La transformación tecnológica y los derechos de los trabajadores

Technological Change and Workers' Rights

Es indudable que los avances tecnológicos han deparado grandes avances en la calidad del empleo, pero una aplicación sin límites jurídicos de cualquier tecnología puede resultar invasiva respecto de ciertos derechos, fundamentales y ordinarios. Por este motivo, el Derecho encarna un código que pretende restaurar el desequilibrio que puede originarse de aplicar masivamente estas tecnologías sobre personas que no son mercancías de intercambio por salario. Existe una notable legislación europea y española que protege a los trabajadores frente a la tecnología, en especial sobre el tratamiento de sus datos personales por parte de la empresa. Sin embargo, algunos operadores jurídicos están cayendo en interpretaciones incorrectas del maremágnum normativo. La escasa, aún, legislación vigente sobre la IA en España y la incipiente legislación europea apuntan por el buen camino, desde la premisa de calificar de "alto riesgo" –respecto a la merma de derechos fundamentales que pueden suponer–, el empleo de esta tecnología en los espacios laborales. Habrá que esperar a comprobar si las garantías que se recogen en el recién aprobado Reglamento Europeo sobre la IA son eficaces.

Zalantzarik gabe, aurrerapen teknologikoek aurrerapen handiak ekarri dituzte enpleguaren kalitatean, baina edozein teknologia muga juridikorik gabe aplikatzea inbaditzailea izan daiteke zenbait eskubide oinarrizko eta arrunten aurrean. Hori dela eta, Zuzenbideak kode bat gorpuzten du, teknologia horiek pertsonen gainean modu masiboan aplikatzean sor daitekeen desoreka berrezarri nahi duena; izan ere, pertsonak ez gara soldaten truke salgaiak. Argi dago langileak teknologiaren aurrean babesten dituen Europako eta Espainiako legeria nabarmena dagoela, batez ere enpresak datu pertsonalak tratatzeari dagokionez. Hala ere, operadore juridiko arau-maremagnumaren interpretazio okerretan erortzen ari dira. Espainian AAri buruz indarrean dagoen legedi urriak eta Europako legedi hasiberriak bide onetik doaz, "arrisku handikotzat" jotzeko premisatik –horrek ekar ditzakeen oinarrizko eskubideen murrizketari dagokionez–, teknologia hori lan-eremuetan erabiltzea. AAri buruzko Europako Erregelamendu onartu berrian jasotzen diren bermeak eraginkorrak diren egiaztatu arte itxaron beharko da.

There is no doubt that technological advances have brought great advances in the quality of employment, but an application without legal limits of any technology can be invasive with respect to certain rights, fundamental and ordinary. For this reason, the Law embodies a code that aims to restore the imbalance that can result from the massive application of these technologies on people who are not commodities to be exchanged for wages. It is clear that there is notable European and Spanish legislation that protects workers from technology, especially on the processing of their personal data by the company. However, some legal operators are falling into incorrect interpretations of the normative "mare magnum". The scarce legislation in force on AI in Spain, and the incipient European legislation, point in the right direction, from the premise of classifying the use of this technology in the workplace as "high risk" – in terms of the reduction of fundamental rights that it may entail. We will have to wait and see if the guarantees contained in the recently approved European Regulation on AI are effective.

Edurne Terradillos Ormaetxea
Derecho del Trabajo y de la Seguridad Social
Facultad de Derecho, UPV/EHU

Índice

Palabras clave: tecnología, relaciones laborales, garantías, trabajadores.

Keywords: technology, labour-relations, guarantees, workers.

Nº de clasificación JEL: J50, J83, O31

Fecha de entrada: 30/04/2024 Fecha de aceptación: 15/05/2024

1. INTRODUCCIÓN

En el estudio anual del año 2018 sobre la evolución social y del empleo, la Comisión Europea (2018a) anunciaba que entre el 37% y el 69% de los puestos de trabajo podrían ser parcialmente automatizados en un futuro próximo. Las nuevas tecnologías incrementaron el número de personas trabajadoras atípicas y autónomas (Comisión Europea, 2018a), lo que se tradujo como una aportación beneficiosa en cuanto redundaba en una mayor flexibilidad y mejor equilibrio entre la vida profesional y personal. No obstante, también se observó una relación entre el aumento del trabajo atípico y el deterioro de las condiciones laborales, que incluía una mayor inestabilidad de ingresos, menor seguridad en el empleo y acceso limitado a la protección social, especialmente respecto de las personas trabajadoras de plataformas digitales.

