LOS DERECHOS DIGITALES DEL EMPLEADO PÚBLICO ANTE LAS TRANSFORMACIONES TECNOLÓGICAS Y EL USO DE LA IA EN LOS PROCESOS DE GESTIÓN DE PERSONAS

ENPLEGATU PUBLIKOEN ESKUBIDE DIGITALAK ERALDAKETA TEKNOLOGIKOEN ETA PERTSONAK KUDEATZEKO PROZESUETAN ADIMEN ARTIFIZIALA ERABILTZEAREN AURREAN

THE DIGITAL RIGHTS OF PUBLIC EMPLOYEES BEFORE THE TECHNOLOGICAL TRANSFORMATION AND USE OF IA IN PEOPLE MANAGEMENT PROCESSES

Josefa Cantero Martínez
Catedrática de Derecho Administrativo
Universidad de Castilla-La Mancha
josefa.cantero@uclm.es

https://doi.org/10.47623/ivap-rvgp.28.2025.03

Recibido: 28/03/2025 Aceptado: 23/05/2025

Nota 1: La Revista Vasca de Gestión de Personas y Organizaciones Públicas es consciente de que este trabajo constituye una versión más extensa y desarrollada del trabajo publicado en el n.º 13 de la revista *El Consultor de los Ayuntamientos*, monográfico del mes de abril de 2025, titulado «Transformación digital y derechos digitales de naturaleza laboral del empleo público local». Su Consejo de Redacción considera muy valiosa la aportación de la autora en esta versión extendida sobre un tema actual e importante, cuya comprensión profunda satisface este trabajo.

Nota 2: En la redacción del texto se ha procurado garantizar una visión inclusiva del lenguaje. No obstante, en aras a facilitar la lectura, en determinados casos cuando se utiliza el masculino como genérico, por ejemplo, en el caso de **ciudadanos, los empleados públicos, funcionarios**, se quiere decir ciudadanía, personal empleado público, el funcionariado.

Laburpena: Lan honen helburua da eraldaketa teknologikoek eta langileen kudeaketan adimen artifizialeko sistemak erabiltzeak enplegatu publikoen eskubideetan izan dezaketen eraginaren lehen hurbilketa bat egitea. Gure ordenamendu juridikoak oso apalki erreakzionatu du fenomeno berri horien aurrean; behar besteko ez, eta berandu. Eskubide batzuk aro digital berrira egokituz erantzun du, hala nola deskonexio digitalerako eskubidea eta intimitaterako oinarrizko eskubidea mamituz —Administrazioak bideozaintza edo geolokalizazioko sistemak erabiltzeari aurre egiteko edo beren eginkizunak bete ditzaten enplegatuen eskura gailu digitalak jartzeari aurre egiteko—. Lan-inguruneko «eskubide digital» deritzenak dira, hain zuzen, eta 2018an sartu ziren, Enplegatu Publikoaren Oinarrizko Estatuaren 14. artikuluaren j) bis letra gehitu zenean. Hala ere, eskubide-esparru hori birpentsatu egin behar da errealitate berrira egokitzeko, eta, bereziki, pertsonen kudeaketan adimen artifiziala erabiltzeak planteatzen dituen erronka berrietara egokitzeko. Eskubide Digitalen Gutuna 2021ean onartu zuen gobernuak, eta arauemailea ez izan arren, orientabide garrantzitsuak ematen dizkio legegileari.
Gako-hitzak: algoritmoak, datu biometrikoak, eskubide digitalak, intimitaterako eskubidea adimen artifiziala.

Abstract: The purpose of this paper is none other than to make a first approximation to the impact that technological transformations and the use of artificial intelligence (AI) systems in personnel management may have on the rights of public employees. Our legal system has only reacted very modestly to these new phenomena and has done so insufficiently and belatedly. It has done so by adapting some rights to the new digital era, such as the right to digital disconnection and the fundamental right to privacy when the administration uses video surveillance or geolocation systems, or when it makes digital devices available to its employees for the performance of their duties. These are the so-called 'digital rights' in the work environment that were introduced in 2018 with the addition of letter j.bis) to art. 14 of the Basic Statute of the Public Employee. However, this framework of rights needs to be reworked to adapt it to the new reality and, in particular, to the new challenges posed by the use of AI in people management. The Charter of Digital Rights, approved by the Government in 2021, although lacking normative value, provides the legislator with important guidance in this respect.
Keywords: algorithms, artificial Intelligence (AI), biometric data, digital rights, right to privacy.

Resumen: El objeto de este trabajo no es otro que realizar una primera aproximación al impacto que las transformaciones tecnológicas y el uso de los sistemas de inteligencia artificial (IA) en la gestión del personal pueden tener en los derechos del empleado público. Nuestro ordenamiento jurídico ha reaccionado solo muy modestamente ante estos nuevos fenómenos y de forma insuficiente y tardía. Y lo ha hecho adaptando algunos derechos a la nueva era digital, tal como sucede con el derecho a la desconexión digital y con el derecho fundamental a la intimidad frente al uso por parte de la Administración de sistemas de videovigilancia, de geolocalización o cuando pone a disposición de sus empleados dispositivos digitales para el cumplimiento de sus funciones. Son los llamados «derechos digitales» en el entorno laboral que se introdujeron en el año 2018 al añadir la letra j.bis) al art. 14 del Estatuto Básico del Empleado Público. Sin embargo, este marco de derechos debe ser repesando para acomodarlo a la nueva realidad y, de modo especial, a los nuevos retos que plantea el uso de la IA en la gestión de personas. La Carta de Derechos Digitales, aprobada por el Gobierno en el año 2021, aunque carece de valor normativo, proporciona al legislador importantes orientaciones al respecto1.
Palabras clave: algoritmos, datos biométricos, derecho a la intimidad, derechos digitales, Inteligencia Artificial (IA).

Sumario:

1. Introducción: las transformaciones tecnológicas en el empleo público

La utilización de las tecnologías en la Administración no es un fenómeno nuevo. Hace más de veinte años que la Comisión Europea definió la llamada «Administración electrónica» (*eGovernment)* como aquella Administración que se proponía utilizar las tecnologías de la información y la comunicación (TICs) para mejorar la calidad y accesibilidad de los servicios públicos, reducir los costes a las empresas y conseguir un sector público más abierto, transparente y más comprensibles para los ciudadanos[2]. El impacto más inmediato que tuvieron estas tecnologías fue permitir a la Administración usar y conectar datos, así como sustituir el papel por los procedimientos electrónicos o telemáticos. Las relaciones electrónicas entre la Administración y sus empleados públicos son ya una realidad en todas las Administraciones públicas al ser una obligación legal prevista en el art. 14.2.e) de la *Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas* (Cortés Abad, 2025; Fondevila Antolín, 2021).

Ahora bien, cuando se habla de la transformación tecnológica —e incluso algorítmica— de la Administración se quiere hacer referencia a un fenómeno mucho más amplio y complejo, a la utilización de las nuevas tecnologías de forma importante, innovadora y disruptiva, así como al uso intenso de datos y de algoritmos en el funcionamiento de la Administración y en la gestión de los empleados públicos. La IA es una parte importante de estas tecnologías de la información y conocimiento que implica el uso de algoritmos y modelos matemáticos que permiten a las máquinas realizar tareas que requieren inteligencia humana, como el aprendizaje, el razonamiento y la toma de decisiones. Estas capacidades se desarrollan gracias a la computación avanzada, el procesamiento de datos y las redes. A diferencia de la llamada Administración «electrónica», que ha consistido básicamente en la sustitución del papel por medios electrónicos y en la automatización de algunas fases de los procedimientos administrativos, la llamada Administración digital o Administración algorítmica supone avanzar todavía más en la utilización de las herramientas tecnológicas y hacerlo, asimismo, de forma intensiva y disruptiva (Gamero Casado, 2022). Como expresa el Libro Blanco sobre Inteligencia Artificial de la Comisión Europea, la inteligencia artificial es una combinación de tecnologías que agrupa datos, algoritmos[3] y capacidad informática (Ortiz de Zárate Alcarazo y Guevara Gómez, 2021). Los avances en computación y la creciente disponibilidad de datos explican el crecimiento tan importante que se está produciendo de la IA, aunque su uso conlleva también una serie de riesgos potenciales, como la opacidad en la toma de decisiones, sesgos, errores, discriminación de género o de otro tipo, la intromisión en nuestras vidas privadas o su uso con fines delictivos[4].

El fenómeno no es sencillo de abordar jurídicamente. Puede incidir de modo importante en la dignidad humana y en el derecho a la intimidad y a la protección de datos. Puede socavar los derechos fundamentales de los empleados públicos. Por ello, no solo debe ir acompañado de un proceso de cambios organizativos y de gestión de las personas, sino también de una importante reflexión sobre los derechos fundamentales y laborales de los empleados públicos que se van a ver afectados por este nuevo entorno laboral cada vez más digitalizado y afectado por la utilización de sistemas algorítmicos. El Derecho ha de guiar y dirigir estos avances tecnológicos para que dicha transición se haga de una forma plenamente respetuosa con los derechos del empleado público.

Núm. 28 zk./2025. Págs. 46-74 or.
ISSN: 2173-6405 e-ISSN: 2531-2103

Estas transformaciones digitales podrían facilitar mucho la gestión de las personas en la Administración, reducen el tiempo en la ejecución de tareas, pueden mejorar el rendimiento de los empleados y, en consecuencia, redundan en una mayor eficacia y eficiencia de la Administración. No obstante, implican también importantes riesgos. Y no me refiero solo a los posibles errores en la utilización de los datos, que constituyen la materia prima de la IA, ni a los sesgos, sino también y de modo importante a la incidencia que pueden tener en los derechos fundamentales de los empleados. La utilización de la tecnología está teniendo un impacto muy importante en cuanto a las posibilidades que tiene la Administración de vigilar y controlar que sus empleados cumplen adecuadamente con sus funciones y tareas. Puede videovigilarlos, usar sistemas de geolocalización o de grabación de sonidos y puede acceder al contenido de sus ordenadores y de los demás dispositivos tecnológicos que haya puesto a su disposición, lo que afecta de modo directo a sus derechos fundamentales. Estos dispositivos informáticos permiten usar cuentas de correo electrónico institucionales, almacenar datos personales, como pueden ser agendas de contactos, datos de cuentas del banco, fotografías o incluso datos de especial sensibilidad como son los datos relativos a la salud. Ya tenemos algunos ejemplos de ello e incluso de la imposición de sanciones de apercibimiento a algunas Administraciones públicas por el acceso ilegítimo a todos estos datos con menoscabo de los derechos fundamentales de sus funcionarios (STS de 7 de octubre de 2024, Sala contencioso-administrativa, Sección 3.ª).

De esta faceta, de los derechos de los empleados públicos ante los avances de las nuevas posibilidades de «supervisión digital» de la Administración me quiero ocupar básicamente en este trabajo por ser la faceta que más se ha desarrollado hasta el momento presente, a pesar de que el TREBEP no contiene ninguna referencia expresa a la atribución de semejantes potestades de intervención de la Administración en la esfera jurídica de sus empleados. En este sentido, como veremos, la jurisdicción contenciosa ha asumido en bloque la prolija doctrina social que se ha elaborado durante muchos años a partir de las poderes que el art. 20.3 del *Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores* (ET) atribuye al empresario para adoptar «las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales».

La Administración, efectivamente, está facultada para acceder a las cuentas de correo institucional de sus empleados y técnicamente podría conocer qué páginas Web visitan en el horario de trabajo o incluso fuera del horario laboral cuando permite que sus empleados puedan hacer también un uso privado de los ordenadores. Podría supervisar el estado técnico en el que se encuentran estos dispositivos y la utilización que se hace también de los teléfonos fijos y móviles, de sus cuentas de correo electrónico institucional o de la utilización que hacen de las distintas plataformas de colaboración que permiten a los empleados colaborar y trabajar en equipo a través de videollamadas, reuniones en línea, mensajería instantánea y audios, entre otras muchas funciones (Rodríguez Escanciano, 2018).

Como ya ha resaltado la doctrina laboralista, los avances tecnológicos han convertido al empleador público en una especie de «gran hermano» que todo lo ve. Si parafraseamos a Mercader Uguina y trasladamos la terminología laboral al ámbito administrativo, podríamos decir que nos encontramos ante una perspectiva nueva de la Administración en su relación con los empleados públicos, ante una Administración panóptica que puede utilizar las nuevas tecnologías para ver todo lo que sus empleados hacen y para probar cómodamente la comisión de infracciones administrativas y abrir expedientes disciplinarios (Mercader Uguina, 2001 y Rodríguez Fernández, L. 2023). Al mismo tiempo, los avances en los sistemas de IA y su utilización en la gestión de personal nos sitúan ante una nueva faceta de la Administración sobre la que todavía no hemos tenido tiempo de reflexionar pausadamente. Esta nueva tecnología dota a la Administración de importantes y nuevos poderes «computacionales» o de dirección algorítmica, que le permiten conocer enormes cantidades de datos sobre sus empleados, procesarlos, elaborar perfiles e incluso adoptar decisiones de gestión de personal mediante sistemas de IA, en lo que ya se ha denominado «gestión algorítmica» del empleo (Todolí Signes, 2022).

Esta nueva faceta todavía está en construcción. Nuestro ordenamiento jurídico aún no ha adaptado convenientemente el marco de los derechos laborales de los empleados públicos a la complejidad de los nuevos retos que plantea este nuevo entorno laboral digitalizado, aunque ha dado pasos muy importantes. La disposición final 14 de la *Ley Orgánica 3/2018, de 5 de diciembre de Protección de Datos Personales y garantía de los derechos digitales*, vino a añadir nuevos «derechos digitales» al listado de derechos individuales de los empleados públicos que recoge el art. 14 del *Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público* (TREBEP). Asimismo, sus artículos 89 y siguientes han atribuido expresamente a la Administración nuevas potestades de vigilancia y supervisión tecnológica de sus empleados públicos. Han dotado de contenido

sustantivo a estos derechos y han establecido las notas básicas de su régimen jurídico y de sus garantías. En realidad, se trata básicamente de una adaptación del derecho fundamental a la intimidad y del derecho a la protección de datos (aunque este no se mencione expresamente) al entorno laboral para dar respuesta a estas nuevas realidades tecnológicas. Sobre esta faceta centraré mi trabajo, aunque no sin antes realizar algunas primeras reflexiones sobre el impacto de la IA en los derechos de los empleados públicos.

2. El uso de la IA en los procesos de gestión del personal y sus nuevos desafíos

De todas las tecnologías, la IA representa una de las revoluciones más trascendentales de los últimos tiempos, dado que por sus características tiene la capacidad de abordar los desafíos más complejos del mundo contemporáneo[5]. Los sistemas de IA son aquellos sistemas capaces de procesar una ingente cantidad de datos e información de una manera que se asemeja a un comportamiento inteligente, abarcando generalmente aspectos de razonamiento, aprendizaje, percepción, predicción, planificación o control[6]. Tal como se recoge en el art. 3.1 del Reglamento de Inteligencia Artificial (RIA), *Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo aprobado el 13 de junio de 2024*, un «sistema de IA» es un sistema basado en una máquina que está diseñado para funcionar con distintos niveles de autonomía y que puede mostrar capacidad de adaptación tras el despliegue, y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales.

A diferencia de lo que ocurría con otras tecnologías de la información anteriores, la IA se caracteriza porque es capaz de aprender y actuar con cierto grado de autonomía. Es decir, estos sistemas de IA pueden identificar patrones y descubrir nueva información sin la asistencia de un humano, así como predecir eventos futuros. Pueden, por sí mismos, actuar con autonomía y tomar decisiones, que no están preprogramadas (Custers, 2022). A partir de sistemas basados en la programación humana y de esquemas de decisión predeterminados, se crean sistemas autónomos que son capaces de aprender y establecer las propias pautas de acción sobre la base del análisis de un gran volumen de datos. Por ello, su aplicación en el ámbito de la Administración y, más en concreto, en la gestión de su personal, presenta, nuevos desafíos, tanto para la Administración como para sus empleados.

Esta capacidad de aprender a partir de la experiencia y de los datos es lo que le ha valido el apodo de «inteligencia» a esta tecnología, en la medida en que se le atribuye capacidad para reproducir y simular capacidades hasta ahora solo asociadas a los seres humanos utilizando distintas técnicas que pueden usar los algoritmos como son el *machine learning,* el *deep learning* o las *neural networks*, entre otras muchas, que se basan en el reconocimiento de patrones para hacer inferencias que le permitan derivar y crear nuevas reglas que, a su vez, permiten nuevamente evaluar su entorno usando datos y tomar decisiones procesando datos (Ortiz de Zárate Alcarazo y Guevara Gómez 2021).

La Administración acumula una cantidad ingente de datos sobre sus propios empleados públicos que pueden ser muy valiosos, en la medida en que estos datos son la materia prima de los sistemas de IA y su adecuado análisis puede ser utilizado para adoptar decisiones sobre política de personal[7]. De ahí la interacción continua que existe entre el RIA y *el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE* (Reglamento general de protección de datos, RGPD) y la necesidad de tener presente, en todo momento, los derechos digitales que proclama el reglamento europeo de protección de datos. En este sentido, es preciso recordar que el art. 71 del TREBEP obliga a cada Administración a constituir un Registro en el que han de inscribirse los datos relativos a su personal e incluso pueden contar también con la información agregada del resto del personal de su respectivo sector público. El nuevo régimen proclama el principio de la gestión integrada de recursos humanos y permite que, a través de convenios de Conferencia Sectorial, puedan establecerse criterios que permitan el intercambio homogéneo de la información entre las distintas Administraciones públicas.

