulación de las tecnologías en la negociación colectiva y en la jurisprudencia. Albacete (Bomarzo), 2019, pgs. 20 y ss.; SIERRA HERNÁIZ, E., "El papel de la negociación colectiva en el tratamiento de los datos personales de los trabajadores", Temas Laborales, 2020, núm. 152, pg. 120 y ALMENDROS GONZÁLEZ, M.A., "Nuevas tecnologías y derechos digitales en la negociación colectiva (I)", Trabajo y Derecho, 2021, núm. 83, pgs. 7 y 23. Y ello pese a las recomendaciones para impulsar el empleo de calidad y con derechos que el III AENC propone a los convenios colectivos, uno de cuyos objetivos fundamentales es la incidencia de las TIC en el desarrollo productivo general y en las relaciones laborales, y cuyo Cap. II compromete el establecimiento de canales de comunicación entre las partes como vehículo de información entre trabajadores y sus representantes. En este sentido, UGT elaboró un Protocolo de actuación para la Negociación Colectiva. Protección de datos personales y garantía de los derechos laborales (2019) que encomienda a la autonomía colectiva en todos los ámbitos la protección del derecho, el derecho de información y consulta y ampliar los márgenes del art. 64 ET (pg. 15). En parecidos términos, CC.OO., en su Guía de Negociación Colectiva y Digitalización 2020, destaca el papel a desarrollar por la negociación colectiva a fin de regular la digitalización en el ámbito laboral, a la que se proporcionan criterios de actuación, considerando que su impacto no es homogéneo y afecta de distinta forma y con distinta intensidad a los diferentes sectores productivos y de servicios (pgs. 5, 7 y 9). Finalmente, el propio Acuerdo Marco Europeo sobre Digitalización recuerda también en diversos apartados que el convenio colectivo es la norma más específica para la protección de los derechos y la libertad en relación con el tratamiento de los datos personales de los empleados en la relación laboral (vid. sobre el mismo, GOERLICH, J.Mª., "El Acuerdo Marco Europeo sobre Digitalización, Documentación Laboral, 2021, núm. 122, pgs. 49-57; SEPÚLVEDA GÓMEZ, M., "El Acuerdo Marco Europeo sobre Digitalización. El necesario protagonismo de la norma pactada", Temas Laborales, 2021, núm. 158, pgs. 213-244.

Es este, sin duda, un ámbito regulador propicio para prever qué datos pueden ser tratados en la empresa[37], bajo la premisa de su carácter imprescindible para la toma de decisiones en ella, asegurando una ponderación de intereses que la ley no expresa, preconfigurada esa visión general de presunción de legitimidad del tratamiento empresarial de datos personales ajustada a las genéricas reglas señaladas.

Establecido el genérico contexto digital de entorno, procede afirmar en este punto que el avance que mayor impacto ha tenido en el ámbito laboral es el fenómeno de las plataformas[38], tanto por ser pionero como por su radical transformación de las condiciones de trabajo. Tras la irrupción del fenómeno y su tratamiento en la célebre Sentencia del Tribunal Supremo ("**STS**"), que declaró la laboralidad de los trabajadores de Glovo[39], se hace evidente una idea fuerza: "en la sociedad postindustrial la nota de dependencia se ha flexibilizado. Las innovaciones tecnológicas han propiciado la instauración de sistemas de control digitalizados de la prestación de servicios"[40]. Sea como fuere, lo cierto es que España ha sido uno de los primeros países europeos en dar respuesta judicial al máximo nivel al fenómeno del trabajo en plataformas[41], lo que se reproduce a nivel legal y convencional[42]. La anticipada Ley 12/2021, prevista para los casos en los que el poder de dirección se ejerce mediante una plataforma o un sistema de IA, permite determinar con mayor precisión si existe una relación laboral. Es decir, aunque pueda parecer que la norma dibuja *a priori* un supuesto de aplicación amplio e indeterminado, aumenta las posibilidades de aplicación del Derecho del Trabajo y, con ella, la extensión de su tutela, precisamente por el hecho de utilizarse la plataforma para la gestión empresarial[43].

Situación que no siempre ha resultado tan clara desde el punto de vista legal. Huelga decir que hasta la STS referida abundaban las zonas grises en lo concerniente a la situación de los *riders*. Así, las plataformas alteraron los contornos tradicionales de ajenidad y dependencia, entendido este último concepto como el conjunto del poder de dirección, que acoge no solo el sometimiento a la esfera rectora de la empresa, sino, a su vez, la facultad de control, *ius variandi* y organización y dirección del trabajo[44]. No obstante, tras aquella resolución, hay una única cuestión esencial: determinar si la persona trabajadora está subordinada a la facultad de la empresa de organizar el trabajo. En este sentido, el TS entiende que "[l]a dependencia es la `situación del trabajador sujeto, aun en forma flexible y no rígida, a la esfera organicista y rectora de la empresa´ (…). Es decir, la dependencia o subordinación se manifiesta mediante la integración de los trabajadores en la organización empresarial"[45].

38 PÉREZ DEL PRADO, D., "Los tradicionales conceptos de trabajador y empresario en un mundo digital", cit, pg. 96.

39 STS núm. 805/2020, de 25 de septiembre de 2020, rec. 4746/2019, ECLI:ES:TS:2020:2924.

40 *Ibidem*, Fundamento Jurídico Séptimo.

41 ADAMS-PRASSL, J, LAULOM, S., y MANEIRO VÁZQUEZ, Y., "El papel de los tribunales nacionales en la protección de los trabajadores de plataformas", en MIRANDA BOTO, J.M. y BRAMESHUBER, E. (eds.), *Negociación colectiva y Economía de Plataformas*, Madrid (Cinca), 2022, pgs. 97-121.

42 A nivel normativo, cfr. la Ley 12/2021 de 28 de septiembre (BOE, 29), por la que se modifica el Estatuto de los Trabajadores aprobado por el Real Decreto Legislativo 2/2015, de 23 de octubre, para garantizar los derechos laborales de las personas dedicadas al reparto en el ámbito de plataformas digitales. En la negociación colectiva, vid., por ejemplo. la Resolución TSF/510/2018, de 23 de febrero (DOGC, 5 enero 2023), por la que se dispone la inscripción y la publicación del Convenio colectivo interprovincial del sector de la industria de hostelería y turismo de Cataluña.

43 PÉREZ DEL PRADO, D., "El Juego de los Futuribles: hipótesis para una hipotética transposición de la Directiva de trabajo en plataformas", *El Foro de Labos,* 19.05.2022.

44 MONTOYA MELGAR, A., "Libertad de empresa y poder de dirección del empresario en las relaciones laborales", en: SÁNCHEZ TRIGUEROS, C. y GONZÁLEZ DÍAZ, F. A. (eds.), Libertad de empresa y poder de dirección del empresario en las relaciones laborales: estudios ofrecidos al profesor Alfredo Montoya Melgar, Cizur Menor, Navarra: Aranzadi, Thomson Reuters, 2011., pgs. 35-48.

45 STS de 25 de septiembre de 2020, Fundamento Jurídico Décimo, citando, por todas, las SSTS 8 febrero 2018, rec. 3389/2015; 1 julio 2020, rec. 3585/2018; y 2 julio 2020, rec. 5121/2018.

Es más, el propio concepto de "empresa" o "empresario" se ve desbordado por las nuevas formas de digitalización del trabajo, al punto de alterar su morfología[46]. Si hasta la irrupción de estos sistemas y de las propias plataformas la empresa se concebía como un puesto de trabajo en un lugar concreto, en el que "el jefe" supervisaba el trabajo *in situ,* los sistemas de IA precisamente han demostrado que el control empresarial de la actividad laboral puede intensificarse sin recurrir en modo alguno a la presencialidad, la medición del rendimiento o del comportamiento de la plantilla[47]. No obstante, estas nuevas formas de organización de las empresas no deben inducir a error: no es que "el jefe" sea un algoritmo, sino que se encuentra oculto tras él[48]. Esto es, las plataformas, y cualquier empresa que emplee globalmente sistemas de IA, cumplen las funciones propias de cualquier empleador, no pudiendo considerarse un empresario nuevo, sino más bien una nueva forma de organización empresarial que reproduce los caracteres más propios de la figura del empleador[49].