El objeto de este trabajo se enfoca en identificar la repercusión de la tecnología aplicada en el lugar de trabajo. Las Tecnologías de la Información y la Comunicación (TIC) comprenden el conjunto de recursos y soluciones tecnológicas que posibilitan la recopilación, procesamiento, almacenamiento y transmisión de in-

El trabajo se enmarca en el Grupo de Investigación consolidado del Gobierno Vasco (IT1630-22) "Un nuevo modelo de Gobernanza empresarial sostenible en la era de la internacionalización y la digitalización", dirigido por Álvarez Rubio, así como en el Proyecto de Investigación MINECO (ID2021-122537NB-I00) "La negociación colectiva como instrumento de gestión anticipada del cambio social, tecnológico, ecológico y empresarial" (Cruz Villalón/Rodríguez Ramos)

formación de todo tipo, información que se traduce en datos, y que en el espacio de las relaciones laborales se alimentan de los datos personales de las personas trabajadoras.

Los dispositivos que posibilitan ese acopio de datos personales son de diverso tipo, y se corresponden con teléfonos inteligentes, ordenadores de mesa, cámaras de videovigilancia, tabletas, vehículos y tecnología factible. Si la ley no actúa sobre el tratamiento de los datos, e impone límites u obligaciones al empleador, existe un alto riesgo de que el interés inicialmente legítimo de los empleadores en la mejora de la eficiencia y protección de los activos de la empresa se convierta en un control ilegítimo y desviado. En consecuencia, este seguimiento puede vulnerar los derechos fundamentales de los trabajadores a la intimidad, el secreto de las comunicaciones o la protección de datos personales, sin que importe que el control a través de las TIC se lleve a cabo de forma continuada u ocasional.

Por otra parte, en el mundo actual, todavía no existe una regulación jurídica en vigor que cuente con el propósito de limitar los riesgos y abusos de derechos que provocan los sistemas de algoritmos respecto de las organizaciones colectivas de los trabajadores. Por ejemplo, la Declaración Universal de los Derechos Humanos protege a los trabajadores para organizarse, pero algunos sistemas de IA están siendo usados para perjudicar esa organización. La falta de ejecución y/o regulación provee un incentivo para el uso de sistemas/prácticas algorítmicas que causan muchas veces efectos profundamente negativos para el bienestar de los trabajadores. Los sindicatos afirman que los sistemas de IA se utilizan con una absoluta falta de transparencia (no saben qué sistema algorítmico de dirección de los trabajadores es usado). El Reglamento europeo General de Protección de Datos prevé en su art. 35 que el empleador realice una Evaluación de Protección e Impacto de Datos. A pesar de que los expertos han propugnado que dicha evaluación se organice a modo de diálogo con una "parte representante de los empleados", la realidad corrobora que pocos sindicatos reportan alguna consulta/diálogo.

Los riesgos y daños ya constatados que se proyectan sobre los trabajadores (CCOO Industria, 2016) son los siguientes: intensificación del trabajo, jornadas de trabajo más largas e intensas; discriminación/sesgos en prácticas automatizadas de recursos humanos; presión para la salud mental y física; pérdida de cualificación y desempleo –formas de trabajo contingentes en alza–; menores salarios, inseguridad económica, menos movilidad en el mercado de trabajo; supresión de la sindicalización; pérdida de autonomía y dignidad con respecto a las prácticas de control y vigilancia, además de la pérdida de privacidad.

A lo largo de este trabajo, me ceñiré a las operaciones de tratamiento de datos derivadas del uso de las TIC y de la IA en el lugar de trabajo. Por motivos de espacio, se descarta analizar otros escenarios[1].

2. TECNOLOGÍA DIGITAL APLICADA A LAS RELACIONES LABORALES "VERSUS" DERECHOS FUNDAMENTALES Y DERECHOS DIGITALES DE LAS PERSONAS TRABAJADORAS

2.1. Derecho a la protección de datos. Aproximación a su régimen jurídico y a las normas jurídicas que lo contemplan

El derecho a la protección de datos tiene el reconocimiento de derecho fundamental en el ordenamiento español, lo que se traduce en una serie de garantías reforzadas de las personas titulares del mismo, garantías que se concretan, por ejemplo, en que cuando existan indicios de la vulneración de este derecho, las personas podrán acudir a un procedimiento judicial sumario (más rápido) y preferente (respecto de otros procedimientos judiciales), y que cuando ese procedimiento finalice, podrán acudir, en recurso de amparo, hasta la máxima instancia interpretadora de la Constitución, el Tribunal Constitucional (art. 53.2 Constitución Española).