Todos estos datos, sin duda, abren un abanico importante de posibilidades de explotación a través de sistemas de IA, especialmente si se usa un sistema de IA generativa que esté diseñado para crear contenido nuevo a partir de datos existentes[8]. Como se ha señalado, las características tecnológicas que gobiernan la IA, como el *Machine Learning*, el *Deep Learning*, el

Text Mining o el *Entity Recognition*[9], pueden ser aplicadas a los datos contenidos en el Registro y a los curriculums vitae de los funcionarios. Las técnicas implementadas por estos avances tecnológicos se podrían enfocar predominantemente en las actividades de selección de personal que involucran tareas repetitivas y que manejan grandes volúmenes de datos. Ejemplos de estas actividades incluyen la revisión y filtrado de currículums, el contacto con candidatos, la realización de entrevistas y la elaboración de informes finales[10].

En todo caso, la utilización del Big Data y de sistemas de IA tiene un enorme potencial para la gestión del personal. Facilitan las funciones de las unidades responsables de los Recursos Humanos y pueden aligerar notablemente la carga de trabajo de los empleados públicos. La utilización de estos sistemas de IA convierte automáticamente a la Administración en «responsable del despliegue» (art. 3 del RIA) y, en consecuencia, debe someterse al régimen de cautelas y garantías que prevé dicho reglamento cuando pretenda utilizar esta tecnología en la gestión de las personas. El RIA pretende un desarrollo de los sistemas de IA que estén verdaderamente centrados en el ser humano y que respeten los derechos fundamentales de las personas. Establece como uno de sus principales objetivos garantizar «un elevado nivel de protección de la salud, la seguridad y los derechos fundamentales consagrados en la Carta» (art. 1 RIA) y, en línea con el enfoque basado en el riesgo adoptado por el legislador de la UE, la evaluación del impacto de la IA en los derechos fundamentales se incluye en todos los procedimientos de gestión de riesgos establecidos por el Reglamento, garantizando también una evaluación específica del impacto que el sistema de IA que se pretenda diseñar, desarrollar o desplegar vaya a tener en los derechos fundamentales con arreglo al artículo 27 del RIA[11].

2.1. **Sus potencialidades**

La transformación digital de la Administración abarca fenómenos muy complejos y dispares entre sí que afectan al empleo público. La IA puede tener aplicaciones infinitas en el ámbito de la gestión de las personas empleadas en las Administraciones públicas. Prácticamente todas las instituciones del empleo público podrían en un futuro verse afectadas por estos avances tecnológicos. Sin duda, hay que incluir la toma de decisiones de manera completamente autónoma, en las denominadas actuaciones administrativas automatizadas, que se caracterizan porque prescinden directamente de la intervención humana y son realizadas íntegramente a través de medios electrónicos, sin la participación del funcionario[12]. Forma parte de este fenómeno tecnológico la llamada robotización de puestos de trabajo a partir de la automatización de determinados procesos rutinarios y repetitivos. La automatización de los procedimientos administrativos —o de determinados trámites— y la utilización de sistemas de IA permitirán que las máquinas realicen muchas de las tareas que realizan los empleados públicos, especialmente aquellas que respondan a un patrón, sean repetitivas y rutinarias, no requieran de la creatividad, de la realización de procesos interpretativos o de la toma de decisiones discrecionales (Gorriti Bontigui, 2018; Jiménez Asensio 2019; Ramió Matas, 2018; Padilla Ruíz, 2023). Según los estudios realizados en el Instituto Nacional de Administración Pública (INAP), el impacto de la IA en la función pública deberá conllevar un rediseño de los puestos de trabajo y de las estructuras organizativas, que tenderán a ser más planas y menos burocratizadas y habrá que pensar cómo captar talento experto en datos y potenciar el carácter multidisciplinar de los perfiles (tecno-jurídico-social). Habrá que definir las funciones propias de la reserva de «humanidad[13]» que no son externalizables a algoritmos, toda vez que el art. 22 del *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE* (Reglamento general de protección de datos, RGPD), consagra el derecho de las personas a no ser objeto de una decisión administrativa automatizada (incluida la elaboración de perfiles) cuando ello les afecte[14].

La gestión y explotación de los datos, la aplicación de técnicas de *Big Data* en el ámbito de los recursos humanos (*People Analytics),* es también una importante manifestación de esta transformación digital. Instrumento valioso podría ser la elaboración de perfiles, que se define en el art. 4.4 del RGPD como toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física[15]. A través de estas predicciones, técnicamente sería posible adoptar decisiones para gestionar los procesos de provisión de puestos de trabajo, diseñar itinerarios de carrera profesional u ordenar la movilidad del personal. Sin embargo, pueden menoscabar los derechos fundamentales a la intimidad y a la protección de datos de los empleados públicos[16].

Los avances tecnológicos permitirían procesar la ingente cantidad de datos que la Administración po-

see de sus empleados y utilizarlos a través de la elaboración de algoritmos para adoptar decisiones que pueden afectar a las distintas instituciones del empleo público, como la evaluación de desempeño, la carrera, la movilidad, la provisión de puestos de trabajo o la determinación de los componentes retributivos relacionados con el rendimiento y desempeño de sus empleados (Galindo Caldés, 2023). En todo caso, la utilización de la IA va a constituir siempre una importante «ayuda funcional» del empleado público en el desempeño de sus funciones, lo que le permitirá ahorrar tiempo, ser más productivo y eficiente (Almonacid Lamelas, 2024). Puede contribuir a su mejor formación, mejorando su experiencia profesional y reteniendo el talento dentro de la Administración. Puede facilitar su trabajo proporcionando respuestas rápidas a consultas frecuentes e incluso ayudar en la resolución de problemas. Pensemos, por ejemplo, en la creación de un sistema que permita chatear fácilmente con los empleados para responder a sus preguntas, darles recomendaciones de desarrollo profesional, sugerirles cursos de formación o darles información sobre oportunidades de carrera y promoción profesional dentro de su Administración o incluso de movilidad hacia otras Administraciones públicas. De esta manera puede aumentar su grado de satisfacción, su motivación y, con ello, su grado de imbricación con los intereses de la organización administrativa. La IA puede ofrecer a los empleados de forma automatizada recomendaciones personalizadas sobre oportunidades de desarrollo, programas de formación y opciones de carrera. En ese sentido, es preciso tener en cuenta que el propio RIA consagra el deber de alfabetización en inteligencia artificial por parte de la Administración (Todolí Signes, 2025). Esta obligación debería tener como correlato el consiguiente derecho de los empleados públicos a dicha alfabetización (art. 4 y considerandos números 20 y 91 del RIA). En todo caso, estos sistemas podrían facilitar la identificación de las necesidades formativas de los empleados y facilitar el diseño de itinerarios formativos e itinerarios de carrera profesional, a través del desarrollo de competencias y habilidades personalizadas que permitan adaptar convenientemente los intereses del empleado público con las necesidades de la organización administrativa.

Desde un punto de vista estrictamente técnico, la IA podría permitir a la Administración seleccionar fácilmente a su personal evaluando candidatos, analizando y filtrando solicitudes o tomando directamente decisiones sobre la gestión de las personas. Podría gestionar todos los datos que acumula de sus empleados públicos, elaborar perfiles de todo su personal, recopilar y usar sus datos biométricos y hasta incluso reconocer y gestionar sus emociones y expresiones faciales para adoptar decisiones sobre la provisión de puestos de trabajo, situando, por ejemplo, en los puestos de atención a las personas a aquellos empleados que se muestren siempre contentos, que sean más simpáticos, que no tengan mal humor y que posean mayores dosis de empatía. La tecnología lo permite. Otra cosa es que ello sea compatible con los principios de igualdad, mérito y capacidad que han de inspirar las distintas instituciones del empleo público y que ello sea además oportuno en virtud de los grandes riesgos que supondría de discriminación algorítmica, de cometer errores y del impacto que posiblemente tendría en los derechos fundamentales de las personas y, en particular, de los que ya reúnen la condición de empleado público.

Estas tecnologías, sin duda, podrían ser muy interesantes para el control del cumplimiento de los horarios de los empleados, de sus obligaciones y, sobre todo, del rendimiento de su desempeño. Permitirían avanzar hacia una Administración panóptica que fácilmente ve todo lo que su empleado hace. La Administración podría utilizar programas *in accounting* que permiten un control computerizado de la actividad que realizan los empleados que usan ordenadores en su trabajo y que permiten controlar el número de tecleos por minuto, el número de operaciones que realizan, el número de expedientes que tramitan, los errores que cometen, el tiempo que pasan delante del ordenador, el número y la frecuencia de las pausas que realizan en el trabajo, etc. Como señala Jesús Mercader, ya se conocen incluso algunas experiencias en Bélgica de empresas privadas que han implantado a sus empleados un microchip bajo la piel que permite un control total del trabajador y que funciona como una llave de identificación para acceder al ordenador y abrir las puertas (Mercader Uguina, 2022).

Los sistemas de IA permitirían, además, comparar toda esta información con la generada por los demás empleados públicos, posibilitando, en definitiva, la evaluación del desempeño y una gestión de la diferencia en el ámbito del empleo público. En la medida en que la IA puede analizar datos en tiempo real puede ser utilizada para facilitar también la evaluación de desempeño como herramienta que permite medir y valorar la conducta profesional, el rendimiento y el logro de resultados del empleado público (art. 20 del TREBEP). Estas tecnologías permiten analizar importantes volúmenes de datos sobre el desempeño de sus empleados públicos e identificar patrones en su rendimiento, proporcionando a los responsables de los recursos humanos y a los superiores jerárquicos información relevante para asignar tareas, funciones y proyectos, así como para tomar decisiones estratégicas en la estructura organizativa. En este sentido, los sistemas de IA permiten incluso proporcio-

nar *feedback* en tiempo real sobre el progreso de un empleado, recibiendo así una retroalimentación inmediata sobre el desempeño de sus tareas que puede contribuir a mejorar su desempeño en el puesto de trabajo. Su utilización, no obstante, requiere importantes cautelas, toda vez que nuestra legislación exige que los sistemas de evaluación del desempeño se adecúen, en todo caso, a criterios de transparencia, objetividad, imparcialidad y no discriminación, lo que apunta a la necesidad de garantizar el derecho del empleado a la transparencia en el uso de los algoritmos e información sobre su diseño y el código de fuente utilizado, así como la necesidad de garantizar que no se producen discriminaciones por sesgos.

Más incisivos pueden resultar todavía los sistemas de IA que usan datos biométricos. Los datos biométricos son datos personales obtenidos a partir de un tratamiento técnico específico de las características físicas, fisiológicas o conductuales de una persona física[17]. Dichos datos permiten confirmar la identificación única de dicha persona, tal como sucede con las imágenes faciales o con los datos dactiloscópicos (huellas dactilares). El sistema permite comparar la plantilla de la imagen facial de una persona con otras muchas plantillas almacenadas en una base de datos para averiguar si su imagen está almacenada en ella. La correspondencia entre dos plantillas concretas permite la autenticación o verificación de una persona, esto es, que es quien dice ser. Estos datos biométricos permitirían técnicamente su utilización en múltiples facetas de la gestión del personal. Con ellos es posible realizar un control exhaustivo de los horarios y de la presencia del empleado en el puesto de trabajo, pero es también posible realizar una clasificación biométrica de las personas por raza u orientación política, religiosa o sexual o realizar la puntuación de individuos o grupos basándose en comportamiento sociales o rasgos personales como método de selección. Como ha reconocido el propio Ministro de Transformación Digital y Función Pública, un sistema de categorización facial biométrica es incluso capaz de deducir la orientación política o sexual de un individuo mediante análisis de sus fotos en redes sociales[18]. Por ello, no es de extrañar que el propio RIA haya trazado algunas líneas rojas y haya prohibido la utilización de algunos de estos sistemas en el entorno laboral.

2.2. Los riesgos de los datos y algoritmos. Su impacto en los derechos fundamentales del empleado público

Estas tecnologías son especialmente peligrosas, ya no solo por los errores que pueden producir y los sesgos que puedan contener, sino también por el notable impacto que pueden tener en los derechos fundamentales de sus empleados, por la invasión de su intimidad y por el riesgo de discriminación que conllevan.

La utilización de la IA en el empleo público supone un aumento de los riesgos de error o discriminación y puede contener sesgos. El sesgo de IA en el ámbito del empleo público es una diferencia sistemática en el tratamiento de ciertas personas o grupos, por ejemplo, estereotipos, prejuicios o favoritismos, en comparación con otros mediante algoritmos de IA. Y ello porque el procesamiento digital de los datos de los empleados para la toma de decisiones es un proceso muy delicado, que debe realizarse concienzudamente y ser vigilado de cerca por personas que puedan detectar sesgos o anomalías en el procedimiento y corregir lo que proceda (Fernández de la Cigoña Fraga, 2022). Como ha señalado el Comité Europeo de Protección de Datos (CEPD), si los datos se tratan sistemáticamente sin el conocimiento de los interesados, es probable que se genere una sensación general de vigilancia constante, lo que puede dar lugar a efectos disuasorios en relación con algunos o todos los derechos fundamentales afectados, como la dignidad humana en virtud del artículo 1 de la Carta, la libertad de pensamiento, de conciencia y de religión en virtud del artículo 10 de la Carta, la libertad de expresión en virtud del artículo 11 de la Carta y la libertad de reunión y de asociación en virtud del artículo 12 de la Carta[19]. De hecho, se ha propuesto que la utilización de sistemas de IA vaya acompañada de una importante reflexión sobre la necesidad de instaurar procedimientos de vigilancia algorítmica -que evite los errores y los sesgos- y de la creación de un nuevo cuerpo de «inspectores algorítmicos»[20].

Cuando afecta al empleo público las cautelas han de ser todavía mayores dada la falta de libertad de la Administración para adoptar decisiones de gestión de personal, toda vez que todas sus decisiones obedecen a procedimientos formalizados y plenamente respetuosos con los principios constitucionales de igualdad, mérito y capacidad. Como se ha dicho, un empleado es algo más complejo que los datos que genera y existe el riesgo de que los algoritmos aplicados a los procesos de selección puedan descartar personas con mucho talento (Fernández de la Cigoña Fraga, 2022). Las discriminaciones pueden surgir por los datos utilizados, pues los algoritmos son tan precisos como lo sean los datos que manejan y, con frecuencia, los datos no son de calidad, contienen errores o son imperfectos. Los sesgos pueden haber sido introducidos, voluntariamente o involuntariamente, por los diseñadores, por los usuarios de los algoritmos o pueden surgir también del aprendizaje que haga un algoritmo a partir de datos sesgados (Cerrillo I Martínez, 2019).

La utilización de los sistemas de IA puede impactar de modo considerable en los derechos fundamentales de los empleados públicos, especialmente en su derecho a la intimidad (art. 18.1 CE), en su derecho a la igualdad o no discriminación (art. 14, art. 23.2 y art. 103.3 CE) y en su derecho a la protección de datos (art. 18.4 CE). Incluso el derecho fundamental a la integridad física podría verse menoscabado si en un futuro remoto se permitiera la utilización de algunas tecnologías más extremas como la implantación de microchips bajo la piel del empleado (art. 16 CE). La utilización de datos biométricos puede conllevar también la deducción de múltiples datos de salud del empleado. Como ha señalado la Agencia Española de Protección de Datos (AEPD), en sistemas biométricos basados en el reconocimiento facial se pueden tratar datos que permiten extraer información de salud. Algunos sistemas de identificación mediante huella dactilar permiten el registro de parámetros como la temperatura o la presión sanguínea, mientras que los análisis biométricos de la voz humana pueden recoger más de cien parámetros distintos de salud que detectan problemas físicos o psicológicos, entre otros[21]. Es decir, la utilización de sistemas de control biométrico para vigilar el cumplimiento de los horarios puede impactar de un modo muy significativo en sus derechos sanitarios e invadir su derecho a la intimidad, proclamado específicamente en el art. 7 de la *Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica*, que instituye el derecho de toda persona a que se respete el carácter confidencial de los datos referentes a su salud y a que nadie pueda acceder a ellos sin previa autorización amparada por la Ley.

La Comisión Europea, en el Libro Blanco sobre Inteligencia Artificial ya alertaba de que su uso puede afectar a los valores sobre los que se fundamenta la propia Unión Europea y provocar una conculcación de derechos fundamentales, como la libertad de expresión, la libertad de reunión, la dignidad humana, la ausencia de discriminación por razón de sexo, raza u origen étnico, religión o credo, discapacidad, edad u orientación sexual. Asimismo, la falta de transparencia de la IA hace difícil detectar y demostrar los posibles incumplimientos de la legislación, especialmente las disposiciones legales que protegen estos derechos fundamentales. Si seguimos en este punto las advertencias de dicho Libro Blanco podemos hacernos una idea de algunos de los riesgos más significativos que pueden impactar en el ámbito del empleo público y en la posición jurídica de sus empleados.