Sentado lo anterior, cabe afirmar que el uso de algoritmos y de sistemas de IA está produciendo un incremento incomparable de las capacidades empresariales de vigilancia y control[50], hasta el punto de que ahora puede conocerse información ignorada hasta el momento. Algunos autores afirman, con razón, que estos medios suponen una "verdadera ventana indiscreta para la empresa"[51], con la consiguiente amenaza a los derechos a la privacidad y protección de datos que ello conlleva.

1. Uso de dispositivos digitales y desconexión, grabación de imágenes y sonido y geolocalización

El artículo 87 LOPDGDD comienza reconociendo el derecho de las personas trabajadoras a la protección de su intimidad en el uso de los dispositivos digitales dispuestos por la empleadora para la actividad laboral, para validar de inmediato el acceso empresarial a los contenidos derivados de su uso para controlar el cumplimiento de las obligaciones laborales o la integridad de dichos equipos, regulando la obligación empresarial de establecer criterios de utilización de esos medios, participados por la representación de los trabajadores cuando sea preciso. En este sentido, el precepto presume legítimo el conocimiento empresarial de datos privados del trabajador derivados de la trazabilidad del uso de tales equipos, otorgándole un espacio de intromisión comúnmente amparada en el propósito de control y vigilancia (artículo 20.3 ET). La amplitud finalista del acceso empresarial llega hasta casi descausalizarse por la ausencia de pautas y controles, incluidos los colectivos, solo previstos expresamente para determinar los criterios de utilización de los dispositivos, no para la extracción de la información contenida en ellos; de otro, la sola referencia a los usos sociales y derechos constitucionales y legales dificulta extraer parámetros seguros de carácter previo, prevaleciendo la adaptación de la interpretación jurídica a la volatilidad de "lo íntimo" fruto de los cambios digitales, más que a un espacio de intangibilidad anticipada de los derechos constitucionales y legales que, sin duda, están implícitamente incorporados[52].

46 PÉREZ DEL PRADO, D., "Los tradicionales conceptos de trabajador y empresario en un mundo digital", cit., pg. 110.

47 PRASSL, J., *Humans as a service: the promise and perils of work in the gig economy* Oxford, United Kingdom; New York, NY: Oxford University Press. 2018, pgs. 56-61. También, VALDEOLIVAS GARCÍA, Y., "Derechos de información, transparencia y digitalización", cit., pg. 195.

48 MERCADER UGUINA, J. R., "La gestión laboral a través de algoritmos", en AEDTSS, *Digitalización, recuperación y reformas laborales: XXXII Congreso anual de la Asociación Española de Derecho del Trabajo y de la Seguridad Social*, cit., pg. 270.

49 Vid. PÉREZ DEL PRADO, D., "Los tradicionales conceptos de trabajador y empresario en un mundo digital", cit., pgs. 108-109. Estas funciones serían, *grosso modo*: (i) los poderes contractuales, desde su celebración hasta terminación; (ii) el derecho a percibir los frutos del trabajo; (iii) el deber de abonar el salario pactado; (iv) el deber de realizar las actividades necesarias de gestión interna de la empresa; y (v) la gestión externa de la compañía.

50 DE STEFANO, V., "Algorithmic Bosses and How to Tame Them", *C4E The Future of Work in the Age of Automation and AI*, 2020, pg. 14.

51 GINÈS i FABRELLAS, A., *"La gestión algorítmica del trabajo: nuevos retos jurídicos, tecnológicos y éticos", en Digitalización, recuperación y reformas laborales, XXXII Congreso Anual de la Asociación Española de Derecho del Trabajo y de la Seguridad Social*, cit., pg. 302.

La vaguedad normativa y una jurisprudencia permisiva sobre el control del correo electrónico por la empresa promueven al Convenio colectivo como el medio adecuado para especificar reglas y garantías añadidas que, sobre establecer mayores facultades de participación de las instancias representativas, identifique mejor el objeto y causa del posible acceso empresarial, asegurando los principios de necesidad, idoneidad y proporcionalidad, separando netamente la ponderada potestad empresarial de extraer información del uso laboral del dispositivo de su rigurosa exclusión si afecta a datos almacenados en el ámbito de utilización privada.

En todo caso, el principal problema de colisión entre la facultad empresarial de acceso a la información contenida en los medios digitales facilitados y el derecho a la intimidad de la persona trabajadora se plantea en relación con los eventuales usos privados, cuya atribución y condiciones de ejercicio el artículo 87 LOPDGDD confiere a la empresa. Frontera difusa en la práctica, porque las finalidades privadas y profesionales con frecuencia convergen en un único equipo indistintamente utilizado para ambas, haciendo más asequible el conocimiento, con presuntas finalidades laborales, de datos privados sobre los que no opera el consentimiento del afectado, implícito en la relación de trabajo con el mero reconocimiento a la empresa de poderes directivos y sancionadores. De ahí las reforzadas garantías del artículo 87 LOPDGDD sobre la determinación clara y precisa de los usos y períodos temporales autorizados, participados por las instancias colectivas, así como el deber de información individual sobre dicho régimen de uso privado. Lo que conduce a los principios de minimización, proporcionalidad y restantes referidos que calificarían como restrictivamente selectivo y causal el conocimiento empresarial y su uso para tomar decisiones contractuales.

Sobre esta cuestión sobrevuela también la desconexión digital que el artículo 88 LOPDGDD reconoce como derecho individual de la persona trabajadora y que reitera el artículo 20 bis ET. El derecho redunda en la protección clásica de la persona trabajadora al respeto de su jornada y descansos, con idéntica finalidad de garantizar una neta separación entre vida profesional y privada, añadiendo realmente poco a la regulación estatutaria sobre tiempo de trabajo que incorpora esos límites, aunque los dispositivos digitales que acompañan a la persona trabajadora en todo momento, dentro y fuera de la empresa y susceptibles de monitorización y conectividad constantes, pueden conducir a interpretar que se sigue bajo la órbita del poder de control empresarial. Eso explica el reconocimiento del derecho a la desconexión digital como un derecho individual y básico, que cobra especial relevancia en el trabajo a distancia con medios telemáticos. La plurilesividad potencial de la conectividad constante de la persona trabajadora exige un tratamiento que, sobre generar derechos de información más rigurosos elaborar una política interna dirigida hacia ellos, introduce mayores poderes colectivos, con intervención de la negociación colectiva o, en su defecto, acuerdo de empresa, ampliando el contenido de los derechos de información y consulta por la especial sensibilidad de los derechos laborales implicados. Derechos que, ya integrados en las normas reguladoras del tiempo de trabajo, enfatizan aquí la perspectiva de género y la corresponsabilidad[53].

52 Como señaló claramente la Sentencia del Tribunal Europeo de Derechos Humanos ("**STEDH**") 5 sep. 2017 (caso Barbulescu v. Rumanía), mucho más precisa en el test de garantía de la intimidad y derechos fundamentales que nuestra doctrina constitucional contenida en las SSTC 173/2011, 241/2012 y 170/2013, porque la flexibilidad otorgada en estas últimas a los intereses empresariales se endurece en aquella, incrementando la garantía de privacidad que exige un motivo justificativo de la decisión empresarial, el juicio de proporcionalidad y la acreditación de que la medida de control y vigilancia es previa al inicio del eventual procedimiento disciplinario.