De conformidad con el art. 8 de la Carta de Derechos Fundamentales de la UE (en adelante, la Carta)[2] –Tratado internacional que tiene normas específicas de aplicación a los Estados miembros–, "Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan". La mención del sujeto titular del derecho es muy amplia, lo más amplia que podría ser. Y, sin embargo, costó que los empleados –tanto los del sector privado como los del sector público– fueran amparados por la normativa europea de protección de datos que ha estado vigente hasta hace bien poco y que bebía de las fuentes de la Directiva 95/46/CE del Parlamento y del Consejo, de 24 de octubre de 1995, relativa a la protección de datos de las personas y de la libre circulación de datos (Terradillos Ormaetxea, 2017).

---

1 Se descarta abordar, por ejemplo, las operaciones de tratamiento de datos durante el proceso de selección (inspección de las redes sociales de los posibles candidatos) o el uso de las TIC fuera del lugar de trabajo, en incremento exponencial debido al crecimiento de las políticas de trabajo a domicilio, el trabajo a distancia y la utilización por el trabajador de su propio dispositivo. Tampoco se abordará el derecho a la desconexión digital, reconocido legalmente en España, dado que el referido derecho se conecta con el tiempo de descanso, reconocimiento que proclama la no utilización de la tecnología en dichos espacios temporales. Por último, se ha decidido no acometer el tratamiento sensible que supone gestionar datos que reúnen la condición de "categorías especiales" (art. 8 RGPD). Dichos datos "especiales" aluden a la ideología, afiliación sindical, religiosa, orientación sexual o creencias u origen racial o étnico de los trabajadores (art. 9 LOPDGDD), y su tratamiento está prohibido (sin perjuicio de las excepciones consignadas en el art. 9.2 RGPD; esto es, que exista un consentimiento explícito o que una norma con rango legal –o convenio colectivo– obligue a la empresa a tratar los datos biométricos).

2 http://europarl.europa.eu/charter/pdf/text_es.pdf (último acceso: 4 de septiembre de 2019).

La Carta no describe qué datos son de carácter personal, ni menos aún cómo pueden obtenerse pero, ya en el segundo apartado del art. 8, se refiere a alguno de los principios que deben alumbrar la recogida y tratamiento de los datos, así como a la relación causa-fin exigible entre la recogida y el tratamiento: "Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley". Una vez recogidos los datos, la persona no pierde el control sobre ellos, ni siquiera mediando su consentimiento o un interés legítimo que lo haya justificado. Al contrario, continúa la Carta, "La persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación". Es importante advertir, no obstante, que los derechos recogidos en la Carta tienen eficacia directa –es decir, la Carta se aplica a los ciudadanos europeos y estos pueden alegar su incumplimiento ante un órgano judicial– *cuando se aplica el Derecho de la Unión*[3] (y no lo tendrán, por tanto, cuando se aplique el Derecho de los Estados miembros), por lo que es realmente importante conocer qué prevé este Derecho sobre la protección de datos de los trabajadores. Asimismo, el art. 16 del Tratado de Funcionamiento de la Unión Europea reconoce ese derecho, e invoca al Parlamento Europeo y al Consejo a que establezcan sus normas de desarrollo con arreglo al procedimiento legislativo ordinario.