Efectivamente, no son pocos los problemas y los riesgos que plantea la utilización de esta tecnología. Incrementa notablemente la posibilidad de que pueda invadirse el derecho a la intimidad del empleado público. Puedan elaborarse perfiles de las personas y hacerse un seguimiento y un análisis de sus costumbres y patrones de comportamiento. Existe el riesgo de que, incumpliendo las normas de protección de datos, las autoridades puedan recurrir a la IA para la vigilancia masiva o para observar cómo se comportan sus empleados. Sobre este aspecto ya tenemos una regulación mínima en el art. 14.j.bis) del TREBEP, pero está centrada exclusiva y expresamente en el uso de cámaras de videovigilancia. Y, sobre todo, es preciso analizar con mucho mayor detenimiento los efectos que puede tener la utilización de estos sistemas en los principios rectores del empleo público, esto es, en el principio de igualdad, mérito y capacidad.

El tratamiento de los datos, el modo en el que se diseñan las aplicaciones y la envergadura de la intervención humana pueden afectar al derecho a la intimidad y al derecho a la protección de los datos personales. Al analizar grandes cantidades de datos y detectar la conexión existente entre ellos, la IA también puede utilizarse para rastrear y desanonimizar datos relativos a personas, y generar así nuevos riesgos en torno a la protección de los datos personales con relación a conjuntos de datos que, en sí mismos, no contienen datos personales. Puede suceder también que el sistema de IA «aprenda» mientras está funcionando. En tales casos, cuando los resultados no puedan preverse ni anticiparse en la fase de diseño, los riesgos no se deberán a fallos en el diseño original del sistema, sino más bien a las repercusiones prácticas de las correlaciones o de los modelos que reconozca el sistema en un gran conjunto de datos[22].

Las nuevas tecnologías han supuesto un notable refuerzo de las posibilidades de vigilancia y control que tiene la Administración sobre la actividad que realizan sus empleados. En el ámbito de las relaciones laborales existe un importante riesgo de que se vean lesionados los derechos fundamentales cuando se ejerce el poder de vigilancia y control sobre el uso que el empleado hace de las herramientas informáticas puestas a su disposición. Son varios los derechos fundamentales que pueden verse menoscabados, el derecho a la intimidad y el derecho al secreto de las comunicaciones si el control afecta, por ejemplo, a los correos que escribe o recibe el empleado en su cuenta institucional (art. 18.1 y 18.2), así como el derecho a la protección de datos que consagra el art. 18.4 de la Constitución cuando se utilizan mecanismos de grabación de imágenes o de sonidos. Este derecho abarca la protección de la amplia diversidad de datos que pueden guardarse en un sistema informático o dispositivo, pues estos son capaces de almacenar y gestionar un gran número de datos, además de po-

tenciar las comunicaciones entre las personas. Por ello, cualquier medida invasiva en los terminales habrá de realizarse con la máxima prudencia. En la línea de la STC 173/2011, de 7 de noviembre. F.J. 3.º los datos obtenidos en un ordenador pueden quizás considerarse irrelevantes aisladamente; sin embargo, si se analizan en conjunto se puede obtener un perfil altamente descriptivo de la personalidad de su titular que afecta a la individualidad de la persona y por ello, ha de resultar digno de protección frente a terceros y a poderes públicos (STS de 29 de septiembre de 2023, Sala de lo Contencioso-Administrativo, Sección Segunda, núm. 1207/2023).

La doctrina del Tribunal Constitucional se ha pronunciado en numerosas ocasiones sobre las facultades de vigilancia y supervisión que tiene el empresario respecto de sus trabajadores, pero sus planteamientos son igualmente aplicables al ámbito funcionarial. En principio, hay que entender que el empleador no queda apoderado para llevar a cabo, so pretexto de las facultades de vigilancia y control que le confiere el art. 20.3 del ET, intromisiones ilegítimas en la intimidad de sus empleados en los centros de trabajo (STC 186/2000, de 10 de julio). La existencia de un contrato de trabajo o de un nombramiento funcionarial no priva al empleado de sus derechos fundamentales. Los equilibrios y limitaciones recíprocos que se derivan para ambas partes del contrato de trabajo suponen que también las facultades organizativas empresariales se encuentran limitadas por los derechos fundamentales del trabajador, quedando obligado el empleador a respetar aquéllos (STC 292/1993, de 18 de octubre, FJ 4). El ejercicio de las facultades organizativas y disciplinarias del empleador no puede servir en ningún caso a la producción de resultados inconstitucionales, lesivos de los derechos fundamentales del trabajador (así, entre otras, SSTC 94/1984, de 16 de octubre, 108/1989, de 8 de junio, 171/1989, de 19 de octubre, 123/1992, de 28 de septiembre, 134/1994, de 9 de mayo, y 173/1994, de 7 de junio). Por el contrario, dada la posición preeminente de los derechos fundamentales en nuestro ordenamiento, debe realizarse un equilibrio y una modulación de todos los intereses concurrentes, respetando los derechos fundamentales del empleado y, muy especialmente, el derecho a la intimidad personal que protege el art. 18.1 CE (STC 39/2016, de 3 de marzo y STS de 2 de febrero de 2017, Sala de lo Social).

En consecuencia, la existencia de una relación especial de sujeción entre el funcionario y la Administración o de un contrato de trabajo entre la persona empleada laboral y la Administración en la que presta sus servicios no anula los derechos fundamentales de estos empleados. Como ha subrayado la STC 12/2012, de 30 de enero, la existencia de un contrato de trabajo no supone una renuncia del trabajador a sus derechos como ciudadano y en el ámbito laboral se generan relaciones interpersonales, vínculos o actuaciones que pueden constituir también manifestaciones de la vida privada. La misma argumentación sería extensible al nombramiento de un funcionario público.

2.3. Las líneas rojas de la IA en la gestión de personas. Los sesgos

Siendo consciente de todos estos riesgos, el RIA ha trazado determinadas líneas rojas y ha prohibido directamente la utilización de algunos de estos sistemas de IA en el ámbito de las relaciones laborales y, por tanto, también en el ámbito de la Administración. En la medida en que los datos biométricos constituyen una categoría de datos personales sensibles los ha clasificado directamente como de alto riesgo y los ha sometido a un especial régimen jurídico para intentar amortiguar el impacto que pueden tener en los derechos fundamentales de los empleados públicos. Ha prohibido algunos sistemas de IA que utilizan datos biométricos en el ámbito de las relaciones laborales. Así sucede directamente con los que crean o amplían bases de datos de reconocimiento facial mediante la extracción no selectiva de imágenes faciales a partir de internet o de imágenes de circuito cerrado de televisión, que están prohibidas en el entorno laboral digitalizado, pues esas prácticas agravan el sentimiento de vigilancia masiva y pueden dar lugar a graves violaciones de los derechos fundamentales, incluido el derecho a la intimidad (considerando n.º 43 del RIA). Aunque los sistemas de identificación biométrica remota se clasifiquen como de alto riesgo por los riesgos que entrañan, se prohíben en el ámbito laboral. No se podrían usar sistemas de IA biométricos para la categorización de personas, así como los sistemas destinados a la identificación biométrica remota de las personas físicas, toda vez que sus imprecisiones técnicas pueden dar lugar a resultados sesgados y tener efectos discriminatorios en los empleados públicos, especialmente en lo que respecta a la edad, la etnia, la raza, el sexo o la discapacidad.

Lo mismo sucede con los sistemas de reconocimiento de emociones, que son sistemas de IA destinados a distinguir o deducir las emociones o las intenciones de las personas físicas a partir de sus datos biométricos (la felicidad, la tristeza, la indignación, la sorpresa, el asco, el apuro, el entusiasmo, la vergüenza, el desprecio, la satisfacción y la diversión, etc). Inferir emociones en centros de trabajo podría ser utilizado como método de evaluación o como criterio en una posible promoción, para la provisión de puestos o incluso para la apertura de un procedimiento disciplina-

rio o para un despido laboral. Ello explica que su utilización está también prohibida en el entorno laboral, y por tanto también y con mayor motivo en el ámbito del empleo en la Administración, no solo por las deficiencias de su base científica y fiabilidad, sino también por la incidencia que puede tener en el derecho a la intimidad y el derecho a la igualdad en el trato de los trabajadores (considerandos n.º 18 y 44 del RIA). Se han considerado escasamente fiables porque la expresión de las emociones varía de forma considerable entre culturas y situaciones, e incluso en una misma persona. Pueden tener resultados discriminatorios y pueden invadir los derechos y las libertades de las personas afectadas. Además, dado el desequilibrio de poder que se produce en el contexto laboral y el carácter intrusivo de estos sistemas de IA, su utilización podría dar lugar a un trato perjudicial o desfavorable de determinadas personas físicas o colectivos enteros. Ello explica que solo se permitan con fines estrictamente médicos o de seguridad y se prohíban para detectar el estado emocional de las personas en situaciones relacionadas con el lugar de trabajo y el ámbito educativo (considerando n.º 44 del RIA).

En principio, el reglamento excluye de esta prohibición los sistemas de IA destinados a la verificación biométrica, que incluyen la autenticación, cuyo único propósito es confirmar que una persona física concreta es quien dicha persona dice ser, así como confirmar la identidad de una persona física con la finalidad exclusiva de que tenga acceso a un servicio, desbloquee un dispositivo o tenga un acceso seguro a un local (considerando n.º 54 del RIA). Ello significa que, al no estar prohibidos por el RIA, podrían ser utilizados. No obstante, habría que analizar con mucho más detalle su impacto en nuestro sistema constitucional. La postura de nuestras autoridades en materia de protección de datos ha sido mucho más restrictiva respecto a la posibilidad de utilizar los sistemas biométricos para controlar la presencia del empleado público en su puesto de trabajo y su control horario por los graves riesgos que plantean. Después nos referiremos a ello.

En todo caso, la eventual utilización de sistemas de IA en la gestión del empleo público presenta el reto de hacer compatibles sus resultados con los principios de igualdad, mérito y capacidad. El problema es que los datos que alimentan los sistemas de IA pueden ser inexactos, incompletos o poco representativos. Pueden contener errores o pueden ser material sin importancia o estar mal etiquetados. Asimismo, los algoritmos pueden estar impregnados de sesgos. Los sistemas de IA no son neutros, a pesar de su aparente automaticidad, sino que pueden reflejar las preferencias, prioridades y prejuicios, conscientes o inconscientes, de sus creadores. En este sentido, los sistemas alimentados por datos masivos se exponen a la creación de bolsas de discriminación no solo presentes en los sesgos de los datos que alimentan el modelo y que acaban provocando su réplica al servir para el autoaprendizaje del propio sistema, el llamado aprendizaje automático (Asquerino Lampero, 2022).

Es cierto que la toma de decisiones de las personas responsables del empleo público no está tampoco exenta de error ni de subjetividades. En este sentido, la utilización de sistemas de IA y algoritmos se ha querido presentar como una oportunidad para tomar decisiones de forma matemáticamente objetiva y basadas exclusivamente en datos, en méritos, eliminando errores o prejuicios inconscientes por razón de sexo, género, edad, origen racial, apariencia física de las personas o diversidad funcional, pero, como señala Rodríguez Escanciano, esta pretendida neutralidad y objetividad es solo aparente. El diseño y despliegue de un algoritmo puede condicionar su presunta objetividad, lo que puede ocasionar, de forma voluntaria o involuntaria, discriminaciones y vulneraciones de derechos fundamentales de los empleados, atentando a los principios de igualdad y no discriminación (Rodríguez Escanciano, 2024). Es más, como se ha señalado, cada sesgo presente en el sistema algorítmico no solo afectará a una futura decisión discriminatoria sino que su engarce a través de las matemáticas hace que sus efectos adversos no solo se den para el caso concreto, sino que se pueden multiplicar y extrapolar exponencialmente a otros muchos supuestos, llegando a convertirse, a la postre, en una amenaza reforzada por su escalabilidad (Todolí Signes, 2023).

Efectivamente, en el caso de la IA, esta misma subjetividad puede tener efectos mucho más amplios si los datos que utiliza el algoritmo están viciados o contienen algún sesgo, bien en el propio diseño que se haya realizado del sistema de IA, bien en los datos de entrenamiento del algoritmo o bien en la validación y evolución del modelo. Los sesgos pueden afectar y discriminar a numerosas personas sin que existan mecanismos como los de control social que rigen el comportamiento humano. Todolí Signes (2023) lo explica de una forma muy gráfica, aunque referido al ámbito empresarial. «*Es posible que los responsables de los recursos humanos tengan también sus propios sesgos, pero cada persona tenía el suyo. Esto significaba que, dentro de lo malo, una persona que era discriminada en un empleo podría encontrar empleo en otro lugar al entender que no todos los jefes de recursos humanos buscaban lo mismo ni discriminaban o rechazaban por la misma razón. Con la expansión de los algoritmos es probable que los sesgos se estandaricen y se multipliquen. Los algoritmos buscarán los mismos*

patrones y las personas que no entren dentro de los mismos pueden quedar fuera del mercado laboral con independencia de en cuantas empresas se intente solicitar empleo».

Algunos de estos riesgos pueden ser directamente el resultado de defectos en el diseño general de los sistemas de IA (especialmente en lo que se refiere a la supervisión humana) o del uso de datos que puedan ser sesgados si no se someten a un proceso de corrección previa, tal como sucedería, por ejemplo, si se entrena un algoritmo utilizando única o principalmente datos relativos a hombres, lo que posiblemente acabe traduciéndose en resultados peores con relación a las mujeres. La lógica de este argumento podría trasladarse también al ámbito de los procedimientos selectivos, de los procedimientos de movilidad y de los procedimientos de provisión de puestos de trabajo.

2.4. **Su consideración como sistemas de alto riesgo**

Aunque el RIA se dicta principalmente para favorecer el mercado, es perfectamente consciente de los riesgos que la utilización de estos sistemas puede causar en los derechos de las personas empleadas, especialmente en el derecho a la intimidad y a la protección de datos. Por ello, además de prohibir la utilización de algunos de estos sistemas en el entorno laboral, directamente considera como sistemas de alto riesgo a todos los sistemas de IA relacionados con la gestión del empleo, cuando se aplican a la selección, a la asignación de funciones, a la contratación, cese y a otros posibles usos. Los somete a importantes cautelas en la medida en que estos sistemas pueden afectar de un modo considerable a las futuras perspectivas laborales, a los medios de subsistencia de dichas personas y a los derechos de los trabajadores.

Por todo ello, tanto el art. 6 del RIA como su anexo III han considerado como sistemas de IA de alto riesgo a todos los sistemas que supongan una elaboración de perfiles de personas físicas, los destinados a ser utilizados para la contratación o la selección de empleados, en particular para publicar anuncios de empleo específicos, analizar y filtrar las solicitudes de empleo y evaluar a los candidatos. Asimismo, aplicando las categorías de nuestro ordenamiento jurídico funcionarial a las instituciones mencionadas en dicho anexo, podríamos considerar que tendrían también esta consideración de alto riesgo los sistemas de IA destinados a ser utilizados para tomar decisiones que afecten a las condiciones de trabajo de los empleados públicos, a la promoción y carrera, al despido o a la extinción del vínculo funcionarial, a la asignación de tareas a partir de comportamientos individuales o rasgos o características personales, así como los sistemas para la evaluación del desempeño.

Los sistemas de IA en la gestión del empleo público constituyen, por tanto, sistemas de alto riesgo porque pueden contener sesgos y perpetuar patrones históricos de discriminación, por ejemplo, contra las mujeres, determinados grupos de edad, las personas con discapacidad o las personas de orígenes raciales o étnicos concretos o con una orientación sexual determinada, durante el proceso de selección, en la evaluación, promoción o retención de personas en las relaciones contractuales de índole laboral. Asimismo, según explicita el RIA, los sistemas de IA empleados para controlar el rendimiento y el comportamiento de estas personas, nuestra evaluación de desempeño, también pueden socavar sus derechos fundamentales a la protección de los datos personales y a la intimidad (considerando n.º 57).

A partir de estos elevados riesgos de incidencia en los derechos de los empleados públicos, el RIA establece un régimen especial de garantías y controles para estos sistemas. Para garantizar un alto nivel de fiabilidad se someten a un sistema de gestión de riesgos, que debe consistir en un proceso iterativo continuo que sea planificado y ejecutado durante todo el ciclo de vida del sistema de IA de alto riesgo. Dicho proceso debe tener por objeto, en lo que a nosotros nos interesa, detectar y mitigar los riesgos pertinentes de los sistemas de IA para los derechos fundamentales. El sistema de gestión de riesgos debe revisarse y actualizarse periódicamente para garantizar su eficacia continua, así como la justificación y documentación de cualesquiera decisiones y acciones significativas adoptadas con arreglo al presente Reglamento. Se someten a requisitos referentes a la gestión de riesgos, la calidad y la pertinencia de los conjuntos de datos utilizados, la documentación técnica y la conservación de registros, la transparencia y la comunicación de información a los responsables del despliegue, la supervisión humana, la solidez, la precisión y la ciberseguridad. Dichos requisitos son necesarios para mitigar de forma efectiva los riesgos para la salud, la seguridad y los derechos fundamentales (considerando n.º 66).