53 Así, PRECIADO, C.H., *Los derechos digitales de las personas trabajadoras…*, cit., pgs. 150-151.

En cuanto a la grabación de imágenes y sonidos, cabe extender ahora parecidas garantías a las recién analizadas, con algún obvio matiz de refuerzo de la intimidad y la propia imagen de las personas trabajadoras que aquí se involucran, a la legítima capacidad de la empresa de grabar y tratar imágenes y sonidos en el trabajo para el ejercicio de su función de control de la actividad laboral. Y ello a pesar de que el artículo 89 LOPDGDD al que se remite el artículo 22 de la misma norma en cuanto a videovigilancia, tras confirmar el carácter especial del entorno laboral, obvia toda mención a la intimidad y propia imagen de la persona trabajadora, limitándose a prever que el ejercicio del poder empresarial se desenvuelva "dentro de su marco legal y con los límites inherentes al mismo", lo que el artículo 20 bis ET extiende a la aplicación judicial y constitucional de los derechos fundamentales en el ámbito laboral, que asegura su contenido esencial[54]. Principios de necesidad, idoneidad y proporcionalidad, unidos a confidencialidad y minimización de datos, entre otros, parecen imponerse también ahora como garantías imprescindibles, porque la persona trabajadora sometida a estos sistemas se vuelve transparente y permanentemente visible y audible para su empresa. Así, la grabación de imágenes y sonido, más estricto este segundo, debe responder a un criterio finalista conforme a las reglas citadas, no quedando al albur de la discrecionalidad empresarial; y el eventual tratamiento debe cohonestarse con la protección de datos personales conforme a los límites antevistos. Ello resulta coherente con la expresión legal sobre el regular ejercicio del derecho, que presupone la existencia de razones organizativas y necesidades empresariales justificativas de semejante afectación a lo que, en expresión judicial, significa una razonable expectativa de privacidad en el ámbito laboral[55].

En este contexto general, las reglas legales inciden en el derecho de información previa, expresa y clara a las personas trabajadoras, que afecta no solo a la existencia de los dispositivos, sino a su finalidad de control y posible utilización para la imposición de sanciones. A esa información individual, la norma suma la de carácter colectivo, que debiera aplicarse en todo caso como garantía de equilibrio entre los intereses de trabajadores y empleadores, y defendible, primero, a tenor del artículo 64.1 ET y, en especial, su apartado 4.4.d) si las imágenes van a tratarse con algoritmos o IA[56]. Aunque recuérdese que el deber se entiende cumplido por la norma, en caso de captarse la comisión flagrante de un acto ilícito, con un dispositivo informativo en lugar suficientemente visible e identificativo de la existencia del tratamiento, identidad del responsable y posible ejercicio de los derechos de acceso y rectificación, cumplidos mediante un código de conexión o dirección de internet (artículo 22.4 LOPDGDD). Información en exceso genérica que, validada judicialmente, no parece cumplir las exigencias mínimas de respeto a la intimidad y propia imagen, como entendió la más garantista doctrina inicial del TEDH, luego corregida[57], planteando dudas sobre lo que sea acto ilícito suficiente a estos fines. Y tampoco garantiza el anticipado carácter finalista de la medida, que no ampara cualquier uso, reclamando de nuevo la pertinente intervención convencional.

Por su parte, la grabación de sonidos posee un régimen más riguroso, tanto en su causa existencia de riesgos relevantes para la seguridad de las instalaciones,

54 Por todas, cfr. la STC 98/2000, que contempla posibles modulaciones por conectar con otros derechos protegibles, como la libertad de empresa.

55 Entendiendo justificadas, idóneas, necesarias y equilibradas tales razones, vid. la STC 186/2000.

56 Sí es aplicable para la AEPD, según consta en su ficha práctica de videovigilancia - cámaras para el control laboral.

57 STC 39/2016 (con voto particular) y las SSTS 31 en. 2017 (3331/2015) y 1 y 2 feb. 2017 (3252/2015 y 554/2016, respectivamente), en contraste con la STEDH 9 en. 2018 citada, luego rectificada por la STEDH (Gran Sala) 17 oct. 2019 (López Ribalda II), al considerar que los tribunales españoles ponderaron adecuadamente el interés del empresario en proteger su patrimonio por las sospechas razonables de comisión de graves irregularidades.

bienes y personas derivados de la actividad desarrollada en el centro de trabajo como en sus condiciones de ejercicio, con mención expresa, junto a las garantías previstas para grabar imágenes, de los principios de proporcionalidad e intervención mínima, consecuencia de su mayor lesividad sobre la intimidad. Y es que la posibilidad de captar mediante la grabación indiscriminada de voz conversaciones y comentarios privados, de personas trabajadoras y de terceros, puede ser desproporcionada[58].

En lo relativo a la geolocalización, el artículo 90 LOPDGDD faculta a la empresa a la utilización de estos dispositivos a efectos de control de la actividad laboral, sometida al derecho de información expresa, clara e inequívoca a las personas trabajadoras y, en su caso, a sus representantes, de su existencia y características. Son, pues, extensibles a este supuesto idénticas consideraciones a las ya realizadas, añadiendo que la geolocalización encuentra su principal potencial invasivo cuando, como en actividades móviles o itinerantes, acompaña de forma continua y permanente a la persona trabajadora como instrumento de registro horario y control de su prestación de trabajo, pudiendo dar prueba del incumplimiento por realizar actividades privadas[59], por lo que las cautelas resultan especialmente exigibles para acotar su tratamiento a la jornada laboral y obligaciones contractuales, debiendo resultar proporcionado a riesgo de incurrirse en una injerencia de la intimidad. En todo caso, las fronteras pueden ser difusas en supuestos de autogestión o flexibilidad del tiempo de trabajo, en el que no todo el tiempo en que se efectúa el seguimiento se está a disposición empresarial, recomendando una interpretación restrictiva del control, las garantías propias de los datos personales y su solo uso subsidiario y en casos imprescindibles. De ahí que la negociación colectiva sea casi ineludible para valorar la necesidad e idoneidad de implantación de un sistema de geolocalización y el régimen aplicable.

2. El control biométrico en el contexto laboral

Los sistemas de control biométrico son aquellos que permiten la supervisión o seguimiento del individuo mediante la obtención de datos relativos a sus características físicas, fisiológicas o conductuales y que, por tanto, se destinan a identificar de manera unívoca a una persona física[60], en este caso, a una persona trabajadora. De este modo, las características definitorias de los datos biométricos pueden resumirse en las siguientes:

(i) Son datos personales: en el sentido de "toda información sobre una persona física identificada o identificable ("el interesado")", entendiéndose como "persona física identificable" a "toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante (…) uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, (…)"[61].

(ii) Merecen un "tratamiento técnico específico": se concreta en aplicaciones que, mediante el uso de tecnologías biométricas, posibilitan la autenticación

58 STC 98/2000 y AEPD, *Informe* (2019).

59 Cfr. la STC 61/2021. También, la STS 8 de febrero 2021 (163/2021) y las SSTSJ de Castilla y León de 8 mayo de 2013 (453/2017); de Asturias de 3 de octubre de 2017 (1908/2017); de Madrid de 3 de febrero de 2020 (749/2019). Para la AEPD, en un trabajador itinerante cuyo registro de jornada se geolocaliza se puede comprobar cuándo comienza y finaliza el tiempo de trabajo, pero no verificar dónde se encuentra en cada momento, y exige aplicar los principios generales propios de la protección de datos personales (*La protección de datos en las relaciones laborales*, cit., pgs. 36 y 53 y ss.).

60 Cfr. el artículo 4.14 RGPD.

61 Conforme al artículo 4.1 RGPD.

e identificación automática de la persona a través de la codificación de dos categorías de datos, primera, los aspectos puramente físicos y, segunda, los aspectos relativos al comportamiento, a los que se suman "las técnicas basadas en elementos psicológicos, que incluyen la medición de la respuesta a situaciones concretas o pruebas específicas que se ajusten a un perfil psicológico"[62].

(iii) Permiten o confirman la identificación única de una persona: gracias a su capacidad de almacenamiento de datos y de razonamiento lógico, han establecido previamente patrones físicos, fisiológicos o conductuales; a diferencia de otros sistemas de seguridad, los biométricos proporcionan acceso o la respuesta para la que hayan sido programados en función de quiénes son las personas y no de lo que tienen en su poder *v.gr.* códigos, contraseñas o tarjetas de acceso .