El art. 88 del Reglamento europeo sobre protección de datos actualmente en vigor[4] (en adelante, RGPD) hace referencia, por primera vez, al tratamiento de datos personales en el ámbito laboral, aludiendo a los "trabajadores" en sentido amplio. Con ser bienvenida esa emersión de la materia laboral al espectro legislativo, no obstante, hay que añadir que el precepto apenas regula materias laborales donde el derecho a la protección de datos personales de los trabajadores puede verse afectado, y opta por remitirse, en demasiadas ocasiones (Goñi Sein, 2018), a otras fuentes normativas. En concreto, dicho precepto contempla en su primer apartado, que "Los Estados miembros podrán, a través de disposiciones legislativas o de convenios colectivos, establecer normas más específicas para garantizar la protección de los derechos y libertades en relación con el tratamiento de datos personales de los trabajadores en el ámbito laboral, en particular a efectos de contratación de personal, ejecución del contrato laboral, incluido el cumplimiento de las obligaciones establecidas por la ley o por el convenio colectivo, gestión, planificación y organización del trabajo, igualdad y diversidad en el lugar de trabajo, salud y seguridad en el trabajo, protección de los bienes de empleados o clientes, así como a efectos del ejercicio y disfrute, individual o colectivo, de los derechos y prestaciones relacionados con el empleo y a efectos de la extinción de la relación laboral". La inmediata invo-

3 Las cursivas son de la autora.

4 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).

cación a los Estados miembros, si acaso a los interlocutores sociales que gestan convenios colectivos, da cuenta de la delegación de funciones que realiza el RGPD, sin perjuicio de lo que se añadirá después.

A continuación, el apartado segundo del art. 88 del RGPD dispone que las normas más específicas que desarrollen el derecho a la protección de datos de los trabajadores incluirán medidas adecuadas y específicas para preservar la dignidad humana de los interesados, así como sus intereses legítimos y sus derechos fundamentales, prestando especial atención a la transparencia del tratamiento, a la transferencia de los datos personales dentro de un grupo empresarial o de una unión de empresas dedicadas a una actividad económica conjunta y a los sistemas de supervisión en el lugar de trabajo.

En España, la norma jurídica que ha desarrollado el art. 88 RGPD es la Ley orgánica 3/2018, de protección de datos y garantía de los derechos digitales (en adelante LOPDGDD), pero debe tenerse en cuenta que el propio Reglamento europeo es directamente aplicable en España (art. 288 TFUE[5]). Además, desde la aprobación de la Constitución Española en 1978, el art. 18.4 contempla que la ley limitará el uso de la informática para garantizar el honor y la intimidad personal familiar de los ciudadanos y el pleno ejercicio de sus derechos; y una ley orgánica de 1982 desarrolló ese derecho, aunque sin reparar en los "datos".

El derecho a la protección de datos personales representa un derecho más específico que el derecho a la intimidad, también contemplado en el art. 18 CE, apdo. 1. El Tribunal Constitucional, en una temprana sentencia de 2000 (STC 292/2000, Fundamento Jurídico 4º) sostuvo ya que el derecho fundamental a la intimidad (art. 18.1 CE) no aporta por sí sólo una protección suficiente frente a esta nueva realidad derivada del progreso tecnológico. Sin embargo […] con la inclusión del vigente art. 18.4 CE, el constituyente puso de relieve que era consciente de los riesgos que podría entrañar el uso de la informática y encomendó al legislador la garantía tanto de ciertos derechos fundamentales como del pleno ejercicio de los derechos de la persona. Esa misma sentencia añadió que "El derecho a la protección de datos garantiza a los individuos un poder de disposición sobre esos datos. Esta garantía impone a los poderes públicos la prohibición de que se conviertan en fuentes de esa información sin las debidas garantías; y también el deber de prevenir los riesgos que puedan derivarse del acceso o divulgación indebidas de dicha información. Pero ese poder de disposición sobre los propios datos personales nada vale si el afectado desconoce qué datos son los que se poseen por terceros, quiénes los poseen, y con qué fin". En definitiva, el máximo intérprete de la Constitución avaló que el derecho a la protección de datos (en adelante DPD) tiene un objeto más amplio que el derecho a la intimidad, en tanto

5 El artículo prevé que "El reglamento tendrá un alcance general. Será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro".

que "el objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal. Por consiguiente, también alcanza a aquellos datos personales públicos que, por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos. También por ello, el que los datos sean de carácter personal no significa que sólo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo"[6].