Para garantizar eficazmente la protección de los derechos fundamentales, los responsables del despliegue de sistemas de IA de alto riesgo, aunque sean organismos de Derecho público, deben llevar a cabo una evaluación del impacto que el sistema puede causar en los derechos fundamentales de los empleados públicos, determinando los riesgos específicos para los derechos de las personas o colectivos de personas que probablemente se vean afectados y definiendo las medidas que deben adoptarse en caso de que se materialicen dichos riesgos. A la luz

de los riesgos detectados, los responsables del despliegue deben determinar las medidas que han de adoptarse en caso de que se materialicen dichos riesgos, entre las que se incluyen, por ejemplo, sistemas de gobernanza para ese contexto de uso específico, mecanismos de supervisión humana con arreglo a las instrucciones de uso, procedimientos de tramitación de reclamaciones y de recurso, ya que podrían ser fundamentales para mitigar los riesgos para los derechos fundamentales en casos de uso concretos. Cuando el sistema de IA se utilice en el sector público, pueden contar con la participación de las partes interesadas pertinentes, como, por ejemplo, los representantes de colectivos de personas que probablemente se vean afectados por el sistema de IA. Esta parte está por desarrollar para los funcionarios públicos y, en todo caso, debería ser el legislador quien concretara este tipo de participación (considerando n.º 96).

En aplicación de esta normativa se ha previsto que la Agencia Española de Supervisión de la Inteligencia Artificial (AESIA) emita informe sobre el impacto generado por todo sistema de IA que se ponga en marcha en los Ministerios, debiendo realizar evaluaciones más precisas de impacto para que los algoritmos involucrados en la toma de decisiones que se utilicen en las Administraciones públicas tengan en cuenta criterios de minimización de sesgos, transparencia y rendición de cuentas (art. 25.b. 4.ª del *Real Decreto 729/2023, de 22 de agosto, por el que se aprueba el Estatuto de la Agencia Española de Supervisión de Inteligencia Artificial*).

En definitiva, lo relevante para determinar que un sistema de IA es de alto riesgo son los efectos jurídicos que provoca en el empleado público. Si la aplicación del sistema supone la toma de decisiones que inciden de modo directo en la esfera jurídica del empleado, ampliando sus derechos, limitándolos o modificándolos, el sistema ha de someterse, como mínimo, a todas las cautelas que establece el Reglamento de Inteligencia Artificial. Sin embargo, podemos encontrarnos otros supuestos de aplicación de estos sistemas que no tengan esta condición y que faciliten la adopción de determinadas políticas de personal a partir de la valiosa información que proporcionan a la Administración. Un ejemplo de ello se encuentra en el documento elaborado por el INAP, en el Proyecto LIP 1: «IA generativa y espacios de datos», resultado de aplicar sistemas de IA a los datos que ya posee la Administración sobre sus empleados públicos y a los datos que proporcionan sus propios curriculums vitae. La explotación de todos estos datos mediante la utilización de un sistema de IA proporcionaría de forma inmediata a la Administración un conocimiento muy valioso sobre los perfiles y las cualidades principales de todo su personal. Esta preciada información puede ser posteriormente usada de forma predictiva para poder predecir las características futuras de las plantillas, determinar las necesidades de la organización, elaborar las ofertas de empleo público que resulten adecuadas, diseñar programas de formación para cubrir las carencias formativas detectadas o para diseñar itinerarios formativos que coincidan con las necesidades de la organización, alineando los derechos y las perspectivas formativas y de carrera de sus empleados con las necesidades organizativas.

En principio, como señala el documento, este tipo de análisis no parecería afectar lo establecido por el RIA respecto a los sistemas de alto riesgo, toda vez que no se derivarían de él consecuencias que afecten a la esfera jurídica del empleado ni se vería modificado su estatus. La Administración evitaría someterse al régimen estricto de obligaciones y cautelas que establece la normativa europea para los proveedores del sistema o para los responsables del despliegue del sistema de IA. Sin embargo, si se hiciera un uso diferente del sistema de IA y pudiera ser considerado como un instrumento decisorio por implicar consecuencias jurídicas para el empleado, como puede ser, por ejemplo, un traslado de puesto de trabajo o una sanción, entonces sí se debería considerar como un sistema de alto riesgo, de acuerdo con lo que señala el Anexo III, punto 4b, del RIA[23].

3. La respuesta explícita del legislador: los derechos digitales del art. 14.j.bis) del TREBEP

Los avances tecnológicos han venido a revolucionar la idea misma de la Administración como empleadora porque han supuesto un incremento notabilísimo de sus poderes de vigilancia y control digital de toda la actividad que realizan sus empleados. La legislación orgánica sobre protección de datos ha venido a cubrir una importante laguna del TREBEP en esta materia, habilitando explícitamente a la Administración para rastrear a sus empleados a través de sistemas de geolocalización, para videovigilarlos o para controlar el uso que hacen de los dispositivos digitales que pone a su disposición. Técnicamente sería posible incluso realizar un control informático de los niveles de productividad de sus empleados en tiempo real, realizar un seguimiento de sus accesos a los distintos programas

informáticos que utilice, acceder a sus correos electrónicos, conocer las llamadas telefónicas o incluso conocer el historial de las navegaciones por internet (Mercader Uguina, 2022). Se echa en falta que el legislador no haya reconocido explícitamente la prohibición de un uso ilegal e injustificado de estos mecanismos de control, aunque, obviamente, su utilización requiere el escrupuloso respeto a sus derechos fundamentales, en los términos expresados por la doctrina constitucional.

El TREBEP, en su redacción inicial, ya reconocía a los empleados públicos el derecho al respeto a su intimidad, a la propia imagen y a la dignidad en el trabajo (letra h) del art. 14, pero esta protección se ha considerado insuficiente para los riesgos que plantean las nuevas tecnologías. Por ello ha sido necesaria la introducción de nuevos supuestos en su letra j) bis para proteger de una forma más sólida el derecho a la intimidad, proyectado también sobre el uso de los medios digitales puestos a su disposición. Ha sido la *Ley Orgánica 3/2018, de 5 de diciembre de Protección de Datos Personales y garantía de los derechos digitales,* la que ha configurado un nuevo marco jurídico para regular, tanto las potestades de vigilancia y control de la Administración, como los nuevos «derechos digitales» de los empleados públicos frente a las nuevas tecnologías que, en la medida en que éstas van avanzando, se quedan pobres y rezagados. Estos nuevos derechos de naturaleza digital han sido introducidos por la disposición final 14 de la Ley Orgánica, que ha introducido un nuevo marco de derechos para los empleados públicos en el entorno digital. La nueva la letra j) bis del art. 14 ha añadido al listado de derechos individuales, comunes a todos los empleados públicos, el derecho la intimidad en el uso de dispositivos digitales puestos a su disposición y frente al uso de dispositivos de videovigilancia y geolocalización, así como a la desconexión digital en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales. Para no extendernos en exceso en este trabajo dejaré fuera de mi análisis el derecho a la desconexión digital y me centraré solo en el derecho a la protección de la intimidad.

Ya tenemos algunos ejemplos en los que ha sido necesario oponer el derecho fundamental a la intimidad en estos contextos laborales digitalizados.

3.1. El derecho a la intimidad frente al uso de dispositivos de videovigilancia en el lugar de trabajo y de geolocalización

Los artículos 89 y 90 de la Ley Orgánica 3/2018 reconocen a la Administración la potestad de fiscalizar al empleado público a través del uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo y la potestad de geolocalizar al empleado. Le habilitan expresamente para tratar las imágenes obtenidas a través de sistemas de cámaras o videocámaras «para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respectivamente, en el artículo 20.3 del Estatuto de los Trabajadores y en la legislación de función pública, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo». Aunque el precepto se remite expresamente a lo que diga la legislación de función pública, no existe exactamente un precepto similar al art. 20.3 del ET en el ámbito estatutario. La Administración habrá de informar con carácter previo, y de forma expresa, clara y concisa, a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de esta medida. Solo en el supuesto de que se haya captado la comisión flagrante de un acto ilícito se entenderá cumplido el deber de informar cuando existiese al menos el dispositivo al que se refiere el artículo 22.4 de esta Ley Orgánica, esto es, mediante la colocación de una pegatina o un dispositivo informativo en lugar suficientemente visible identificando, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos en los artículos 15 a 22 del RGPD. Es decir, el precepto establece una regla general de información específica a los empleados públicos y una excepción en caso de flagrante actuación ilícita, en cuyo caso es suficiente con la información genérica que se establece para todas las personas en general con las mencionadas pegatinas informativas. La jurisprudencia, no obstante, ha convertido la excepción en regla general, toda vez que se apoya exclusivamente en la existencia de la pegatina para cumplir con este deber de información.

Las garantías se refuerzan en el caso de que se utilice la tecnología de la geolocalización porque la invasión de la esfera jurídica del empleado es todavía mayor. Estos sistemas permitirían constatar los lugares que se han visitado y el tiempo que el empleado público ha invertido en ello (Expósito Gázquez, 2022). En este caso se ha de informar con carácter previo y de forma expresa, clara e inequívoca a los empleados públicos y, en su caso, a sus representantes, acerca de la existencia y características de estos dispositivos, informándoles, asimismo, sobre el posible ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión. También en este supuesto el precepto vuelve a remitirse la legislación de función pública y solo permite usarla cuando «estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo». En el TREBEP, no obstante, no hay ninguna regulación explícita de esta importante potestad. Solo se aborda el derecho a la

intimidad del empleado. Por ello su utilización podría resultar dudosa, dado que no existiría una base legal explícita para ello. Es más, por un defecto de técnica jurídica del legislador, el art. 14.j.bis) solo se refiere explícitamente al derecho a la intimidad, cuando en este caso se ve directamente afectado también el derecho a la protección de datos. En todo caso, la utilización de estos sistemas debería responder a una causa justificada y requiere un respeto escrupuloso del principio de proporcionalidad, que exige limitar esta clase de sistemas a aquellas situaciones donde no existan medios menos invasivos, así como con los principios de minimización y limitación de la finalidad del tratamiento[24].

Con la utilización de estas tecnologías, no solo resulta afectado el derecho a la intimidad del art. 18.1 de la Constitución, sino también y de modo directo el derecho a la protección de datos del art. 18.4 CE que, como estableció la STC 292/2000, garantiza a las personas un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado. A pesar de ello, la doctrina del Tribunal Constitucional ha mantenido en sus últimas sentencias una postura excesivamente flexible sobre sobre las obligaciones de información del empresario que ha supuesto una clara devaluación del derecho a la información del trabajador (Cabellos Espiérrez, 2024).

Efectivamente, en la STC 29/2013, de 11 de febrero, sobre grabaciones en la Universidad de Sevilla, consideró que era necesario informar expresamente a los trabajadores de la finalidad de control sobre el cumplimiento de las condiciones del trabajo y de que el empresario tenía las cámaras instaladas, incluso para la imposición de posibles sanciones disciplinarias. Sin embargo, cambió de criterio con la STC 39/2016, de 3 de marzo, relajando los criterios sensiblemente y considerando que bastaba con el deber de información genérico de las cámaras establecidas para la seguridad de recintos, entendiendo que el consentimiento se entiende implícito en la propia aceptación del contrato que implica reconocimiento del poder de dirección del empresario y que esta potestad del empresario se relaciona directamente con el derecho a la propiedad privada (art. 33 CE) y con el derecho a la libertad de empresa (art. 38 CE). En este caso, la empresa había colocado el correspondiente distintivo informativo en el escaparate de la tienda donde prestaba sus servicios la trabajadora despedida, por lo que se presume que podía conocer la existencia de las cámaras y la finalidad para la que habían sido instaladas.

Esta doctrina ha sido corroborada más recientemente por la STC 119/2022, de 29 de septiembre, que avala también la licitud de un despido ante un hecho que se calificó de irregular por la gerencia de la empresa. Se examinaron las cámaras de seguridad, que estaban instaladas en los lugares de atención al público y se verificó que se había cometido una conducta ilícita por parte de uno de los trabajadores, que había vendido un producto sin registrarlo en la caja. Los trabajadores no habían recibido información previa y expresa sobre la instalación de las cámaras y su eventual uso con fines disciplinarios. No obstante, la instalación del sistema de videovigilancia estaba advertida en un lugar visible de la empresa, mediante un distintivo que se ajustaba a la normativa vigente sobre protección de datos desde hacía más de cinco años y otro trabajador ya había sido despedido años antes por un motivo similar[25]. Es decir, esta doctrina presume directamente el conocimiento de esta información por parte del trabajador, lo que no está amparado en la legislación orgánica, que exige determinadas condiciones para considerar válida la información: información previa, expresa, clara y concisa. Incomprensiblemente se aparta de la obligación de información específica al trabajador sobre la finalidad del tratamiento y rebaja considerablemente los estándares de protección de los derechos de los trabajadores.

En el ámbito administrativo esta misma cuestión ha sido tratada en la STS de 26 de abril de 2021, Sala Tercera, de lo Contencioso-administrativo, Sección 4.ª, Sentencia 557/2021, a propósito del caso de una funcionaria de la Agencia Estatal de la Administración Tributaria (AEAT) que había sido sancionada con 8 meses de suspensión de empleo y sueldo por saltarse los controles horarios, tal como había quedado acreditado en una grabación. Mediante las citadas imágenes de la videocámara se acredita la actividad desplegada por la recurrente para eludir el sistema de control horario, intentando evitar ser detectada, mediante la evasión de fichajes propios, o mediante la sustitución o suplantación de los fichajes de otro funcionario[26]. Se plantea en la sentencia si, en el ámbito de la Administración Pública, el uso de sistemas de videovigilancia, establecidos con carácter permanente y con una finalidad general de vigilancia y seguridad, exige informar a los funcionarios de manera previa, expresa e inequívoca, sobre la finalidad de control de la actividad laboral de dicho sistema y, en su consecuencia, su posible utilización para la imposición de sanciones disciplinarias. La sentencia aplica la doctrina del Tribunal Constitucional dictada en el ámbito empresarial al ámbito de la función pública, aunque hace un importante esfuerzo por trasladar la terminología y la argumentación jurídica usada en el ámbito laboral al ámbito funcionarial.

Efectivamente, al ser la imagen un dato personal que identifica o hace identificable a una persona, su tra-

tamiento necesita una base jurídica, pero esta base no se encuentra en el consentimiento del funcionario, sino «en el contrato de trabajo y las facultades legales de control concedidas al empleador». Se deduce, en consecuencia, que para usar estos sistemas de videovigilancia no se requiere el consentimiento del funcionario, sino que la base jurídica deriva de su nombramiento[27]. Dado que el principio de minimización del art. 5 del RGPD requiere que los datos personales tratados sean adecuados, pertinentes y limitados en relación con los fines para los que son tratados, se ha planteado si este tratamiento establecido por razones de vigilancia de seguridad del centro de trabajo puede servir para otra finalidad diferente, para ejercer la potestad disciplinaria de la Administración. La Sala ha considerado que la regla general del consentimiento para tratar datos personales como son las grabaciones encuentra como excepción la necesidad del mantenimiento y cumplimiento de la relación de servicio que se despliega sobre las obligaciones que se derivan del régimen propio de los funcionarios públicos, es decir, de una relación administrativa que exige velar por el cumplimiento de sus obligaciones, aunque teniendo siempre en cuenta la proporcionalidad. Realiza un importante esfuerzo argumental por trasladar en bloque la doctrina laboral sobre las potestades de vigilancia y supervisión del empresario al ámbito de la Administración, a pesar de que en el ámbito funcionarial no existe un precepto explícito como el del art. 20.3 del ET que atribuya las potestades de vigilancia y supervisión digital a la Administración y, obviamente, no resultan aplicables los derechos de libertad de empresa (art. 38 CE) y de propiedad privada (art. 33 CE) que utiliza la jurisprudencia social en este ámbito. Así, ha dicho el TS que, *«teniendo en cuenta que estamos ante una relación de especial sujeción entre el funcionario público y la Administración, y que dicha captación de imágenes no se realizó mediante la instalación de cámaras nuevas específicamente instaladas para la funcionaria recurrente, sino que la comisión de la infracción se acredita, entre otros medios, con las cámaras existentes, que ya conocía la recurrente como revela la realización de maniobras que pretenden esquivar el control de las condiciones de trabajo como el horario de cumplimiento diario. Todo ello con una potente presencia del interés general ante este tipo conductas que además de mancillar la imagen de la Administración como organización servicial de la comunidad, su generalización afectaría al adecuado funcionamiento de la institución. De modo que la información ordinaria, por las cámaras instaladas con carácter general en el edificio para la seguridad y vigilancia, también del cumplimiento de las condiciones de trabajo, no alcanza a exigir una concreta y específica previsión sobre el posterior uso a los funcionarios públicos afectado, es decir, sobre la finalidad específica de su utilización, en el caso de eventuales procedimientos disciplinarios»*.

La misma argumentación ha utilizado la STSJ de la Comunidad Valenciana de 17 de febrero de 2023, Sala de lo Contencioso-Administrativo, Sección 2.ª, que ha sancionado a 2 días de suspensión de empleo y sueldo por haberse ausentado del puesto de trabajo durante más de dos horas, excediéndose de la media hora de descanso. Pretendía la nulidad de la sanción basándose en que la prueba obtenida mediante videocámara —grabaciones— no puede valer como tal al no haberse informado a los funcionarios del Cuerpo Nacional de Policía (CNP) de que podía ser utilizada como prueba en los expedientes disciplinarios, vulnerando el art. 89 de la LO 3/2018, de 5 de diciembre. Según la Sala, no era necesaria una advertencia específica y previa a los funcionarios del CNP para su uso a efectos disciplinarios sobre hechos acaecidos en la propia Comisaría, cuando ya los propios funcionarios conocían su existencia.