Los sistemas biométricos tienen un funcionamiento aparentemente sencillo[63]. En primer lugar, los datos recogidos por el sensor se evalúan y el algoritmo del sistema se encarga de almacenarlos. Si la calidad es insuficiente, de suerte que no permita identificar de manera concluyente al sujeto, se puede pedir al usuario que vuelva a enviar los datos. En segundo lugar, se selecciona luego un conjunto específico de características para representar el rasgo de identidad calificado, que se almacena en la base de datos del sistema como una plantilla biométrica. En algunos casos, se pueden procesar múltiples muestras para formar una representación en mosaico y algunos sistemas almacenan varias plantillas para compensar las variaciones de datos que pueden surgir de un mismo usuario. Por ejemplo, los modelos más recientes de *Iphone* permiten el acceso al dispositivo mediante el sistema *Face ID* -previamente *Touch ID*, que evaluaba la huella dactilar del usuario-, que toma muestras del rostro de la persona desde muy distintos ángulos para permitir la plena identificación. En adelante, cada vez que el sistema se encuentre con un usuario cuyos patrones ya ha estudiado y registrado, le permitirá acceder a un lugar o activará la función para la que esté programado.

Como se advertirá, los sistemas biométricos resultan particularmente útiles en el seno de la empresa para distintas finalidades, que comparten su misión de controlar y supervisar diversos aspectos de la prestación de servicios de las personas trabajadoras. Baste recordar, como hemos indicado, que la empresa puede exigir en todo momento el cumplimiento de los deberes laborales y, para tal fin, puede establecer cuantos mecanismos de vigilancia entienda convenientes, siempre y cuando garanticen la seguridad y salud de las personas trabajadoras, así como el respeto a su dignidad, conforme al artículo 20.3 ET.

En este sentido, como ya ha expresado el Comité de Ministros del Consejo de Europa a colación de los datos biométricos, su recogida y tratamiento "no debería realizarse salvo en los casos en que sea necesario para la protección de los intereses legítimos de los trabajadores, de los empresarios o terceros y ello solo como última opción, cuando sea imposible utilizar otros métodos alternativos de tratamiento menos intrusivos para la vida privada y siempre que su tratamiento se

62 Dictamen 3/2012 sobre la evolución de las tecnologías biométricas (puede consultarse en Grupo de Trabajo del Artículo 29, cit., pg. 4.

63 THOMAS COMPANY, *Biometric Access Control Systems, Security Measures, and Principles*, s.f.

acompañe de las garantías apropiadas"[64], a lo que debe añadirse que el procesamiento de estos datos debe basarse "en métodos científicamente reconocidos y debe estar sujeto a los requisitos de estricta seguridad y proporcionalidad"[65]. Por tanto, las cautelas en la utilización de sistemas de IA para el control biométrico deben extremarse, más aún ante la ausencia de contornos claros en lo que concierne a las potestades empresariales de vigilancia con estas herramientas. Recuérdese que la prohibición general de tratamiento de datos personales que revelen datos biométricos no es de aplicación cuando sean necesarios para el "cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral"[66].

Así, aun cuando su utilización más frecuente es el control de acceso al centro de trabajo, nada impide su uso con fines de registro de jornada, de vigilancia e incluso disciplinarios. Los expertos apuntan a colación de los sistemas de acceso, sin perjuicio de su posible extensión a otros ámbitos de la empresa, las siguientes ventajas[67]: (i) los sistemas de control biométrico son más seguros, dado que los patrones observados son únicos para cada usuario; (ii) instalado el sistema, su coste de mantenimiento es mucho menor en comparación con otros; y (iii) se elimina la necesidad de utilizar tarjetas personales, interruptores u otra clase de dispositivos, en tanto que la autorización solo requiere de las características únicas de cada sujeto para permitir su acceso.

De lo expuesto hasta aquí, podría colegirse *a priori* que el hecho de captar una huella digital, una imagen del rostro o un patrón de comportamiento de una persona no suponen vulnerar su derecho a la integridad personal. No obstante, esta primera aproximación es muy discutible, en tanto que para obtener esa información el propio cuerpo del usuario se ve involucrado en mayor o menor medida[68]. Valga mencionar en esta sede el caso extremo de la empresa belga que implantó un *chip* en la yema del dedo a ocho de sus empleados con el fin de que lo empleasen tanto para acceder al centro de trabajo como para almacenar sus datos a modo de tarjeta de visita[69]. Precisamente por la afectación al cuerpo de la persona y los riesgos que puede desencadenar el mero uso de estos sistemas, es imperativo que los recursos de control biométrico observen las condiciones y garantías que establecen tanto el RGPD como la LOPDGDD y que, a su vez, las personas trabajadoras sean informadas de los fines que se persiguen y del tratamiento que se da a dichos datos, *ex* artículo 64 ET[70]. Además, los responsables del tratamiento de datos así obtenidos deben tener en cuenta la proporcionalidad de las medidas y adoptar las acciones necesarias para mitigar o reducir la escala e impacto de su tratamiento. En este sentido, el aludido Comité Europeo de Protección de Datos -anteriormente denominado Grupo de Trabajo del Artículo 29- recomienda, como buena práctica, la realización de una evaluación de impacto relativa a la protección de datos ("**EIPD**") previo a la introducción de cualquier tecnología de control en el seno de la empresa[71], si bien la AEPD obliga a que se realice una EIPD en caso de "tratamientos que impliquen el uso de datos biométricos con el propósito de identificar de manera única a una persona física"[72].

64 Principio 18 de la Recomendación (2015) 5, del Comité de Ministros del Consejo de Europa, apartado 1.

65 *Ibidem*, apartado 2.

66 Artículos 9.1 y 9.2 b) RGPD.

67 LARSON, T., "What is a Biometric Access Control System?", *Linkedin*, 12.04.2022.

68 MERCADER UGUINA, J.R., "Datos biométricos en los centros de trabajo", en BAZ RODRÍGUEZ, J. (Dir.), *Los nuevos derechos digitales laborales de las personas trabajadoras* en España, CISS (Madrid), 2021, pg. 2.

69 EFE, "Una empresa belga implanta un chip para controlar empleados", en La Vanguardia, 04.02.2017.

70 STS de 19 de diciembre de 2005, rec. 138 /2005, ECLI:ES:TS:2005:7905.

71 Grupo de Trabajo del Artículo 29, Dictamen 2/2017 sobre sobre el tratamiento de datos en el trabajo, pgs. 4 y15. La regulación de la EIPD se encuentra en el artículo 35 del RGPD, y se recomienda su elaboración antes del tratamiento por parte de su responsable "[c]uando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas (…)" (apartado 1).

72 Agencia Española de Protección de Datos, *Listas de tipos de tratamientos de datos que requieren evaluación de impacto relativa a protección de datos (art 35.4)*, 2019, pg. 2.

Es importante destacar que los sistemas de control biométrico no son novedosos para la jurisprudencia y doctrina administrativa española. Así, la Audiencia Provincial ("**AP**") de Barcelona estudió la propuesta de una cadena de supermercados de establecer un sistema de reconocimiento facial para asegurar el cumplimiento de la pena accesoria de imposibilidad de acceso a sus establecimientos por parte de dos personas condenadas por una tentativa de robo con violencia[73]. El sistema realizaba en 0,3 segundos un proceso ciertamente complejo: detectaba imágenes de todas las personas que accediesen al centro, las relacionaba con las que constasen en su base de datos preexistente y, en caso de que no estuviesen registradas como personas con el acceso prohibido, eliminaba la imagen captada. La empresa argumentó que el sistema era necesario e idóneo para garantizar el cumplimiento de la prohibición de acceso, lo que no impidió a la AP rechazar la propuesta por ser contraria a la normativa de protección de datos. Adicionalmente, la Sala consideró que la medida solo perseguía un interés particular, el de la cadena de supermercados, no el interés general, de manera que se interpretó injustificada la captación e identificación de personas. Curiosamente, a partir de la publicación en prensa de esta resolución, la entonces directora de la AEPD inició un procedimiento de oficio que concluyó en la Resolución de 27 de julio de 2021[74].