Volviendo a la ley orgánica actualmente en vigor, es importante destacar, en primer lugar, que esta norma se encomienda a concretar (se trata de una norma más específica) lo recogido en el Reglamento europeo que, por su naturaleza jurídica, es aplicable directamente en los Estados miembros. Los mandatos de la LOPDGDD específicos que regulan los derechos de los trabajadores afectados por la tecnología y la digitalización se corresponden con los arts. 87 a 91 de la ley. Sin embargo, esta matización no es obstáculo para subrayar que tanto el contenido general del RGPD, aplicable a las personas que no son trabajadoras, como el contenido general de la LOPDGDD, se proyectan también sobre los trabajadores. A la ley, en su totalidad, se remite el actual art. 20 bis) ET, situado en el espacio del poder de dirección de la persona empleadora, como límite del mismo, cuando hubiera sido más acertado reconocer sistemáticamente esos derechos junto a los derechos fundamentales de las personas trabajadoras (Baylos Grau, 2019).

De ahí que los empleados –también los públicos– cuenten, en principio, con el derecho a la protección de datos en toda su plenitud (véase el art. 2 LOPDGDD, referido al ámbito de aplicación, donde también se recogen los tratamientos excluidos de la ley, ninguno relacionado con el ámbito de las relaciones laborales). Así, el importante documento redactado por el Grupo de Trabajo sobre protección de datos del artículo 29 (GT29) (Grupo de Trabajo, 2017), cuyo objeto es evidenciar las obligaciones adicionales que el RGPD impone a los empresarios, señala que "los empre-

6 En una reciente sentencia, el Tribunal de Justicia de la Unión Europea (en adelante TJUE) ha establecido una interpretación amplia tanto del concepto de "dato personal" como del concepto de "tratamiento de datos", en aras al objetivo declarado del RGPD de garantizar un nivel uniforme y elevado de protección de las personas físicas dentro de la Unión y reforzar y especificar los derechos de los interesados (considerandos 10 y 11 RGPD, y apartado 55 de la sentencia del TJUE de 22 de junio de 2023, C-579/21, Pankki S).

sarios deben tener siempre presentes los principios fundamentales de protección de datos, independientemente de la tecnología empleada"; para añadir, a continuación, que los avances tecnológicos hacen que sea "*más* importante que los empresarios respeten dichos principios".

A mayor abundamiento, de conformidad con el art. 6 del Reglamento y del Título II de la LOPDGDD, los principios que alumbran la protección de datos licitud, lealtad y transparencia, limitación de la finalidad, minimización de datos, exactitud, limitación del plazo de conservación de los datos, integridad y confidencialidad, responsabilidad proactiva del responsable de los datos (el empleador)–, el tratamiento que debe hacerse de las categorías especiales de datos (art. 9 tanto del RGPD como de la LOPDGDD); como, de acuerdo con el Capítulo III del RGPD y el Título III de la LOPGDD, los principios de los interesados (esto es, de los empleados) –transparencia, información y acceso a los datos, rectificación y supresión, derecho de oposición, derecho sobre las decisiones individuales automatizadas–, todos ellos deben ser asimismo irradiados sobre las relaciones laborales, aunque con las matizaciones que realizan los artículos citados de la LOPDGDD.

2.2. Protección de la persona trabajadora frente a la monitorización de su ordenador

El art. 87 LOPDGDD comienza proclamando el derecho de los trabajadores y los empleados públicos a la protección de su intimidad en el uso de los dispositivos digitales puestos a su disposición por su empleador.

Una vez reconocido ese derecho a favor del trabajador, ese mismo precepto comienza a limitar su expansión, restricción que corre a cargo del empleador; de modo que éste podrá acceder a los contenidos derivados del uso de medios digitales facilitados a los trabajadores "a los solos efectos de controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la integridad de dichos dispositivos". En este enunciado es fácil reconocer el principio de limitación de la finalidad del tratamiento de datos personales invocado por el RGPD, que se manifiesta en una doble vertiente. Se parte de la premisa de que los ordenadores son propiedad de la empresa, pero a través de ellos las personas trabajadoras no sólo desempeñan la prestación laboral, sino que pueden también utilizarlos para contener ficheros privados con documentos, fotos, vídeos… (datos personales), así como emplearlos para enviar comunicaciones por mensajería electrónica (actividad amparada por el derecho fundamental al secreto de las comunicaciones[7]). Por este motivo, si bien es cierto que el empleador podrá monitorizar los ordenadores puestos a disposición de los trabajadores, sin embargo, el acceso se debe limitar o bien a verificar que los trabajadores cumplen sus compromisos laborales, o bien a