3.2. El derecho a la intimidad ante el uso de dispositivos digitales que la Administración pone a disposición de su empleado

El derecho a la intimidad se aplica también cuando la Administración ejerce sus poderes de vigilancia y supervisión accediendo a los ordenadores, tabletas, teléfonos móviles, correos electrónicos[28] u otros dispositivos digitales que ella mismo ha puesto a disposición de sus empleados y que debería complementarse con el derecho al secreto de las comunicaciones[29].

La atribución explícita de esta potestad a la Administración hemos de encontrarla en el art. 87 de la Ley Orgánica 3/2018. Permite que pueda acceder a los contenidos derivados del uso de medios digitales facilitados a sus empleados a los solos efectos de controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la integridad de dichos dispositivos. En estos casos se regulan determinadas garantías. Debe establecer previamente los criterios de utilización de los dispositivos digitales respetando en todo caso los estándares mínimos de protección de su intimidad de acuerdo con los usos sociales y los derechos reconocidos constitucional y legalmente. El precepto establece limitaciones a ese poder de vigilancia para proteger la intimidad del empleado y ordena con carácter imperativo que la elaboración de los criterios de utilización de dichos medios se realice con la participación de los repre-

sentantes de los trabajadores. Esta participación es imprescindible y lógica para la validez de dichos criterios si se tiene en cuenta, como establece la STS de 6 de febrero de 2024, Sala de lo Social, Sección 1.ª, que *«los dispositivos digitales del trabajador pueden ser en cualquier momento analizados, examinados, formateados y/o reseteados mediante los oportunos medios informáticos al alcance de la empresa, sin ninguna otra precisión relativa a la información del interesado o a la participación o presencia del mismo o de sus representantes»*. Cuando haya admitido su uso para fines privados, el acceso al dispositivo digital requiere que se especifiquen de modo preciso los usos autorizados, que establezcan garantías para preservar la intimidad de los empleados, tales como, en su caso, la determinación de los períodos en que los dispositivos podrán utilizarse para fines privados y, asimismo, que se informe a los empleados de estos criterios de utilización.

Sobre algunas de estas cuestiones se ha pronunciado ya la jurisprudencia. En la Sentencia de la Audiencia Nacional de 6 de febrero de 2024, Sala de lo Contencioso-administrativo, Sección 7.ª**,** el acceso al ordenador del funcionario se ha utilizado para fines disciplinarios y se ha traducido en la suspensión de empleo y sueldo durante diez meses de un funcionario de la AEAT que había cometido numerosas infracciones administrativas que la Administración pudo comprobar tras analizar su ordenador. Recuerda la Sala que no existe un derecho omnímodo a la intimidad respecto a los datos contenidos en los equipos informáticos que son puestos a disposición del funcionario por la Administración, sino que este derecho es instrumental para la realización de las actividades propias del cargo. Por ello, si existe la sospecha de una utilización indebida de los equipos informáticos, en actuaciones que pudieran ser constitutivas de infracción administrativa, como ha sido el caso, es procedente el acceso a dichos equipos para garantizar la prueba necesaria sobre las actuaciones del funcionario. En este caso existía una Instrucción interna de la Administración que advertía de los usos del ordenador y de la posibilidad de ser inspeccionados y de que sus resultados pudieran incorporarse a un expediente disciplinario o aportarse a un procedimiento judicial.

En un sentido similar podemos traer a colación la Sentencia de la Audiencia Nacional de 10 de junio de 2022, Sala de lo Contencioso-Administrativo, Sección 1.ª, que ha determinado, desde la perspectiva de los derechos fundamentales, si el acceso a los contenidos de los ordenadores u otros medios informáticos vulnera el artículo 18.4 de la Constitución. Se declara ilícita la prueba aportada por el ayuntamiento de Algemesí para sancionar a su funcionaria, la tesorera del ayuntamiento. Aparecieron unos documentos en la impresora y en la memoria del escáner que podrían suponer que la funcionaria realizaba actividades profesionales para una empresa privada dentro de la jornada de trabajo, que ni tenían nada que ver con sus funciones de tesorera ni resultaban compatibles con ellas. La alcaldesa ordenó al departamento de informática que investigara los documentos del ordenador personal de trabajo para aclarar esos hechos. El informático, sin necesidad de acudir físicamente al ordenador con clave como administrador, inspeccionó su ordenador y copió varias carpetas de documentos personales sobre actividades privadas que se grabaron en un DVD, en las que aparecía que, efectivamente, estaba trabajando para otra empresa privada, pero también se había hecho copia de datos personales especialmente sensibles y datos de salud.

La actuación del ayuntamiento se hizo sin respetar los derechos de sus empleados y su expectativa razonable de privacidad. En este caso el ayuntamiento no había informado previamente a los empleados de la utilización de los equipos informáticos, con la advertencia de la existencia de medidas de control o supervisión del ordenador sobre las comunicaciones de los empleados. Además, tampoco existió proporcionalidad en el acceso, pues el ayuntamiento accedió a todas las carpetas y archivos sin discriminar su contenido, de una forma especialmente invasiva, afectando a datos de salud y a otros documentos privados de la reclamante. Dirá el Tribunal que, el hecho de que la relación estatutaria sitúe al funcionario en una posición de sujeción especial, delimitada y regida por su específica regulación, no excluye ni impide que se dicten instrucciones dirigidas a los empleados públicos en las que se concrete en qué consiste el uso adecuado de los medios informáticos, así como el alcance del control que puede efectuarse sobre ellos. Lo que está en juego, no es, o no solamente, la utilización adecuada de los medios informáticos, sino la posibilidad de ejercer un control de dichos medios y su compatibilidad con los derechos del funcionario y su expectativa razonable de privacidad. Ante estas circunstancias y su correspondiente denuncia, la Agencia Española de Protección de Datos, aplicando el art. 77 de la Ley Orgánica, declaró que el ayuntamiento de Algemesí había infringido su artículo 6.1, que exige contar con el consentimiento inequívoco del afectado para el tratamiento de sus datos de carácter personal.

Esta doctrina ha sido confirmada por la STS de 7 de octubre de 2024, Sala contencioso-administrativa, Sección 3.ª, (rec.6949/2022), que toma directamente como referencia la interpretación realizada por la STS, Sala de lo Social, de 8 de febrero de 2018 (Rec. 1121/2015) y su análisis sobre la «expectativa de privacidad» para el tratamiento de los datos personales que supone el ac-

ceso al ordenador de un empleado público. La sentencia es importante porque aplica directamente la doctrina de la sentencia del TEDH en el asunto Barbulescu 2, de 5 de septiembre de 2017, al ámbito del empleo público y porque analiza el art. 14, j) bis del TREBEP, trasladando la doctrina generada en el ámbito laboral al ámbito de la Administración pública, rechazando la tesis planteada por el ayuntamiento sobre la inexistencia de una expectativa de privacidad del funcionario, en virtud de la existencia de una especial relación de sujeción entre la funcionaria y la Administración y en la especial naturaleza del ordenador y de la impresora como bienes de dominio público.

Aclara que la relación de sujeción especial entre el funcionario y la Administración implica una situación de dependencia mayor que la que se produce en las relaciones de sujeción general, pero no llega a la exclusión de un derecho fundamental que no encuentra fundamento legal por la naturaleza jurídica pública del Ayuntamiento actuante, pues los principios generales del derecho de protección de datos son aplicables tanto a entidades públicas como privadas aunque en algunos supuestos la normativa pública pueda influir en el tratamiento llevado a cabo. Las particularidades de ser una Administración Pública, que las hay, se refieren fundamentalmente a la no imposición de sanción al Ayuntamiento por las vulneraciones a la normativa de protección de datos, pero el hecho de que el sujeto infractor sea una Administración Pública no lleva, en lo que aquí atañe, a la desaparición del derecho fundamental del artículo 18 CE o del artículo 8 de la Carta Europea de Derechos Humanos.

3.3. La problemática utilización de tecnologías de identificación biométrica para el control de presencia en el puesto de trabajo

La tecnología permite que la Administración pueda utilizar datos biométricos para controlar a sus empleados[30]. En concreto, entre otras posibilidades, puede utilizar el uso de dispositivos de reconocimiento facial y/o huella dactilar con la finalidad de efectuar un control del cumplimiento de horarios y de la jornada laboral del personal, toda vez que, en ocasiones, la utilización de una tarjeta personal e intransferible para el fichaje no garantiza suficientemente el control, pues no hay manera de comprobar que ésta se utiliza de forma adecuada y unipersonal. El control biométrico permite una acreditación fidedigna de la presencia de personal en su puesto de trabajo, los días y horas que corresponden según su calendario de trabajo, toda vez que este dato personal constituye un identificador único. Desde esta perspectiva, evita el riesgo de suplantación del funcionario. Ahora bien, su utilización plantea importantes riesgos e implica un tratamiento de datos personales que impacta de modo directo en el derecho fundamental a la intimidad y a la protección de datos del empleado. La utilización de tecnologías biométricas de identificación y autenticación en el control de presencia supone un tratamiento de alto riesgo que incluye categorías especiales de datos.

Los datos biométricos, efectivamente, son una categoría especial de datos personales que van dirigidos a identificar de manera unívoca a una persona física. A diferencia de lo que ocurre con las fotos, por ejemplo, los datos biométricos se almacenan en forma de una plantilla o patrón biométrico. Una plantilla biométrica es una forma de escritura de una característica biométrica humana, como un rostro o una huella dactilar, de manera que sea interpretable por una máquina de forma eficiente y eficaz para un propósito o propósitos determinados. La plantilla biométrica, tal como aclara la Agencia Española de Protección de Datos (AEPD) no está orientada a ser interpretada por una persona, como una fotografía, sino que está orientada a ser tratada en un proceso automatizado por una máquina[31]. Dados los problemas que presentan estos datos biométricos, esta guía ha mantenido una postura muy cautelosa y restrictiva de su utilización, siguiendo las Directrices 05/2022 del Comité Europeo de Protección de Datos (CEPD), sobre el uso de reconocimiento facial en el ámbito de las fuerzas de orden público, Versión 2.0, elaboradas el 26 de abril de 2023.

Los datos biométricos constituyen una «categoría especial» de datos y, por ello, gozan de una especial protección, que es superior a la de otros datos personales. Esta especial categoría de datos se caracteriza porque su tratamiento debe considerarse, en principio, prohibido conforme a lo dispuesto en el artículo 9.1 del RGPD. No obstante, este mismo precepto admite varias excepciones. Entre otras, y en lo que en este punto nos interesa, permitiría la posibilidad de tratar este tipo de datos biométricos y, en consecuencia, que la Administración utilizara esta tecnología para controlar la jornada y la presencia de los empleados públicos, si el interesado da su consentimiento explícito y si este control es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado. De la misma manera, las letras b) y c) del artículo 6 del RGPD prevén que el tratamiento de datos pueda ser

lícito si es necesario para la ejecución de un contrato en el que el interesado es parte o cuando dicho tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento, aunque para hacer este análisis es preciso que se haya levantado previamente la prohibición del tratamiento de categorías especiales de datos personales pues, si no es así, ya habría una condición que invalidaría el tratamiento y carecería de sentido analizar las bases jurídicas previstas en el art. 6.1 del RGPD.

La posibilidad de que la Administración controle la presencia de sus empleados públicos en sus puestos de trabajo a través de sistemas de identificación biométrica ya se ha planteado en algunos ayuntamientos y ha ocasionado un importante debate sobre la legitimación de la Administración para la utilización de esta tecnología. Así se aprecia, por ejemplo, en el *Dictamen 1/2023, de 28 de julio, del Consejo de Transparencia y Protección de Datos de Andalucía* y en el *Dictamen 2/2022, de 2 de febrero, de la Autoridad Catalana de Protección de Datos*[32], que se han pronunciado sobre el tratamiento de categorías especiales de datos biométricos mediante el uso de dispositivos de reconocimiento facial y/o huella dactilar para el control horario del personal de los ayuntamientos. La propia AEPD ha cambiado su criterio sobre tratamientos de control de presencia mediante sistemas biométricos[33]. Para usar estas tecnologías, no solo es necesario que exista una circunstancia que levante la prohibición de su tratamiento, sino que además debe existir una circunstancia que lo legitime y tiene que respetarse el principio de proporcionalidad[34], en su triple contenido (necesidad, idoneidad y proporcionalidad en sentido estricto). Es necesario justificar la necesidad de un tratamiento adicional de datos cuando las mismas finalidades se han estado alcanzando y se pueden alcanzar con otro tipo de implementación del tratamiento de registro de jornada equivalente y menos intrusivo en los derechos fundamentales del empleado y, en todo caso, requiere superar favorablemente una Evaluación de Impacto para la Protección de Datos (EIPD).

Ambos dictámenes llegan a la conclusión de que la utilización del control biométrico no puede ampararse ni en el consentimiento del empleado público ni en la existencia de una obligación legal de carácter laboral, aunque dejan un importante —y preocupante— margen de actuación a la negociación colectiva. En cualquier caso, antes de la eventual implantación de un sistema de este tipo, es imprescindible realizar una evaluación del impacto sobre la protección de datos para determinar la licitud y la proporcionalidad, fijar las garantías que sean necesarias y analizar la existencia de alternativas menos intrusivas en los derechos fundamentales de los empleados públicos.

En ambos dictámenes se considera que la base legal de este tipo de tratamiento de datos que constituye la biometría no puede ampararse en la causa prevista en el art. 9.2.a) del RGPD, esto es, en el consentimiento explícito del empleado público, en virtud del desequilibrio entre dicho interesado y la Administración Pública responsable del tratamiento[35]. En el ámbito de las relaciones laborales es muy difícil que pueda darse válida y legítimamente un consentimiento del empleado para que la Administración pueda tratar sus datos, no solo por la condición de autoridad que tiene la Administración, sino también por el desequilibrio que existe en las relaciones entre empleador y empleado (considerando n.º 43 del RGPD). Se ha considerado que no es probable que el interesado pueda negar al empleador el consentimiento para el tratamiento de datos sin experimentar temor o riesgo real de que su negativa produzca efectos perjudiciales ni que pueda responder libremente a una solicitud de consentimiento del empleador para, por ejemplo, activar sistemas de vigilancia por cámara en el lugar de trabajo, sin sentirse presionado a dar su consentimiento. Por ello, se ha entendido que, como regla general, en la mayoría de los tratamientos de datos que se dan en el ámbito de las relaciones laborales, la base jurídica no puede y no debe ser el consentimiento de los trabajadores debido a la naturaleza de la relación entre empleador y empleado. Así, por ejemplo, si el empleador pretendiera utilizar la tecnología de identificación biométrica para controlar la jornada, solo se consideraría que el consentimiento es libre si el empleado dispone de una alternativa para cumplir con el control horario y es él mismo quien elige voluntariamente y presta su consentimiento al tratamiento de sus datos biométricos.

Fuera de estos supuestos, tampoco podría ampararse en la circunstancia prevista en el artículo 9.2 b) del RGPD, que permitiría usar esta tecnología si es necesaria para el cumplimiento de obligaciones en el ámbito del Derecho laboral, aunque solo en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado. Aunque esta excepción se refiere al expresamente al ámbito del «Derecho Laboral», ha de incluirse también el régimen estatutario funcionarial, tal como interpretó la propia Agencia Española de Protección de Datos en el informe de su Gabinete Jurídico 2/2022, en el que señaló que, aunque la función pública no se rige, en puridad, por normas laborales sino por el derecho administrativo estatutario de los funcionarios públicos, la interpretación que de ella se deriva, comparte, en términos generales, la misma naturaleza jurídica.

En el caso español no existe ninguna norma legal que contenga tal obligación ni autorice a la utilización de sistemas biométricos en la Administración ni en el TREBEP ni en los artículos 87 y siguientes de la Ley Orgánica 3/2018. Y ello porque no existe una norma con rango de Ley Orgánica que atribuya tal potestad a la Administración, en los términos de previsibilidad y certeza que ya estableció la Sentencia del Tribunal Constitucional 76/2019, de 22 de mayo. En dicho pronunciamiento clarificó el Tribunal que la norma legal que pretenda limitar derechos fundamentales debe reunir todas las características indispensables como garantía de la seguridad jurídica, expresando todos y cada uno de los presupuestos y condiciones de la intervención, de forma que las limitaciones del derecho fundamental establecidas por una ley pueden vulnerar la Constitución si adolecen de falta de certeza y previsibilidad.

Además, el régimen legal de la jornada de los trabajadores es distinto del de los funcionarios públicos. El art. 34.9 del ET obliga a la empresa a garantizar el registro diario de jornada, que deberá incluir el horario concreto de inicio y finalización de la jornada de trabajo de cada persona trabajadora y remite directamente a la negociación colectiva para que organice y documente este registro de jornada, que debe conservarse durante 4 años y permanecer a disposición de las personas trabajadoras, de sus representantes legales y de la Inspección de Trabajo y Seguridad Social. Sin embargo, el art. 47 del TREBEP no contiene una obligación similar ni tampoco existe un precepto expreso habilitante como el establecido en el art. 20.3 del ET que atribuya expresamente las potestades de supervisión y control a la Administración, aunque sí posee la potestad disciplinaria. El código de conducta regulado en el art. 54 del TREBEP establece la obligación de desempeñar las tareas correspondientes al puesto de trabajo de forma diligente y cumpliendo la jornada y el horario establecidos y constituyen una falta grave las acciones u omisiones del funcionario dirigidas a evadir los sistemas de control de horarios o a impedir que sean detectados los incumplimientos injustificados de la jornada de trabajo (art. 7.1.p) del *Real Decreto 33/1986, de 10 de enero, por el que se aprueba el Reglamento de Régimen Disciplinario de los Funcionarios de la Administración del Estado*). De este marco jurídico puede derivarse implícitamente la potestad de supervisión y control del cumplimiento de horarios y jornadas, pero no se deriva en modo alguno ninguna habilitación legal para que pueda usar sistemas de control biométrico.