En este sentido, la AEPD caracteriza el sistema como de reconocimiento facial masivo y remoto, conforme a la definición del Libro Blanco sobre IA de la Comisión Europea, y como apunta la propuesta de Reglamento de Inteligencia Artificial ("**RIA**"), que clasifica como "riesgo inadmisible" la implementación de sistemas que posibilitan la identificación biométrica en tiempo real en espacios de acceso público, con muy escasas excepciones (considerandos 23 y 24 RIA). Las principales conclusiones del informe de la AEPD apuntan a que: (i) los sistemas de reconocimiento facial exigen una base de legitimación del tratamiento excepcional[75]; (ii) la caracterización de los sistemas biométricos impone deberes de información reforzados y muy estrictos, pues se trata de riesgos específicos y muy elevados; y (iii) en caso de que los sistemas de control biométrico se utilicen en la empresa, es imprescindible valorar los riesgos sobre los derechos de la plantilla en la EIPD[76].

En lo que respecta a su uso en ámbitos laborales, la Sala Tercera del TS estudió en 2007 la legalidad de un sistema de control de jornada implantado por la Consejería de Presidencia de Cantabria en junio de 2002 de base dactiloscópica[77]. El sistema exigía que las personas trabajadoras posasen la palma de su mano sobre un escáner dotado de rayos infrarrojos para acceder a su centro de trabajo, gesto que permitía la transformación de la imagen tridimensional de la palma en un algoritmo plasmado en una plantilla biométrica incorporada a una base de datos. Así, el sistema asociaba la imagen de la mano a la identidad del empleado, haciendo posible el registro horario. Cabe destacar que la información convertida en algoritmo no era idónea por sí sola para identificar a la persona trabajadora, sino que podía hacerlo por asociación con la imagen que constaba en la base de datos. Curiosamente, con carácter previo a su implantación definitiva (a resultas

73 Auto de la Audiencia Provincial de Barcelona (sec. 9ª) de 15 de febrero de 2021, num. 72/2021, rec. 840/2020, ECLI:ES:APB:2021:1448A.

74 Determinación del procedimiento por pago voluntario, PS/00120/2021.

75 Artículo 9 RGPD.

76 Artículo 35 RGPD.

77 STS de 2 de julio de 2007, rec. 5017/2003, ECLI:ES:TS:2007:5200.

de la citada STS de 2 de julio de 2007), el TC tuvo la oportunidad de pronunciarse sobre este sistema en su Auto 57/2007, de 26 de febrero, que inadmitió el recurso de amparo frente a la Sentencia del Tribunal Superior de Justicia ("**TSJ**") de Cantabria de 23 de enero de 2003[78] . Después de analizar su doctrina sobre el alcance del derecho fundamental a la integridad física y su relación con el derecho a la salud, el TC rechaza que el sistema vulnere cualquiera de ellos, afirmando que la imputación de vulneración de los derechos en juego desconoce la posible incidencia que el lector biométrico puede tener sobre la salud, lo que no supone una afirmación traducible en una vulneración del derecho a la integridad personal. Por lo tanto, concluye que la decisión del TSJ de Cantabria, que descartó cualquier vulneración tras valorar las pruebas obrantes en el expediente administrativo, era constitucionalmente adecuada, ya que no había pruebas que demostraran los posibles daños que pudieran derivarse de la implantación del nuevo sistema de control de jornada.

En un sentido muy similar, el TS, aclarado que el sistema no lesionaba la integridad personal como ya expresase el TC, analizó su posible colisión con el derecho a la intimidad de las personas trabajadoras, concluyendo que el sistema de control dactiloscópico "no respond[ía] al patrón de las intromisiones ilegítimas en la esfera de la intimidad, tanto por la parte del cuerpo utilizada, como por las condiciones en que se usa"[79]. El TS estima que la finalidad perseguida, el registro horario, es legítima e insiste en que, pese a ser susceptible de identificar a personas (y, por tanto, sometido a la Ley Orgánica 15/1999, de Protección de Datos, a la sazón aplicable) en el caso no se probó que el sistema infringiese dicha norma y, con ella, el derecho fundamental a la protección de datos de carácter personal[80]. En suma, el TS consideró que el sistema elegido por el gobierno cántabro era adecuado, pertinente y no excesivo.

Esta doctrina ha sido replicada por los TSJ. Así, la STSJ de Andalucía, Sala de lo Contencioso-Administrativo, de 3 de diciembre de 2007, sobre toma de datos biométricos con fines de registro horario por parte de la Administración, con idéntico resultado al analizado. También la STSJ de Islas Canarias, de 29 mayo de 2012, se remite expresamente a la repetida STS de 2 de julio de 2007 al declarar que un sistema de control de horario implantado por la empresa, nuevamente basado en el reconocimiento de la huella dactilar, no lesionaba el derecho fundamental a la intimidad personal de la plantilla. Por su parte, la STSJ de Murcia de 25 enero de 2010 señaló algo de sumo interés para concluir que los sistemas dactiloscópicos no suponen una intromisión ilegítima en la esfera de la intimidad, precisamente por la parte del cuerpo utilizada, así como por las condiciones en las que se usa[81].

Ahora bien, en tanto que el uso de la huella dactilar se encuentra generalmente amparado por su escasa injerencia en la integridad de la persona, mayores dudas plantea el uso de la imagen del rostro. Así lo ha entendido la AEPD que afirmó que se trata de una cuestión compleja e interpretable, en la que debe valorarse el "caso concreto según los datos tratados, las técnicas empleadas para su

78 STSJ Cantabria de 23 de enero de 2003, Rec. 166/2002, ECLI:ES:TSJCANT:2003:81.

79 STS de 2 de julio de 2007, rec. 5017/2003, ECLI:ES:TS:2007:5200, Fundamento Jurídico Quinto.

80 *Ibidem.*, Fundamento Jurídico Sexto.

81 Recs. 2203/2007, ECLI:ES:TSJAND:2007:14805 y 398/2012, ECLI:ES:TSJICAN:2012:1286 y 1071/2009, ECLI:ES: TSJMU:2010:47, Fundamento Jurídico Tercero, respectivamente.

tratamiento y la consiguiente injerencia en el derecho a la protección de datos"[82]. Y es que la información que transmite la cara de una persona trasciende su mera identidad, pues normalmente refleja "características fisiológicas y psicológicas tales como el origen étnico, emociones y bienestar"[83]. A mayor abundamiento, los expertos ya han apuntado a los riesgos que los sistemas de control biométrico pueden acarrear, entre ellos, la toma de una fotografía a distancia sin conocimiento del interesado[84] o la clonación de imágenes[85].

IV. Riesgos y desafíos de la digitalización en el entorno laboral: la seguridad y salud en el trabajo

Hasta aquí, puede apuntarse como primera conclusión que el verdadero problema en la empresa no es la obtención de los datos personales de la plantilla (especialmente los datos biométricos), sino su correcto tratamiento. A modo de ejemplo, el considerando 51 del RGPD indica que "el tratamiento del rostro con software de reconocimiento facial se encuentra dentro de los datos biométricos" y que, por ello, su tratamiento se encuentra prohibido, con las excepciones del artículo 9.2 RGPD; por tanto, no se limita a expresar una realidad técnica, sino a reflejar una preocupación. En el terreno laboral, el Comité Europeo de Protección de Datos alertó sobre la necesidad de que las empresas se abstengan de utilizar los sistemas de control biométrico. Así, incluso admitiendo que en determinadas circunstancias podría justificarse el uso del control biométrico sobre las expresiones de las personas trabajadoras, estas serán muy minoritarias y, además, no pueden ser utilizadas para invocar una legitimación general que dé cobertura, sin más, al uso de dicha tecnología[86].

En este escenario, y habida cuenta de las recomendaciones del Grupo de Trabajo del Artículo 29[87], es comprensible que el futuro RIA sea cauto y catalogue como "riesgo inadmisible" a los sistemas de identificación biométrica en tiempo real en espacios de acceso público, con muy contadas excepciones que, de concurrir, implicarían que el riesgo pasase de "inadmisible" a "alto". Entre estos sistemas de "riesgo alto" se encuadran los que, implicando una amenaza para los derechos fundamentales, pueden ser utilizados de la mano de garantías reforzadas, entre los que destacan los utilizados en el contexto del empleo y la gestión de personal[88], que imponen automáticamente el cumplimiento de ciertas obligaciones, como la implementación de un sistema de gestión de riesgos y de gobernanza de datos, el deber de documentación para consulta de las autoridades y la creación de un registro que asegure la posibilidad de auditar el sistema. Así, el legislador europeo ha intentado, de manera muy preliminar, acotar los medios de control disponibles en el seno de la empresa, si bien la normativa europea adolece de falta de previsión de medidas limitativas concretas. En primer lugar, dentro de los límites genéricos a cualquier intromisión en la intimidad personal, los sistemas de control empresarial deberán "preservar la dignidad humana de los interesados, así como sus intereses legítimos y sus derechos fundamentales"[89]. En segundo lugar, estos avances hacia la mayor digitalización y eficiencia del entorno laboral "no

82 Informe del Gabinete Jurídico de la AEPD de 8 de mayo de 2020, N/REF: 0036/2020, pg. 19.

83 Dictamen 3/2012 sobre la evolución de las tecnologías biométricas. (2012). En Grupo de Trabajo del Artículo 29 (00720/12/ES WP193), pg. 23.

84 *Ibid.*

85 MORENO, V., "Los peligros legales de los sistemas", en Expansión, 23.02.2023.

86 Dictamen 2/2017, cit., pg. 21.

87 Documento de trabajo sobre biometría (2003). En Grupo de Trabajo del Artículo 29 (12168/02/EN WP 80).

88 Considerando 36 RIA.

89 Artículo 88.2 RGPD

deben conducir a un uso deshumanizado de las herramientas digitales ni suscitar preocupación por lo que respecta a la privacidad y la recogida desproporcionada e ilegal de datos personales, la vigilancia y el seguimiento de los trabajadores"[90]. En tercer lugar, queda pendiente el hecho de "garantizar que el uso de la inteligencia artificial en el lugar de trabajo sea transparente y siga un enfoque basado en los riesgos, y que se adopten las medidas de prevención correspondientes para mantener un entorno de trabajo seguro y saludable"[91].

Sobre este último aspecto, se ha apuntado la gran utilidad en la mejora en las medidas de prevención y control de la seguridad y salud que el uso de sensores digitales y el análisis de los datos de la actividad laboral pueden aportar a las empresas[92]. En este sentido, recuérdese que, como regla general, está prohibido el tratamiento de los datos relativos a la salud de las personas, si bien la prohibición se excluye cuando el tratamiento de estos datos sea necesario "para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social" (artículo 9.1 y 9.2.h) RGPD).

La anterior no es cuestión menor, ya que la obtención y el tratamiento de estos datos puede permitir a las empresas conocer en qué puntos de la cadena productiva conviene introducir sistemas de IA, en aras de mejorar las medidas de seguridad y salud. Así, la Agencia Europea para la Seguridad y la Salud en el Trabajo ha concluido que los robots en sentido amplio, incluidos los sistemas de IA, liberan de la realización de tareas peligrosas, ya sea por el esfuerzo físico o por la exposición a elementos químicos o ergonómicos que la actividad laboral puede implicar, de modo que contribuyen a paliar los riesgos para la seguridad y la salud de la plantilla[93]. No obstante, en la actualidad el seguimiento de los datos de la actividad laboral se usa principalmente con el fin de controlar la productividad, lo que puede impactar negativamente en la seguridad y salud laboral[94], apuntando algunos estudios los efectos negativos que han tenido en las personas al servicio de las plataformas digitales el empleo de los datos con el mero fin de medir la productividad[95]. Así, la evaluación y el control constante de la actividad, incluso cuando la monitorización no depende directamente de la empresa, sino del consumidor, parece provocar un aumento notable en el ritmo de trabajo y, con él, del riesgo de lesiones o accidentes.

Con todo, los riesgos para la seguridad y salud de las personas no se presentan solo en el ámbito de las plataformas digitales, sino en aquellas empresas de corte tradicional que han implantado en su estructura sistemas de control digital de la actividad, así como la automatización de ciertas decisiones de gestión[96]. De una parte, la mera interacción entre ciertos tipos de sistemas de IA y los humanos, pese a la exigencia de las normas aplicables, puede provocar, entre otros, riesgos de colisión, de seguridad y medioambientales[97]. De otra, los expertos apuntan a que la presión para rendir al mismo nivel que los robots puede provocar estrés y

90 Resolución del Parlamento Europeo, de 21 de enero de 2021, con recomendaciones destinadas a la Comisión sobre el derecho a la desconexión [2019/2181(INL)].

91 PARLAMENTO EUROPEO, CONSEJO y COMISIÓN EUROPEA, *Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital* (2023/C 23/01), vid. epígrafe "condiciones de trabajo justas y equitativas".

92 GINÈS i FABRELLAS, A., "La gestión algorítmica del trabajo: nuevos retos jurídicos, tecnológicos y éticos", en *Digitalización, recuperación y reformas laborales*, cit., pg. 307.

93 AGENCIA EUROPEA PARA LA SEGURIDAD Y LA SALUD EN EL TRABAJO, *Estudio prospectivo sobre los riesgos nuevos y emergentes para la seguridad y salud en el trabajo asociados a la digitalización en 2025*. Oficina de Publicaciones de la Unión Europea, 2018, pg. 38.

94 DZIEZA, J., "How hard will the robots make us work?", *The Verge*, 27.2.2020.

95 GARBEN, S., *Protecting workers in the online platform economy: an overview of regulatory and policy developments in the EU*, European Risk Observatory Discussion paper, European Agency for Safety and Health at Work, Luxemburgo, 2017, pgs. 24-28.

96 MOORE, P. V., "Inteligencia artificial en el entorno laboral. Desafíos para los trabajadores", en *El trabajo en la era de los datos*, BBVA.

97 Organización de los Países Bajos para la Investigación Científica Aplicada, Emergent Risks to Workplace Safety; Working in the Same Space as a Cobot, Ministerio de Trabajo y Asuntos Sociales, La Haya, 28.08.2018, pgs.18-19.

ansiedad[98], especialmente cuando la plantilla siente que debe competir con un elemento no humano al que no tienen acceso y que no pueden controlar.

Todo desemboca en una probable mayor incidencia de riesgos ergonómicos, visuales, psicosociales y aun biológicos, requeridos de una nueva estrategia preventiva en relación con la digitalización en la empresa que ya ha identificado un nuevo riesgo laboral genérico: la fatiga informática, fruto de la confusión vida profesional y personal, prolongación de jornadas, conectividad constante, estrés, entre otros. Estrategia que abarca todas las fases de la actividad de prevención, desde la evaluación de los riesgos hasta la adopción de las oportunas medidas preventivas, que encuentran en la formación e información elementos indispensables capaces de generar una cultura preventiva que todavía no alcanza a incorporar de manera natural que la actual organización del trabajo y la masiva incorporación de las Tecnologías de la Información y Comunicación al entorno laboral representa una amenaza seria para la seguridad y salud en el trabajo.

V. Hacia una gestión colectiva de la digitalización en la empresa: el papel de la negociación colectiva

Como se ha venido analizando, la ausencia de una regulación clara tanto en la UE como en España respecto de los límites de los sistemas de control empresarial en la era tecnológica impide con carácter general y apriorístico su identificación, aun cuando a la cuestión siempre sobrevuela el respeto a los reiterados derechos a la intimidad personal y a la protección de datos y que, como también se ha estudiado, sean aplicables principios básicos de necesidad, idoneidad, proporcionalidad y minimización.