Además, el marco jurídico y el papel de la negociación colectiva en este ámbito difieren notablemente en virtud de la naturaleza laboral o funcionarial del vínculo que une al empleado público con su Administración. Los Dictámenes, en este sentido, realizan una afirmación que, a mi juicio resulta bastante dudosa y preocupante, al menos cuando se aplica al ámbito funcionarial. Realizando una interpretación literal de la mención que realiza el art. 9.2.b) del RGPD a los convenios colectivos, deducen que, a falta de tal previsión legal, la referida autorización o habilitación podría preverse en los convenios colectivos para el personal laboral y en los acuerdos sobre condiciones de trabajo del personal funcionario en el marco de la negociación colectiva con los requisitos previstos para su eficacia. Ahora bien, esta remisión debe realizarse, en todo caso, teniendo en cuenta el régimen particular —y diferenciado del laboral— que tiene la negociación colectiva funcionarial.

A mi juicio, es impensable que los pactos o los acuerdos funcionariales, como fruto de la negociación, puedan contener semejante habilitación que, en todo caso, supondría una limitación de derechos sin que exista una previa ley habilitante. Existe una reserva de ley para el régimen de los funcionarios públicos (art. 103.3 CE), pero, a diferencia de lo que ocurre en el ámbito de la negociación colectiva privada, la ley no funciona como una plataforma de mínimos que pueda ser mejorable en virtud de lo negociado con los sindicatos funcionariales. Los acuerdos funcionariales solo pueden adoptarse estrictamente sobre el listado de materias que prevé el art. 37.1 del TREBEP, cuya letra m) obliga a la Administración a negociar, en su ámbito respectivo y en relación estrictamente con sus competencias, el calendario laboral, los horarios y las jornadas. Ahora bien, de esta mención a la jornada y al horario no se deduce, en modo alguno, una habilitación explicita para negociar sobre el establecimiento de un sistema de control que impacta de un modo tan importante sobre los derechos fundamentales de los funcionarios públicos, tal como sucede con los sistemas de control biométrico. De haberlo querido el legislador lo debería haber contemplado expresamente y en una norma con rango de Ley Orgánica (STC 76/2019, de 22 de mayo y STC 136/2024, de 5 de noviembre). No interpretarlo así sería una burla a la reserva de ley y a las notas de previsibilidad y certeza que ha de tener cualquier injerencia en un derecho fundamental, lo que sirve, no solo para el gobierno y la Administración, sino también, obviamente, para los sindicatos funcionariales que negocian con la Administración.

Todos estos documentos, por lo demás, también alertan de los riesgos que puede conllevar la generalización de estos sistemas de control biométrico, pues, cuanto mayor sea el número de sistemas de identificación que se usan, mayor es el riesgo de que este dato pueda acabar siendo utilizado de forma inadecuada y dando lugar a un riesgo de usurpación o su-

plantación de identidad. Este riesgo puede incrementarse claramente en función de cuál sea la tecnología empleada y del tratamiento que se dé a los datos biométricos en bruto u originales. Dado el carácter personal y único de los datos biométricos, estos datos no son modificables, a diferencia de una contraseña, por lo que, en caso de pérdida no pueden cambiarse, por lo que un fallo de seguridad o una eventual pérdida de confidencialidad de estos datos podría permitir la suplantación. Asimismo, una vez recogidos estos datos para controlar la presencia no es del todo improbable que pudieran ser utilizados para otras finalidades como para el control de acceso a ciertos espacios o recursos de la propia entidad o incluso para la evaluación de rendimiento laboral[36].

4. El problema de una universalización de derechos para funcionarios y laborales a dos velocidades

La equiparación de los derechos y del régimen jurídico de los funcionarios y los laborales quedó plasmada con claridad en el artículo 87.1 de la Ley Orgánica 3/2018, según el cual «*Los trabajadores y los empleados públicos tendrán derecho a la protección de su intimidad en el uso de los dispositivos digitales puestos a su disposición por su empleador*» (STS de 7 de octubre de 2024). Tanto el art. 14.j.bis) del TREBEP como el art. 20 bis. del ET tienen el mismo contenido y garantizan el derecho a la intimidad en el uso de dispositivos digitales puestos a su disposición y frente al uso de dispositivos de videovigilancia y geolocalización. Asimismo, el legislador orgánico ha establecido también el mismo régimen jurídico igualitario en cuanto a las potestades de vigilancia y supervisión tecnológica de la Administración.

El legislador ha consagrado lo que ya había sido recogido por la jurisprudencia contenciosa, que se había remitido en bloque a la doctrina constitucional y a la jurisprudencia social a la hora de analizar la limitación de los derechos fundamentales de los funcionarios en el ámbito estatutario. Sin embargo, este intento de trasvase automático de la doctrina laboral al ámbito funcionarial planteaba algunos problemas importantes para la configuración teórica del modelo. Desde la STC 39/2016, de 3 de marzo, el Tribunal ha explicado los poderes de dirección del empresario del art. 20 del ET como una manifestación del derecho constitucional a la libertad de empresa consagrado en el art. 38 de la Constitución y del derecho a la propiedad privada que recoge el art. 33 del texto constitucional. La sentencia contó con varios votos particulares por entender que esta interpretación supone un retroceso en la protección de los derechos fundamentales de las personas que prestan un trabajo asalariado. Critican que la Sala haya construido una colisión de derechos ficticia al atribuirle a este precepto una conexión con los arts. 33 y 38 CE para deducir, a continuación, un conflicto de intereses entre derechos fundamentales y otros derechos y bienes constitucionales también merecedores de tutela que, en consecuencia, ha de resolverse con la técnica de la ponderación entre derechos y el principio de proporcionalidad. Esta concepción acaba convirtiendo las facultades de vigilancia y control empresarial del art. 20 del ET en una fuente constitucional cuando, en realidad, no es sino una mera regla jurídica rectora de la relación contractual.

Por ello, no es de extrañar que en la configuración de estos poderes de vigilancia en el ámbito de la función pública encontremos algunos problemas jurídicos para la asunción automática del modelo, toda vez que en el TREBEP ni existe un precepto similar que atribuya esos poderes explícitos a la Administración ni se pueden invocar los artículos 33 y 38 de la Constitución para justificar estas facultades de vigilancia de la Administración.

En todo caso, a pesar de esta pretensión de unificar el régimen de los derechos, la construcción jurídica realizada en el TREBEP para sus funcionarios es más pobre que la aplicable en relación con sus empleados laborales, lo que hoy en día no tiene mucho sentido. Así, para el ámbito laboral hay que tener en cuenta el derecho a la información algorítmica que establece la *Ley 12/2021, de 28 de septiembre, por la que se modifica el texto refundido de la Ley del 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,* que ha modificado el art. 64 del Estatuto de los Trabajadores y ha añadido el derecho del comité de empresa a ser informado por el empresario de los parámetros, reglas e instrucciones en los que se basan los algoritmos o sistemas de inteligencia artificial 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. Sin embargo, no existe una previsión similar para los algoritmos que pudieran afectar a los funcionarios públicos, lo que supone una quiebra importante del principio de universalidad del régimen jurídico. Tal vez debería plantearse el legislador básico estatutario añadir una nueva letra en el listado de funciones que establece

el art. 40.1 del TREBEP para establecer un derecho similar para los delegados de personal y para las juntas de personal en el ámbito de las Administraciones Públicas.

Lo mismo sucede con el papel de la negociación colectiva en cuanto a la protección «digital» de los funcionarios. Aunque el reconocimiento de derechos en el entorno digital se caracteriza por su universalidad y carácter unitario, puede haber importantes diferencias en su configuración jurídica final en virtud del papel que puede jugar la negociación colectiva en este ámbito. El legislador se ha olvidado por completo de los funcionarios públicos en este punto. El art. 91 de la Ley orgánica 3/2018 nos describe el sistema de protección digital de los empleados reenviando directamente a los convenios colectivos, que pueden 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. Aunque literalmente se refiere solo a los convenios colectivos, puede interpretarse que este mismo llamamiento puede ser realizado a los Acuerdos y Pactos funcionariales para la protección de los derechos digitales de los funcionarios públicos. No obstante, y si esto es así porque resulta la interpretación teleológica más razonable, no hubiera estado de más que el propio legislador orgánico se hubiera remitido directamente a la realidad funcionarial, toda vez que en el ámbito de la función pública la ley, al menos tradicionalmente, no ha actuado nunca como un mínimo de protección que pueda ser mejorado y ampliado para los funcionarios públicos a través de la negociación colectiva con los sindicatos funcionariales. Posiblemente debería incluirse el listado de materias sobre las que es precisa la negociación colectiva para incluir una nueva letra en el art. 37.1 del TREBEP para referirse a las propuestas sobre derechos digitales en el entorno laboral.

5. La complejidad de un régimen jurídico fragmentado y desfasado

Puede decirse que la respuesta de nuestro ordenamiento jurídico a las transformaciones digitales en el ámbito de la Administración ha sido tardía, escasa y está fragmentada en varios ordenamientos, lo que nos aboca a un escenario de inseguridad jurídica. La composición del régimen de derechos del empleado público se asimila hoy en día a un complejo puzle en el que la primera y más esencial pieza es, sin duda, el art. 14.j.bis) del TREBEP, que reconoce expresamente el derecho de todos los empleados públicos a la intimidad frente al uso por parte de la Administración de estos sistemas tecnológicos. Sin embargo, dicha pieza del puzle ha de ser completada forzosamente con los distintos preceptos de la Ley orgánica 3/2018, que es la que atribuye expresamente las potestades de vigilancia y supervisión digital a la Administración y establece un mínimo marco de garantías que, en cualquier caso, podrían ser completadas a través de la negociación colectiva funcionarial (previa intervención del legislador de función pública, a mi juicio).

Otra pieza importante del puzle es el art. 23.1 de la *Ley 15/2022, de 12 de julio, integral para la igualdad de trato y la no discriminación,* que hace referencia a algunos aspectos esenciales que ha de tener en cuenta la Administración cuando use algoritmos para la toma de decisiones. La ley se aplica a la Inteligencia Artificial y a la gestión masiva de datos (art. 3.1.o) y remite, con carácter general, a la Estrategia Nacional de Inteligencia Artificial, a la Carta de Derechos Digitales y a las iniciativas europeas sobre esta materia. No obstante, a mi juicio, con ser un avance notable, sigue presentando algunas carencias. No se pronuncia con el suficiente carácter imperativo ni consagra explícitamente derechos a favor de los ciudadanos, sino que tiene un marcado carácter programático y abstracto a la hora de fijar obligaciones jurídicamente exigibles.

Efectivamente, al referirse a la IA y a los mecanismos de toma de decisión automatizados, señala que, las Administraciones públicas «favorecerán» la puesta en marcha de mecanismos para que los algoritmos involucrados en la toma de decisiones que se utilicen en las Administraciones públicas tengan en cuenta criterios de minimización de sesgos, transparencia y rendición de cuentas, siempre que sea factible técnicamente. En estos mecanismos se incluirán su diseño y datos de entrenamiento, y abordarán su potencial impacto discriminatorio. Para lograr este fin, se «promoverá» la realización de evaluaciones de impacto que determinen el posible sesgo discriminatorio. Asimismo, en su apartado segundo señala que «las administraciones públicas, en el marco de sus competencias en el ámbito de los algoritmos involucrados en procesos de toma de decisiones, priorizarán la transparencia en el diseño y la implementación y la capacidad de interpretación de las decisiones adoptadas por los mismos» (Lertxundi Lertxundi, 2020).

Es decir, desde el punto de vista de la técnica jurídica utilizada en la redacción de este precepto, solo remotamente podemos intuir que el legislador se está refiriendo a un eventual derecho a la información algorítmica y al derecho a la no discriminación algorítmica, evitando los sesgos. Y ello porque no aparecen

formulados directamente y de forma imperativa como derechos que tengan como correlato la correspondiente obligación para la Administración jurídicamente exigible ante un juez. No se utilizan tiempos verbales imperativos. Simplemente se recoge el compromiso de la Administración de «favorecer» y «priorizar» la transparencia en el uso de algoritmos y en la utilización de criterios de minimización de sesgos, y solo cuando ello sea técnicamente posible. Es decir, ampara el legislador la posibilidad de que técnicamente ello no sea factible y que, a pesar de ello, pueda usar estos sistemas de IA. La solución, pues, es muy poco satisfactoria desde una perspectiva de respeto a los derechos fundamentales de los empleados públicos. El uso imperativo, en forma de obligación, solo se utiliza en su apartado tercero cuando se hace referencia a la obligación de la Administración de promover el uso de una Inteligencia Artificial ética, confiable y respetuosa con los derechos fundamentales, siguiendo especialmente las recomendaciones de la Unión Europea en este sentido. Una fórmula muy bonita, pero que puede quedar vacía de contenido si no va acompañada de las correspondientes garantías.

El marco quedaría incompleto si no se tiene también en cuenta como otra pieza más de este complejo puzle la normativa autonómica, que también aporta algunas novedades de interés en esta materia, tanto desde la legislación aplicable a la IA como desde la legislación sobre transparencia y buen gobierno. Ello se puede traducir en marcos jurídicos diferentes para el funcionario público, dependiendo de la comunidad autónoma en la que preste sus servicios. Así, por ejemplo, podemos traer a colación la regulación extremeña que afectaría a sus empleados públicos. El art. 11 del *Decreto-ley 2/2023, de 8 de marzo, de medidas urgentes de impulso a la inteligencia artificial en Extremadura,* regula específicamente los sistema de inteligencia artificial en la toma de decisiones y habilita de forma expresa a la Administración autonómica extremeña para que pueda adoptar actos administrativos mediante sistemas de inteligencia artificial. Pues bien, remite directamente a que dichas decisiones se dicten «de acuerdo con los derechos digitales de la ciudadanía en sus relaciones con las Administraciones Públicas, descritos en la Carta de Derechos Digitales del Gobierno de España y la Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital (2023/C 23/01)». Es decir, el contenido programático de la Carta de Derechos Digitales parece asumir directamente carácter normativo con esta disposición del legislador autonómico. Asimismo, además de los requisitos generales previstos en el art. 41 de la Ley 40/2015, parece reconocer un eventual derecho a la transparencia y a la información al referirse a la necesidad de que se dé «la debida publicidad del mecanismo de decisión, de las prioridades asignadas en el procedimiento de evaluación y de la toma de decisiones, así como de todos los datos que puedan impactar en su contenido».

En otras ocasiones, la regulación de los derechos sobre esta materia se aborda desde el punto de vista de la transparencia y buen gobierno. Así sucede, por ejemplo, con los principios de transparencia y explicabilidad a los que se refiere la letra l) del art. 16 de la *Ley 1/2022, de 13 de abril, de Transparencia y Buen Gobierno de la Comunitat Valenciana,* que ha considerado el derecho a la información como «información de relevancia jurídica» e efectos de imponer obligaciones de publicidad activa a dicha Administración. En consecuencia, obliga a la Administración a publicar la relación de sistemas de inteligencia artificial de alto riesgo de acuerdo con el reglamento de inteligencia artificial que desarrollen o implanten. Asimismo, deben incluir la relación de sistemas automatizados y sistemas de inteligencia artificial de uso general cuyo empleo impacte de manera significativa en los procedimientos administrativos o la prestación de los servicios públicos. La información que debe facilitar la Administración debe incluir la descripción, en un lenguaje claro y sencillo, del diseño, funcionamiento y lógica del sistema, su finalidad, su incidencia en las decisiones públicas, el nivel de riesgo que implica, la importancia y consecuencias previstas para la ciudadanía, el punto de contacto al que poder dirigirse, y en su caso, el órgano u órganos competentes a efectos de impugnación.

Todo ello, claro está, teniendo en cuenta directamente el régimen protector de los derechos digitales que establece el Reglamento general de protección de datos de 2016, pues no hemos de olvidar que los sistemas de IA se nutren de datos y que, al utilizarlos para el diseño o despliegue de la IA, se ha de respetar escrupulosamente su régimen jurídico[37]. Y, obviamente, el operador jurídico también ha de aplicar el Reglamento de Inteligencia Artificial de 13 de junio de 2024 que, tal como proclama, la IA debe ser una tecnología centrada en el ser humano. Aunque se trata de una herramienta que está pensada y regulada para favorecer el mercado, debe ser al mismo tiempo una herramienta para las personas y tener por objetivo último aumentar el bienestar humano, garantizando un elevado nivel de protección de los derechos fundamentales consagrados en la Carta de los Derechos Fundamentales de la Unión Europea. La normativa europea sobre datos, como reconoce el reglamento, garantiza la vida privada, la confidencialidad de las comunicaciones y establece condiciones para cualquier almacenamiento de datos personales y no personales en los equipos terminales y el acceso desde estos. Todo ello nos sitúa ante un marco ciertamente complejo para determinar el nivel concreto de protección de los derechos del em-

pleado público y ante un escenario de inseguridad jurídica, tanto para los empleados como para los responsables de recursos humanos. Sería necesario clarificar dicho escenario y, tal vez, incorporar expresamente en el texto de la ley algunas de las garantías que ha incorporado la jurisprudencia, siguiendo la línea marcada por la STS de 29 de septiembre de 2023, Sala de lo Contencioso-Administrativo, Sección Segunda, núm. 1207/2023, que ha extendido la doctrina sobre la solicitud de autorización judicial para la entrada y registro de un domicilio constitucionalmente protegido también para el acceso al contenido almacenado en un ordenador personal sin el consentimiento de su dueño, exigiendo el escrupuloso cumplimiento de los requisitos de adecuación, necesidad y proporcionalidad en tanto que su finalidad es acotar y controlar, como limitaciones, la invasión de un derecho fundamental.

6. A modo de conclusión: sobre la necesidad de repensar y fortalecer el marco de derechos digitales

Frente a los retos y riesgos que plantean estas nuevas realidades tecnológicas en la gestión del empleo público, especialmente los sistemas de IA, es preciso reflexionar y repensar cómo pueden impactar en los derechos de los empleados públicos para establecer los adecuados mecanismos de protección, ya sea adaptando los derechos fundamentales a los nuevos escenarios, ya sea creando nuevos derechos que fortalezcan su posición jurídica. Es claro que las personas afectadas por la utilización de estos sistemas de IA deben seguir disfrutando de todos sus derechos fundamentales y de los derechos y garantías que les confiere la normativa sobre protección de datos, incluidos los derechos relacionados con las decisiones individuales totalmente automatizadas a las que se refiere el art. 22 del RGPD. Como reconoce el propio RIA, el derecho a la intimidad y a la protección de datos personales debe garantizarse a lo largo de todo el ciclo de vida del sistema de IA (considerando número 69).

A fin de proteger los derechos de los empleados públicos frente a la discriminación que podría provocar el sesgo de los sistemas de IA, se establecen determinadas obligaciones de transparencia para los proveedores de estos sistemas y para los responsables de su despliegue, con la intención de poder garantizar la detección y corrección de los sesgos asociados a los sistemas de IA de alto riesgo. Es necesario garantizar la trazabilidad de los sistemas de IA de alto riesgo, para vigilar su funcionamiento y esencial disponer de información comprensible sobre el modo en que se han desarrollado y sobre su funcionamiento durante toda su vida útil (considerando n.º 71). Dicha información debe incluir las características generales, las capacidades y las limitaciones del sistema y los algoritmos, datos y procesos de entrenamiento, prueba y validación empleados, así como documentación sobre el sistema de gestión de riesgos pertinente, elaborada de manera clara y completa. Posiblemente habría que dar un paso más en la construcción de un nuevo marco jurídico de derechos digitales para los empleados públicos, de modo que todas estas obligaciones puedan tener su correlato en el reconocimiento de un nuevo derecho a la información algorítmica, no solo para los representantes legales de los empleados, sino también para ellos. La normativa laboral solo ha reconocido este derecho para los miembros del comité de empresa.

De la mera lectura de los distintos considerandos del reglamento se podría deducir también la necesidad de garantizar otros derechos nuevos, como el derecho a la supervisión humana, el derecho a la participación en la instauración de estos sistemas por parte de los representantes legales de los empleados públicos, el derecho a la alfabetización en IA o el derecho a la no discriminación algorítmica. Del art. 22 del RGPD se derivaría el derecho del empleado público a no ser objeto de una decisión automatizada cuando dicha decisión le vaya a afectar, lo que podría reformularse expresamente en el derecho a la reserva funcionarial o a la reserva de humanidad en las decisiones de gestión de personal que afecten a sus condiciones de trabajo o a su vínculo con la Administración. Se ha considerado que la IA debe desarrollarse y utilizarse para mejorar la autonomía humana y la toma de decisiones, en lugar de reemplazar o influir indebidamente en el juicio humano.

En todo caso, existen distintos documentos que pueden inspirar la labor del legislador en este punto. En el ámbito europeo es destacable la *Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital* del Parlamento Europeo, el Consejo y la Comisión, publicada en el Diario Oficial de la Unión Europea el 23 de enero de 2023, (C 23/01), que pretende establecer el marco integral que ha de guiar estos procesos de transformación digital, que han de estar basados en los valores europeos y en los derechos fundamentales de la UE, situando a las personas en el centro y reafirmando los derechos humanos universales. Resalta la necesidad de promover que los sistemas de IA sean fiables y éticos, que respondan a un nivel adecuado de transparencia en el uso de los algoritmos y de la inteligencia, así como la necesidad de garanti-

zar que las personas estén informadas y capacitadas para utilizarlos cuando interactúen con ellos. Se mencionan determinados derechos fundamentales que tienen también repercusión específica en el ámbito de las relaciones laborales entre la Administración y sus empleados, especialmente cuando se ponen a su disposición el uso de herramientas tecnológicas o se utilizan dispositivos de videovigilancia o de grabación de sonidos para controlar la actividad laboral del empleado público, garantizando el derecho de toda persona a la confidencialidad de sus comunicaciones y de la información contenida en sus dispositivos electrónicos, y a no ser objeto de vigilancia en línea y seguimiento generalizado ilegal ni de medidas de interceptación.

Aunque dicho documento solo tiene carácter declarativo, establece los objetivos que han de conseguirse, que deberán traducirse en una pléyade de derechos de naturaleza digital para todos los trabajadores y, por tanto, también para los empleados públicos. Se insiste en el derecho a la formación digital y al reciclaje profesional, el derecho a unas condiciones de trabajo equitativas, justas, saludables y seguras, así como a una protección adecuada en el entorno digital. La declaración contiene el compromiso de garantizar que el uso de la inteligencia artificial en el lugar de trabajo sea transparente y siga un enfoque basado en los riesgos, garantizando que las decisiones importantes que afecten a los trabajadores cuenten con supervisión humana y que, en general, se les informe de que están interactuando con sistemas de inteligencia artificial.

En el mismo sentido hemos de tener en cuenta la Carta de Derechos Digitales, que ha de servir de guía para la implantación y desarrollo de este nuevo marco de derechos del empleado público. Como se ha dicho, representa un buen punto de partida para reconfigurar, adecuar y generar las facultades que el personal empleado público necesita para preservar sus derechos fundamentales en el marco de la sociedad digital (Expósito Gázquez, 2022). Aunque no es un reglamento ni tiene carácter normativo, establece el marco de referencia que han de tener en cuenta los poderes públicos para hacer frente al reto que supone la IA. Fue aprobada por el Consejo de Ministros en el año 2021 como la medida n.º 28 de la Estrategia Nacional de Inteligencia Artificial para crear confianza en los ciudadanos sobre la utilización de la IA y con la intención de establecer un marco ético y normativo que refuerce la protección de los derechos individuales y colectivos, a efectos de garantizar la inclusión y el bienestar social.

Ha sido configurada como un marco dinámico y humanista que permita garantizar la protección de los derechos individuales y colectivos de la ciudadanía en el ámbito digital. Con ella se identifican un conjunto de principios fundamentales que deben inspirar la producción normativa para adaptarla a las nuevas situaciones y circunstancias del ámbito digital y, en particular, las relativas a la extensión de la IA. Aunque dicha Carta carece de valor normativo directo para reconocer derechos a los empleados públicos e imponer las correlativas obligaciones a la Administración, debe ser tomada también como un importante marco de referencia porque se ha elaborado precisamente para crear un marco adecuado para el desarrollo tecnológico.

El punto 4 de la Carta regula los derechos en el ámbito laboral, garantizando la dignidad y los derechos fundamentales de las personas trabajadoras en los entornos digitales. A partir de este reconocimiento general, garantiza a las personas trabajadoras, tanto del sector privado como del sector público, un importante listado de derechos, aunque siempre con «arreglo a la normativa vigente», lo que requeriría para su desarrollo la correspondiente intervención por parte del legislador básico, al ser esta intervención requisito imprescindible para la igualdad de estos derechos básicos de todos los empleados públicos en todo el territorio nacional y con total independencia del ámbito territorial de la Administración en la que presten sus servicios.

En este sentido, es resaltable que la Carta pretenda poner límites a las facultades de vigilancia y supervisión digital, toda vez que hace referencia a un »uso lícito, leal, proporcionado y transparente de los controles empresariales digitales». Debería insistirse también en que este uso debería se justificado.

Con mejor técnica jurídica que la empleada en el art. 14.j.bis) del TREBEP reproduce aquellos derechos y mejora el ámbito objetivo y subjetivo de la protección, al mencionar explícitamente otros derechos fundamentales que se ven directamente afectados por estas tecnologías, además del derecho a la intimidad. Así, reconoce la protección de los derechos a la intimidad personal y familiar, al honor, a la propia imagen, a la protección de datos y al secreto de las comunicaciones, no solo en el uso de dispositivos digitales, ante la videovigilancia, geolocalización y la grabación de sonidos, sino también en el caso de que el empleador utilice herramientas de monitoreo, sistemas biométricos, analítica y procesos de toma de decisión en materia de recursos humanos y relaciones laborales y, en particular, la analítica de redes sociales. Igualmente se hace referencia a la necesidad de garantizarlos frente al uso por la entidad empleadora de procedimientos de analítica de datos, inteligencia artificial y, en particular, los previstos en la legislación respecto del empleo de decisiones automatizadas en los procesos de selección de personal. Asimismo, protege frente al acoso por razón de sexo, por causa discriminatoria y acoso laboral utilizando medios digitales.

Proclama también algunos derechos de transparencia e información algorítmica que ya han sido recogi-

dos en el entorno laboral. Así sucede con el derecho a informar a la representación legal de las personas trabajadoras cuando el empleador use tales dispositivos o herramientas digitales, alcanzando dicha información a los parámetros, reglas e instrucciones en los que se basan los algoritmos o sistemas de inteligencia artificial 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. Este derecho alcanza también a la información sobre los cambios tecnológicos que vayan a producirse en los procesos de transformación digital.

De la Carta se deriva también la necesidad de reconocer el derecho a la cualificación digital del empleado para la adquisición de las competencias digitales requeridas en el ámbito laboral o, en los procesos de transformación digital, a recibir una formación adecuada que permita su adaptación a las nuevas condiciones laborales. Por lo demás, se remite a la negociación colectiva para establecer garantías adicionales de los derechos y libertades relacionados con el tratamiento de los datos personales de las personas trabajadoras y la salvaguarda de derechos digitales en el ámbito laboral, así como vehicular la participación de las personas trabajadoras en los procesos de transformación digital y en la determinación de las consecuencias laborales que la misma pueda implicar.

En fin, ante la afectación de los derechos fundamentales de los empleados públicos es preciso avanzar hacia un modelo más sólido de derechos digitales que proporcione una mayor y mejor cobertura de protección ante los riesgos y desafíos que presentan los avances tecnológicos y, en particular, los sistemas de inteligencia artificial, en consonancia con los principios establecidos en la Declaración europea y en la Carta de Derechos Digitales. Es necesario que estos nuevos procesos de cambio vengan acompañados del correspondiente marco regulatorio para garantizar la seguridad jurídica y los derechos de los empleados (Cortés Abad, 2020). Se trata, en definitiva, de que este respaldo normativo sirva para pasar de las declaraciones vacías a las obligaciones jurídicamente exigibles (Cotino hueso, 2013).

7. Bibliografía

Almonacid Lamelas, V. (2024). IA y Recursos Humanos: aplicaciones prácticas en las Administraciones públicas. Post publicado en Nosoloaytos el 3 de octubre. https://nosoloaytos.wordpress.com/2024/10/03/ia-y-recursos-humanos-10-aplicaciones-practicas-en-las-administraciones-publicas/

Asquerino Lampero, M.J. (2022, 26 y 27 de mayo). Algoritmos, procesos de selección y reputación digital: una mirada antidiscriminatoria. *Digitalización, recuperación y reformas laborales. Comunicaciones del XXXII Congreso Anual de la Asociación Española de Derecho del Trabajo y de la Seguridad Social.* Alicante.

Cabellos Espiérrez, M.A. (2024). El derecho a la protección de datos personales ante la videovigilancia en el ámbito laboral: la progresiva devaluación en la jurisprudencia constitucional de la obligación de informar al trabajador. *Revista Vasca de Administración Pública*, 128-I, 17-45. DOI: https://doi.org/10.47623/ivap-rvap.128.2024.1.01

Cantero, J. (2025). Transformación digital y derechos digitales de naturaleza laboral del empleado público local. *El Consultor de los Ayuntamientos*. Abril 2025.

Cerrillo I Martínez, A. (2019). El impacto de la inteligencia artificial en el Derecho administrativo ¿nuevos conceptos para nuevas realidades técnicas? *Revista General de Derecho Administrativo*, 50.

Cortés-Abad, O. (2025). Digitalización de los procesos selectivos en la Administración pública: lecciones desde el Ayuntamiento de Madrid. *Revista de Estudios de la Administración Local y Autonómica,* publicación anticipada, 23. https://doi.org/10.24965/reala.11480

Cortés Abad, O. (2020). Algoritmos y algunos retos jurídico-institucionales para su aplicación en la Administración Pública. *Revista Vasca de Gestión de Personas y Organizaciones Públicas,* 18, 54-63. https://doi.org/10.47623/ivap-rvgp.18.2020.03

Cotino Hueso, L. (2013). Derecho y «Gobierno Abierto». La regulación de la transparencia y la participación y su ejercicio a través del uso de las nuevas tecnologías y las redes sociales por las Administraciones públicas. Propuestas concretas. *Revista Aragonesa de Administración*, número extraordinario 14.

Custers, B. (2022). *Law and Artificial Intelligence. Regulating AI and applying AI in legal practice.* Países Bajos: Leiden University. Volumen 35.

Expósito Gázquez, A. (2022). Los derechos digitales del personal empleado público: ¿realidad plausible o utopía imposible?. *Revista Vasca de Gestión de Personas y Organizaciones Públicas*, n.º 22, 156-169.

Fernández de la Cigoña Fraga, J.R. (2022, 26 de abril). Digitalización de los Recursos Humanos de tu empresa: ventajas e inconvenientes. [Post de CEF Laboral Social].https://www.laboral-social.com/digitalizacion-recursos-humanos-empresa-ventajas-inconvenientes.html

Fernández García, A. (2023). Los algoritmos y la inteligencia artificial en la Ley 12/2021, de 28 de septiembre. En J. Moreno y Gené y A.M Romero Burillo (coords.), *Los nuevos escenarios laborales de la innovación tecnológica.* Tirant Lo Blanch.

Fondevila Antolín, J. (2021). La obligación de utilización de medios electrónicos en los procesos selectivos: ciudadanos o súbditos. *Revisa Vasca de Gestión de Personas y Organizaciones Públicas,* 20, 88-111. https://doi.org/10.47623/ivap-rvgp.20.2021.05

Galindo Caldés, R. (2023). *Transformación digital local y función pública: aspectos organizativos. Estudios de Relaciones Laborales*, 16. Diputación de Barcelona.

Gamero Casado, E. (2022). El tránsito hacia la Administración digital (o la historia interminable). Su conexión con el desarrollo económico y social. En A. Cerrillo Martínez (dir.), *Administración digital.* Dykinson.

Gorriti Bontigui, M. (2018). Innovar en selección desde la evidencia empírica y las nuevas competencias. *Revista Vasca de Gestión de Personas y Organizaciones Públicas*, 14, 66- 85.

Jiménez Asensio, R. (2019, 12 de abril). Seis hipótesis sobre la Administración Pública y la selección de empleados públicos en la próxima década. [Post *La Administración al día*]. https://laadministracionaldia.inap.es/noticia.asp?id=1509526.

Lertxundi Lertxundi, A. (2020). El impacto de la digitalización en los derechos fundamentales del personal empleado público en España. *Revista Vasca de Gestión de Personas y Organizaciones Públicas*, 18, 38-53. https://www.ivap.euskadi.eus/contenidos/informacion/18_revgp/eu_def/Lertxundi_38_53.pdf

Mercader Uguina, J.R. (2001). Derechos fundamentales de los trabajadores y nuevas tecnologías: ¿hacia una empresa panóptica? *Relaciones laborales: Revista crítica de teoría y práctica*, 1, 665-686.

Mercader Uguina, J.R. (2022). En busca del empleador invisible: algoritmos e inteligencia artificial en el derecho digital del trabajo. *El Cronista del Estado Social y Democrático de Derecho,* 100, 136-145.

Ortiz de Zárate Alcarazo, L., Guevara Gómez, A. (2021). *Inteligencia artificial e igualdad de género. Un análisis comparado entre la UE, Suecia y España.* Fundación Alternativas, 101/2021.

Padilla Ruíz, P. (2023). Actuaciones administrativas automatizadas y automatización robótica de procesos en la gestión de personas. *Revista Vasca de Organización de Personal y Organizaciones Públicas*, 24, 52-67.

Ponce Solé, J. (2024). Límites jurídicos de la toma de decisiones discrecionales automatizadas mediante inteligencia artificial: racionalidad, sabiduría y necesaria reserva jurídica de humanidad en el ámbito digital. *Revista General de Derecho Administrativo* 66. Iustel.

Ramió Matas, C. (2018). *Inteligencia Artificial y Administración pública: robots y humanos compartiendo el servicio público*. Catarata.