A falta de que la regulación concreta de estos aspectos cristalice en lo que la doctrina acierta en llamar "Estatuto de los Trabajadores del siglo XXI"[99], cuando no "del siglo XXII"[100], lo cierto es que la negociación colectiva parece un marco idóneo y casi imprescindible para colmar las lagunas existentes en la actualidad y para especificar y acomodar los límites de ejercicio de la digitalización en la empresa, adaptando el uso de los recursos digitales a las circunstancias del entorno laboral, como se reconoce a nivel doctrinal, convencional y aun desde la propia Administración laboral[101]. Aún más, en el establecimiento de normas específicas relativas al tratamiento de datos personales de las personas trabajadoras como tarea que cada Estado Miembro debe acometer, se contempla que esta actuación no se lleve a cabo exclusivamente a través de leyes, sino que puede desarrollarse mediante convenios colectivos, de sector y de ámbito empresarial[102]. Como ya se ha expresado, el artículo 91 RGPD reitera la relación típica de complementariedad y suplementariedad entre la ley y los convenios colectivos, otorgando a la autonomía colectiva la capacidad de mejorar los requisitos mínimos y, sobre todo, de especificar su contenido; con la ventaja añadida de que las imprecisiones legales pueden colmarse correctamente y sin duplicidades y con mayor adecuación por la proximidad y asequible acercamiento a las circunstancias de sectores

98 MOORE, P. V., "Inteligencia artificial en el entorno laboral. Desafíos para los trabajadores", en El trabajo en la era de los datos, BBVA; AGENCIA EUROPEA PARA LA SEGURIDAD Y LA SALUD EN EL TRABAJO, *Estudio prospectivo sobre los riesgos nuevos y emergentes para la seguridad y salud en el trabajo asociados a la digitalización en 2025*, cit., pg. 38.

99 VALDEOLIVAS GARCÍA, Y., "Derechos de información, transparencia y digitalización", cit., pg. 192.

100 GORDO GONZÁLEZ, L., "¿Existirán trabajadores por cuenta ajena en el futuro? La necesidad de desarrollar un Estatuto de los Trabajadores para el Siglo XXI (… y para el XXII)", *El Foro de Labos*, 20.12.2022.

101 *Guía práctica y herramienta sobre la obligación empresarial de información sobre el uso de algoritmos en el ámbito laboral: Información algorítmica en el ámbito laboral* (2022), Ministerio de Trabajo y Economía Social, Consultado el 20 de febrero de 2023, pg. 17, que señala que dado que el uso de algoritmos puede afectar a estas principales condiciones de trabajo, debería ser objeto de tratamiento en la negociación colectiva.

102 Considerando 115 del RGPD. Más ampliamente, sobre el contenido convencional en la materia, BLÁZQUEZ AGUDO, E. M., "¿Qué están incluyendo los convenios estatales en materia de protección de datos? La todavía escasa regulación", en *El Foro de Labos*, 17.10.2022.

y empresas[103]. Por su parte, en la normativa española, a lo anterior se añade el papel de los convenios como garante de derechos fundamentales[104], toda vez que el artículo 91 LOPDGDD les atribuye la posibilidad de establecer "garantías adicionales de los derechos y libertades relacionados con el tratamiento de los datos personales de los trabajadores y la salvaguarda de derechos digitales en el ámbito laboral".

El impacto tecnológico, que desenvuelve sus efectos sobre todas las fases y contenido de la relación contractual, reclama el protagonismo de la negociación en la adaptación de múltiples aspectos laborales, hasta considerar este ámbito como un espacio de genuino autogobierno colectivo[105]. La cualificación profesional y la adquisición de competencias digitales por parte de las personas trabajadoras, la adaptación de los sistemas de clasificación profesional y de retribución, las medidas de flexibilidad interna y, en fin, el propio desenvolvimiento de la acción representativa en el nuevo entorno digital son materias que reclaman una acción anticipatoria por parte de la negociación colectiva. La autonomía colectiva no puede ser retardataria de los cambios necesarios que de forma dinámica y adaptativa puede asegurar en los lugares de trabajo y debe asumir como propia la función de gobernanza del fenómeno digital en las relaciones laborales. De un fenómeno tan volátil y cambiante como la digitalización en el empleo, de potencial lesivo tan relevante, es esperable que los sujetos colectivos, y los operadores jurídicos, sean conscientes de la necesidad e idoneidad de la autonomía colectiva para establecer un equilibrio adecuado entre los intereses intrínsecamente enfrentados, articulando fórmulas de cooperación, a veces limitadas a la relación de complementariedad con la norma estatal, otras de suplemento (no de minoración) de garantías y derechos, pero siempre bajo el prisma de flexibilidad que el nuevo modelo impone, evitando los efectos perversos y sesgos potencialmente tan sensibles en esta realidad normativa[106]. Con estas coordenadas, cabe confiar en un verdadero salto cualitativo en la gestión colectiva del reto digital en las relaciones de trabajo.

Con todo, no es objetable que la negociación colectiva todavía dispone de un amplio recorrido para cubrir todo su particular potencialidad reguladora en este ámbito y que los resultados, en términos globales, aún son insuficientes. Por ello, resultan de especial interés algunos instrumentos convencionales concretos que abren brecha en este campo y que pueden servir de adecuada referencia a los Convenios por negociar, como los que se relacionan a continuación.

En efecto, un ejemplo significativo de los esfuerzos de la negociación colectiva por regular el papel de los algoritmos en la prestación de servicios es el Convenio colectivo acordado por la empresa *Just Eat* y los sindicatos CCOO y UGT el 17 de diciembre de 2021 en el Servicio Interconfederal de Mediación y Arbitraje FSP[107]. Su artículo 68 se refiere a los derechos digitales de las personas trabajadoras, entre los que se garantizan el derecho a la supervisión humana en el uso de algoritmos y a recibir información sobre las herramientas de trabajo digitales, prohibiéndose expresamente que el uso de esos datos pueda producir discriminación.

103 VALDEOLIVAS GARCÍA, Y., "Derechos de información, transparencia y digitalización", cit., pg. 218.

104 *Ibidem.*

105 VALDEOLIVAS GARCÍA, Y., "Derechos de información, transparencia y digitalización", cit., pg. 218

106 De especial valor son tanto la *Guía práctica y herramienta sobre la obligación empresarial de información sobre el uso de algoritmos en el ámbito laboral*, como las elaboradas por la propia AEPD y las distintas organizaciones sindicales citada supra, con interesantes y apropiados criterios y pautas de actuación a aplicar en las mesas de negociación, cuyas indicaciones deberían traspasarse pronto al articulado de los convenios colectivos. Acta de acuerdo en el procedimiento de mediación promovido por Federación de Servicios CCOO, FSC-CCOO y FeSMC-UGT frente a TAKEAWAY EXPRESS SPAIN, S.L. (JUST EAT), [M/441/2021/N], 17.12.2021.

107 Acta de acuerdo en el procedimiento de mediación promovido por Federación de Servicios CCOO, FSC-CCOO y FeSMC-UGT frente a TAKEAWAY EXPRESS SPAIN, S.L. (JUST EAT), [M/441/2021/N], 17.12.2021.

En la misma línea, los Convenios sectoriales han querido regular los derechos de las personas trabajadoras, tanto frente al uso de dispositivos[108], especialmente de videovigilancia y/o de geolocalización como en la garantía de los deberes de información debidos individuales y colectivos[109], completándose con ello la genérica previsión de información a la representación legal de los trabajadores del artículo 64.4.d) ET respecto 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.

Debemos destacar, por último, la curiosa iniciativa del IV Convenio colectivo estatal de la industria, las nuevas tecnologías y los servicios del sector del metal, que cuenta con un capítulo entero dedicado a la protección de datos de carácter personal y garantías digitales[110], entre cuyos artículos se encuentra la recomendación de crear en las empresas con convenio propio una comisión paritaria para la protección de los derechos digitales, atribuyéndole el convenio algunas competencias de suma importancia como "la salvaguarda de derechos digitales en el ámbito laboral, de negociar los criterios referidos en los preceptos anteriores de utilización de los dispositivos digitales durante la vigencia del convenio, el establecimiento de las garantías relativas a los derechos y libertades relacionados con el tratamiento de datos personales de las personas trabajadoras, y la regulación de las modalidades de ejercicio del derecho a la desconexión"[111].

En un fenómeno volátil como es la digitalización en el empleo al margen de su potencial lesivo que, como hemos visto, es muy considerable, es de esperar que los negociadores colectivos y los operadores jurídicos sean conscientes de la necesidad y la idoneidad de la autonomía colectiva para establecer un equilibrio ponderado entre los intereses de la empresa y los derechos de las personas trabajadoras[112]. Para ello, es necesario que los operadores jurídicos cooperen[113], tanto para evitar solapamientos en la regulación como para preparar a las personas trabajadoras y empresas del futuro para lo que está por venir en aras de la flexibilidad que impone el nuevo modelo, evitando, con ello, los posibles efectos perversos que esta tecnología es susceptible de generar.

VI. Conclusiones

La revolución digital en la empresa se está produciendo ante nosotros con una rapidez y sofisticación sin precedentes en la historia. Esta agilidad, por el momento, no se ha visto acompañada de actos normativos del legislador a la altura de las necesidades reales y del valor de los intereses en juego, hasta permitir acotar los límites de la aplicación de tan significativos avances tecnológicos sobre los

108 Resolución de 19 de julio de 2022, de la Dirección General de Trabajo, por la que se registra y publica el Convenio colectivo de elaboradores de productos cocinados para su venta a domicilio, artículo 57.3; Resolución de 29 de diciembre de 2021, de la Dirección General de Trabajo, por la que se registra y publica el IV Convenio colectivo estatal de la industria, las nuevas tecnologías y los servicios del sector del metal, artículos 120-121; Resolución de 12 de julio de 2022, de la Dirección General de Trabajo, por la que se registra y publica el Convenio colectivo de recuperación y reciclado de residuos y materias primas secundarias, artículo 7 bis.

109 Resolución de 26 de julio de 2018, de la Dirección General de Trabajo, por la que se registra y publica el Convenio colectivo general de la industria química, artículo 8; Resolución de 23 de julio de 2022, de la Dirección General de Trabajo, por la que se registra y publica el Convenio colectivo para la industria fotográfica, artículo 4.2.

110 Resolución de 29 de diciembre de 2021, de la Dirección General de Trabajo, por la que se registra y publica el IV Convenio colectivo estatal de la industria, las nuevas tecnologías y los servicios del sector del metal, capitulo XX.

111 Resolución de 29 de diciembre de 2021, de la Dirección General de Trabajo, por la que se registra y publica el IV Convenio colectivo estatal de la industria, las nuevas tecnologías y los servicios del sector del metal, artículos 123.

112 VALDEOLIVAS GARCÍA, Y., "Derechos de información, transparencia y digitalización", cit., pg. 220.

113 Dictamen del Comité Económico y Social Europeo sobre la «Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Plan coordinado sobre la inteligencia artificial» COM (2018) 795 final, [2019/C 240/12], puntos 2.4, 2.5 y 4.4.

derechos de las personas trabajadoras. Con todo, no cabe obviar que comienzan a dibujarse los contornos de los derechos digitales en el contexto laboral y que el debate académico y de los operadores jurídicos, económicos y sociales al respecto comienza a ganar terreno en la agenda.

Las muestras que vamos conociendo de esta preocupación y de la creciente gestión del fenómeno, tanto en informes de expertos y declaraciones de organismos públicos como en las nuevas versiones de convenios colectivos sectoriales y de empresa, son extremadamente interesantes y arrojan luz a falta de un pronunciamiento definitivo a cuenta del legislador. El denominador común de todos ellos es el respeto a la dignidad de la persona, así como a los derechos fundamentales más básicos, lo que es especialmente importante en un contexto en el que estos bienes colisionan con intereses de carácter empresarial. No obstante, aunque a nivel convencional se estén compatibilizando los derechos digitales de las personas trabajadoras con las potestades de dirección y de control de la empresa, el consenso no debe presumirse definitivo, menos aún en un escenario tan cambiante.

Aún se aprecian escenarios de conflicto que recomiendan adaptaciones o especificaciones sistemáticas para proteger los bienes constitucionales con garantías instrumentales que aporten seguridad jurídica a ambas partes y equilibrio en la relación de trabajo. La notable capacidad empresarial de utilización de información obtenida de medios digitales y su uso con fines de control laboral deben traducirse en decisiones más eficientes desde el plano organizacional, pero que, desde el contexto de los derechos fundamentales de las personas trabajadoras, preserven los espacios íntimos y privados que impidan hacerles sujetos incondicionada y permanentemente transparentes, y dirigido al cumplimiento de legítimos y ponderados intereses empresariales. Esta dimensión reclama una posición legal y convencional más proactiva, porque los límites se han articulado básicamente mediante derechos individuales de información y, en su caso, presupuesta la exactitud y transparencia, de consentimiento informado de la persona trabajadora afectada, a menudo tan débiles que permiten cuestionar su existencia, quedando relegados los controles colectivos, meramente secundarios o subsidiarios.

Se propone aquí un modelo de gobernanza colectiva de la digitalización en las empresas que, sobre permitir la participación colectiva en la elaboración de las políticas empresariales en relación con este fenómeno, asegure un adecuado balance de los contrapuestos intereses involucrados, sin sospechar abusos en las empresas, pero constatando que el imparable incremento de información disponible pueden provocar, cuando los límites no están claros, decisiones automatizadas que pueden no discriminar la cualidad de la información e introducir sesgos. Aplicar idénticas reglas y cautelas a las existentes en un momento en que los datos eran muy inferiores cuantitativa y cualitativamente ignora la creciente potencialidad en este momento de injerencias injustificadas y lesiones a los derechos laborales. Ello solo se compensa con la intervención de las instancias colectivas, cuyos derechos de información aseguran un conocimiento cierto y más completo,

y cuya participación en el diseño digital en la empresa permite incorporar medidas preventivas y anticipatorias de actuaciones desviadas.

Justamente esa finalidad preventiva y de anticipación y evitación de las lesiones promueve la mayor intervención de la negociación colectiva. La legislación se mueve por criterios individualistas y con controles a posteriori preferentemente reparadores. Sin embargo, faltan marcos de actuación previos a la medida empresarial misma que establezcan el ámbito de actuación legítima y la limitación de los poderes. En este contexto, la negociación colectiva se presenta como la fuente idónea de determinación de las condiciones de ejercicio de los poderes empresariales en el entorno digital. Junto a un modelo de cogobernanza empresarial y colectiva del fenómeno digital, ese esquema serviría para una implantación real, natural y equilibrada del hecho digital, otorgando mayor legitimidad y certidumbre a las facultades empresariales de control y vigilancia, ahora prácticamente copadas por el uso de equipos tecnológicos. Ese modelo de autorregulación haría de este ámbito un marco más garantista y transparente, con mayor seguridad jurídica, al tiempo que más proclive a la expansión sin recelos de una realidad imparable.

El futuro en la empresa pasa por convencerse de que las herramientas basadas en algoritmos e IA han venido para quedarse y que la defensa frente a sus posibilidades invasivas no puede ser menos digitalización, sino más segura y ecuánime. Bajo este nuevo paradigma, fortalecer la colaboración de todos los agentes en aras de dotar de seguridad y previsibilidad al trabajo del siglo XXI concierne a las autoridades, las organizaciones públicas y privadas y la fuerza laboral en una acción conjunta y coordinada para regular un proceso que, en la actualidad, no conoce límites y cuyas connotaciones aún resultan inimaginables.