Rodríguez Escanciano, S. (2024). *Proyección de la Inteligencia Artificial en las relaciones laborales.* Lección inaugural curso académico 2024-2025, Campus de León. León. Servicio de Publicaciones de la Universidad de León.

Rodríguez Escanciano, S. (2019). Posibilidades y control de los correos electrónicos de los empleados públicos. *Revista Vasca de Gestión de Personas y Organizaciones Públicas*, 16, 110-127.

Rodríguez Fernández, L. (2023, 17 de abril). Robots, algoritmos y trabajos. *El País.* https://www.iustel.com//diario_del_derecho/noticia.asp?ref_iustel=1232476&utm_source=DD&utm_medium=email&nl=1&utm_campaign=17/4/2023&popup=

Todolí Signes, A. (2022). La inteligencia artificial no te robará tu trabajo, sino tu salario. Retos del Derecho del Trabajo frente a la dirección algorítmica. *El Cronista del Estado Social y Democrático de Derecho,* 100, 150-159.

Todolí Signes, A. (2023). *Algoritmos productivos y extractivos. Cómo regular la digitalización para mejorar el empleo e incentivar la innovación.* Aranzadi.

Todolí Signes, A. (2025, 19 de febrero). Entra en vigor la obligación de <<alfabetización>> en materia de IA de las empresas hacia sus trabajadores vía Reglamento IA. [Blog *Argumentos en Derecho Laboral]*. https://adriantodoli.com/2025/02/19/entra-en-vigor-la-obligacion-de-alfabetizacion-en-materia-de-ia-de-las-empresas-hacia-sus-trabajadores-via-reglamento-ia/

Notas

1 Este trabajo se ha elaborado en el marco del Convenio entre la entidad pública empresarial Red.es y la Universidad de Castilla-La Mancha para impulsar la implementación de la Carta de Derechos Digitales en el ámbito de los derechos digitales en el entorno laboral y empresarial C039/23-OT.

2 Comunicación de la Comisión, de 26 septiembre 2003, al Consejo, al Parlamento Europeo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre «*El papel de la administración electrónica en el futuro de Europa*». Según se expresa en dicha Comunicación, el término TIC cubre un amplio abanico de servicios, aplicaciones, tecnologías, equipos y programas informáticos, es decir, herramientas como la telefonía e Internet, el aprendizaje a distancia, la televisión, los ordenadores, las redes y los programas necesarios para emplear estas tecnologías. disponible en: https://eur-lex.europa.eu/ES/legal-content/summary/egovernment.html?fromSummary=24

3 un algoritmo es un sistema, conjunto o secuencia de reglas u operaciones lógicas que permite realizar cálculos de distinto tipo y, por lo tanto, encontrar soluciones a eventuales problemas o demandas.

4 *Libro Blanco sobre la inteligencia artificial. Un enfoque europeo orientado a la excelencia y la confianza,* Comisión Europea, Bruselas, 19 de febrero de 2020, COM (2020) 65 final.

5 Estrategia de Inteligencia Artificial 2024, Ministerio para la Transformación Digital y de la Función Pública, 2024, disponible en: https://portal.mineco.gob.es/es-es/digitalizacionIA/Documents/Estrategia_IA_2024.pdf

6 Definición utilizada por la Recomendación de la UNESCO sobre Ética de la inteligencia artificial, adoptada por la Conferencia General el 23 de noviembre de 2021.

7 Así, por ejemplo, el art. 13 del *Real Decreto 2073/1999, de 30 de diciembre, por el que se modifica el Reglamento del Registro Central de Personal y las normas de coordinación con los de las restantes Administraciones públicas*, establece un listado de 20 tipos de datos que han de recogerse en el Registro Central de Personal para cada funcionario y que constituyen una perfecta radiografía de lo que el funcionario es, hace y ha hecho en la Administración.

8 Según la información solicitada a la Agencia Estatal de Administración Digital (AEAD), en la actualidad, las aplicaciones de gestión de personal no hacen uso de tecnologías de inteligencia artificial, Big Data, etc. Las aplicaciones permiten la digitalización de los procedimientos y contribuyen a una mayor eficiencia en la gestión. Sin embargo, en ningún caso se automatiza la toma de decisiones en la resolución de expedientes, siendo esta responsabilidad exclusiva de los gestores encargados de las aplicaciones. Por otro lado, se utilizan cuadros de mando relacionados con la gestión del personal, siempre con datos anonimizados. Estos cuadros de mando permiten la publicación de boletines, informes para toma de decisiones, etc.

9 El *Machine Learning* implica la capacidad del sistema para aprender automáticamente mediante la identificación de patrones complejos en grandes volúmenes de datos. El *Deep Learning* es un modelo que evalúa ejemplos y aplica un número reducido de instrucciones cuando surge un error, en vez de establecer múltiples reglas para resolver un problema. El *Text Mining* permite buscar palabras clave o conceptos relacionados con parámetros previamente establecidos. El *Entity Recognition*, es un algoritmo que extrae información y la clasifica en categorías predefinidas, como lugares, fechas o personas.

10 Ministerio para la Transformación Digital y de la Función Pública, *Consenso por una Administración abierta. Proyecto 1: IA generativa y espacios de datos,* INAP, 2024, pág. 35. La instauración de sistemas de chatbots a través de IA generativa, que pueden facilitar información a los ciudadanos y gestionar sus consultas, son un importante ejemplo de ello. Posibilitan fácilmente el ejercicio del derecho que tienen los ciudadanos a obtener información y orientación, descargando al funcionario de estas tareas para que pueda centrarse realmente en aquello que aporte más valor a la organización. Disponible en: https://www.inap.es/documents/10136/2342224/GT1-%20IAGenerativaYEspaciosDeDatos.pdf/5ae519f3-fad5-ac66-ffa7-068b73eec720

11 Por su interés, nos remitimos al documento elaborado por la Autoridad Catalana de Protección de Datos, *Modelo para la EIDF: guía y casos de uso Metodología aplicada de la avaluación de impacto sobre los derechos fundamentales en el diseño y desarrollo de la IA,* 2025, disponible en: https://www.dpdenxarxa.cat/pluginfile.php/2468/mod_folder/content/0/FRIA_es_2.pdf

12 Art. 41 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y art. 13 del Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.

13 Para profundizar nos remitimos a PONCE SOLÉ, Juli, «Límites jurídicos de la toma de decisiones discrecionales automatizadas mediante inteligencia artificial: racionalidad, sabiduría y necesaria reserva jurídica de humanidad en el ámbito digital», *Revista General de Derecho Administrativo* n.º 66, Iustel, mayo 2024.

14 Ministerio para la Transformación Digital y de la Función Pública, *Consenso por una Administración abierta. Proyecto 1: IA generativa y espacios de datos,* INAP, 2024, pág. 10, disponible en: https://www.inap.es/documents/10136/2342224/GT1-%20IAGenerativaYEspaciosDeDatos.pdf/5ae519f3-fad5-ac66-ffa7-068b73eec720

15 Como aclara el Grupo de Trabajo del art. 29, la elaboración de perfiles puede usarse para hacer predicciones sobre personas, utilizando datos de distintas fuentes para inferir algo sobre un individuo, sobre la base de las cualidades de otros que parecen similares estadísticamente. Por ello podría usarse, por ejemplo, en los procesos selectivos, en la provisión de puestos de trabajo, en la movilidad y en la carrera profesional.

16 Para una visión general de este nuevo marco de derechos nos remitimos al *Observatorio de Derechos Digitales*, https://www.derechosdigitales.gob.es/es/derechos-digitales

17 Artículo 3, apartado 13 de la Directiva sobre protección de datos en el ámbito penal; artículo 4, apartado 14, del RGPD; artículo 3, apartado 18, del Reglamento (UE) 2018/1725.

18 *El Gobierno da luz verde al anteproyecto de ley para un uso ético, inclusivo y beneficioso de la Inteligencia Artificial*, fecha de consulta, el 12 de marzo de 2025. Disponible en: https://laadministracionaldia.inap.es/noticia.asp?id=1516706&nl=1&utm_source=newsletter&utm_medium=email&utm_campaign=12/3/2025

19 *Directrices 05/2022 del Comité Europeo de Protección de Datos (CEPD), sobre el uso de reconocimiento facial en el ámbito de las fuerzas de orden público, Versión 2.0*, op. cit., pág. 6. Concluyen que las tecnologías que utilizan datos biométricos están vinculados de forma permanente e irrevocable a la identidad de una persona, por lo que tienen un impacto directo o indirecto en una serie de derechos y libertades fundamentales consagrados en la Carta de los Derechos Fundamentales de la UE que pueden ir más allá de la privacidad y la protección de datos, como la dignidad humana, la libertad de circulación, la libertad de reunión, etc. Por ello, el sistema de reconocimiento facial no cumple los requisitos de necesidad y proporcionalidad y constituye una interferencia desproporcionada en los derechos de los interesados al respeto de la vida privada y la protección de los datos personales en virtud de la Carta (pág. 56).

20 Ministerio para la Transformación Digital y de la Función Pública, *Consenso por una Administración abierta. Proyecto 1: IA generativa y espacios de datos,* INAP, 2024, pág. 10, disponible en: https://www.inap.es/documents/10136/2342224/GT1-%20IAGenerativaYEspaciosDeDatos.pdf/5ae519f3-fad5-ac66-ffa7-068b73eec720

21 Agencia Española de Protección de Datos, *Guía sobre tratamientos de control de presencia mediante sistemas biométricos,* noviembre de 2023, págs. 13 y 14.

22 Estamos siguiendo de modo directo el *Libro Blanco sobre Inteligencia Artificial..., op. Cit.*, págs. 13 a 17.

23 Ministerio para la Transformación Digital y de la Función Pública, *Consenso por una Administración abierta. Proyecto 1: IA generativa y espacios de datos,* INAP, 2024, págs. 36 y ss., disponible en: https://www.inap.es/documents/10136/2342224/GT1-%20IAGenerativaYEspaciosDeDatos.pdf/5ae519f3-fad5-ac66-ffa7-068b73eec720

24 Esto es, como establece la AEPD, si la finalidad de la geolocalización es el registro horario, los datos no podrán ser utilizados para verificar la ubicación de la persona trabajadora en cada momento, sino las horas de inicio y fin de la actividad, que es lo que permite la base jurídica del registro horario (art. 34.9 del ET). Agencia Española de Protección de Datos, *La protección de datos en las relaciones laborales, mayo de 2021, pág. 53.*

25 En el mismo sentido la STS de 26 de abril de 2023, Sala de lo Social, sec. 1.ª ha declarado legal el despido del camarero de un afamado restaurante de Albacete por no haber emitido y entregado los tickets a los clientes, y haberlos borrado luego y no registrado, comportamiento que fue descubierto a raíz de las grabaciones tomadas por las cámaras visibles instaladas en el establecimiento.

26 Se sigue la doctrina de la **STEDH de 17 de octubre de 2019 (números 1874/13 y 8567/13) (asunto López Ribalda II),** en la que se abordó el uso de cámaras de vigilancia ocultas en el lugar de trabajo y su relación con los derechos a la privacidad de los empleados. En este caso, varias trabajadoras de un supermercado fueron despedidas tras ser grabadas sin su conocimiento a través de cámaras de videovigilancia ocultas en el establecimiento que había instalado el dueño ante la sospecha de que algunas empleadas estaban robando productos, sin que ellas estuvieran al tanto de la vigilancia. La sentencia es relevante porque establece que el derecho a la privacidad de los trabajadores no es absoluto y puede ser limitado en ciertos contextos, especialmente cuando hay un interés legítimo de la empresa, como la protección de la propiedad. Sin embargo, también resalta la necesidad de un equilibrio entre la seguridad del empleador y los derechos fundamentales del trabajador.

27 El valor que tiene el consentimiento de un empleado público como base jurídica cuando la Administración pretende hacer un tratamiento de sus datos es bastante limitado, dado el desequilibrio de poder que suele producirse entre las relaciones de aquéllos con los interesados, que impide que el consentimiento pueda considerarse libre. *Directrices 05/2022 del Comité Europeo de Protección de Datos (CEPD), sobre el uso de reconocimiento facial en el ámbito de las fuerzas de orden público, Versión 2.0*, elaboradas el 26 de abril de 2023, disponibles en: https://www.edpb.europa.eu/system/files/2024-05/edpb_guidelines_202304_frtlawenforcement_v2_es.pdf

28 La STSJ Asturias de 24 de octubre de 2023, Sala de lo Social, Sección 1.ª, declara que el uso del correo electrónico está amparado por derecho al secreto de comunicaciones y el derecho a la intimidad, aunque su fiscalización por parte del empresario dependerá de cada caso concreto. En el supuesto analizado en la sentencia considera que no se produce ninguna violación porque no podía tener expectativa de privacidad, en la medida en que el convenio colectivo vetaba su uso privado si no era previamente autorizado. El trabajador había sido despedido y solicitó que le remitieran los correos a otra dirección electrónica. El gerente, no obstante, dio orden de imprimir los correos electrónicos que se recibieran en la cuenta del trabajador, así como que se remitieran a su asesoría y se remitieron hasta cuatro sobres que contenían los mensajes recibidos en el antiguo correo del trabajador. La atribución de cuentas corporativas deben ser valoradas según las medidas empresariales de vigilancia y control, que son variables en función de la propia configuración de las condiciones de disposición y uso de las herramientas informáticas y de las instrucciones que hayan podido ser impartidas por el empresario a tal fin» (FJ 5)

29 Pueden consultarse en este sentido la STEDH de 3 de abril de 2007 (caso Copland contra Reino Unido), que consideró tempranamente que «los correos electrónicos enviados desde el lugar del trabajo» están incluidos en el ámbito de protección del art. 8 del Convenio europeo para la protección de los derechos humanos y de las libertades fundamentales, por cuanto pueden contener datos sensibles que afecten a la intimidad y al respeto a la vida privada (apartados 41 y 44).

30 El artículo 4.14 del RGPD define los datos biométricos como datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirman la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos. Los sistemas biométricos más utilizados son la huella digital, una foto facial, la voz, el iris y el patrón de venas de la palma o el dedo.

31 Agencia Española de Protección de Datos, *Guía sobre tratamientos de control de presencia mediante sistemas biométricos,* noviembre de 2023, págs. 5 y 21. Las Directrices están disponibles en: https://www.edpb.europa.eu/system/files/2023-05/edpb_guidelines_202304_frtlawenforcement_v2_en.pdf

32 Dicho informe está disponible en: https://apdcat.gencat.cat/es/documentacio/resolucions-dictamens-i-informes/cercadorOn/cercador-detall/CNS-2-2022-00001. Asimismo, nos remitimos para profundizar en este tipo de evaluaciones de impacto en los derechos fundamentales a la guía elaborada por la Autoridad Catalana de Protección de Datos: https://www.dpdenxarxa.cat/pluginfile.php/2468/mod_folder/content/0/FRIA_es_2.pdf

33 Agencia Española de Protección de Datos, *Guía sobre tratamientos de control de presencia mediante sistemas biométricos,* noviembre de 2023.

34 Según el Dictamen 3/2012 del Grupo de Trabajo del Artículo 29, sobre la evolución de tecnologías biométricas, adoptado el 27 de abril de 2012, 00720/12/ES WP193, al analizar la proporcionalidad de un sistema biométrico hay que ponderar si la pérdida de intimidad resultante

Núm. 28 zk./2025. Págs. 46-74 or.
ISSN: 2173-6405 e-ISSN: 2531-2103

es proporcional a los beneficios esperados. Si el beneficio es relativamente menor, como una mayor comodidad o un ligero ahorro, entonces la pérdida de intimidad no es apropiada. Informe disponible en: https://www.aepd.es/documento/wp193_es.pdf

35 En este sentido, podría considerarse que existe consentimiento libre si el interesado dispone de una alternativa para cumplir con el control horario o controlar su presencia o ejecución del horario, siendo éste quien elige y presta su consentimiento al tratamiento de sus datos biométricos a través de sistemas de reconocimiento facial, pero no parece que sea así en un caso como el descrito en la consulta. En cualquier caso, antes de la implantación de un sistema de este tipo, hace falta hacer una evaluación del impacto sobre la protección de datos a la vista de las circunstancias concretas en que se lleve a cabo el tratamiento para determinar la licitud y la proporcionalidad, incluida el análisis de la existencia de alternativas menos intrusivas, y establecer las garantías adecuadas.

36 La utilización de estos sistemas también plantea importantes dudas jurídicas cuando se insertan como decisiones automatizadas que puedan producir efectos sobre el empleado. Pensemos, por ejemplo, en que no permiten el acceso del empleado a otras dependencias del centro de trabajo. En estos casos es preciso aplicar los derechos recogidos en el art. 22 del RGPD, esto es, el derecho a la intervención humana, a expresar su punto de vista y el derecho a impugnar la decisión. Agencia Española de Protección de Datos, *Guía sobre tratamientos de control de presencia mediante sistemas biométricos,* noviembre de 2023, págs. 12, 22 y 30.

37 Asimismo, habría que tener en cuenta el Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo de 14 de noviembre de 2018 relativo a un marco para la libre circulación de datos no personales en la Unión Europea, así como la Directiva (UE) 2019/1152 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, relativa a unas condiciones laborales transparentes y previsibles en la Unión Europea.

Núm. 28 zk./2025. Págs. 46-74 or.
ISSN: 2173-6405 e-ISSN: 2531-2103