7 En efecto, el art. 18.3 CE proclama el secreto de las comunicaciones, salvo resolución judicial.

comprobar el estado de seguridad de dichos dispositivos. El legislador es consciente de que derechos fundamentales del trabajador como la intimidad, pero también el secreto de las comunicaciones, pueden verse afectados con la monitorización de los ordenadores. De ahí que limite su acceso por parte de la empresa y, si sucediera, apela a los principios que alumbran el derecho a la protección de datos para que estos actúen en garantía de los derechos de los trabajadores. El GT29 se pronuncia con rotundidad al respecto y señala que "El hecho de que un empresario sea propietario de los medios electrónicos no excluye el derecho de los trabajadores a mantener en secreto sus comunicaciones, los datos de localización relacionados y la correspondencia".

Tan importante como los fines empresariales, o el "para qué" de acceder al ordenador, lo son (i) las normas de utilización de los ordenadores, (ii) que no sólo deberán existir, sino que además deberán ser conocidas por los trabajadores con carácter previo a la posible monitorización. De esta forma, el apdo. 3 del art. 87 LOPDGDD es tajante cuando mandata a los empleadores que establezcan criterios de utilización de los dispositivos digitales. En sí, esos criterios no deberán ser establecidos unilateralmente por la empresa, sino que en su elaboración deberán participar los representantes de los trabajadores[8].

(I) Exigencia de establecer los criterios de uso privado de dispositivos digitales

(I) El precepto no facilita ninguna pauta añadida al mandato anterior pero, para el supuesto de que esos criterios hubieran permitido el uso privado de los ordenadores de la empresa, especifica que el acceso por el empleador al contenido de dispositivos digitales requerirá que se concreten, de modo preciso, los usos autorizados y se establezcan garantías para preservar la intimidad de los trabajadores, tales como, en su caso, la determinación de los períodos en que los dispositivos podrán utilizarse para fines privados. Esta orden, leída a contrario, se traduce en que, efectivamente, la empresa puede prohibir el uso privado de los ordenadores. Para el GT29 (pág. 16), el bloqueo de ciertos sitios web, por ejemplo, podría ser una buena opción: es mejor esta solución que controlar todas las comunicaciones del empleado de forma continua.

En cualquier caso, también cuando se pretenda acceder al contenido del ordenador para verificar si se ha respetado la prohibición del uso privado del ordenador, el art. 5.1 c) RGPD recuerda que los datos que se traten serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados, principio conocido como de "minimización de datos". Por ello, aunque el trabajador haya realizado un uso privado del ordenador, desobedeciendo los criterios para la utilización del mismo, la empresa debería actuar a través de medi-

8 Véase la STS n. 225, 6 de febrero de 2024.

das técnicas y organizativas destinadas a minimizar el tratamiento de datos personales atendiendo a los criterios de proporcionalidad y necesidad.

(II) Exigencia de informar a los trabajadores los criterios establecidos por la empresa

(II) En aras de que el trabajador actúe en consonancia con los criterios establecidos por la empresa, elaborados, como se recordaba más atrás, con la participación de los representantes de los trabajadores, la legislación exige que se informe a los trabajadores de dichos *criterios*[9]. Esta orden se aloja en el art. 87 "in fine" de la LOPDGDD, y es un ejemplo de norma jurídica "más específica", en comparación con la legislación general existente de protección de datos en el caso de personas no trabajadoras. Con todo, esta norma más específica no anula los principios elementales que recogen tanto el RGPD como la LOPDGDD –al contrario, los refuerza–, y que también se aplicarán a las personas trabajadoras (véanse los art. 12.2 y 13 RGPD; y también el art. 11.3 de la propia LOPDGDD). En efecto, el art. 87 citado exige que cuando los empleadores establezcan los criterios de utilización de los dispositivos digitales respeten en todo caso los estándares mínimos de protección de su intimidad de acuerdo con los usos sociales y *los derechos reconocidos constitucional y legalmente*.

2.3. Protección de la persona trabajadora frente a la videovigilancia y la grabación de sonidos

El art. 89 LOPDGDD acomete la posibilidad de que la empresa trate datos personales del trabajador, obtenidos a través de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo.

La finalidad permitida por la ley para proceder a grabar imágenes en el lugar de trabajo es más amplia que la del art. 87 LOPDGDD, referida a la monitorización de los ordenadores. Debe quedar claro, entonces, que la colocación de una videocámara en el lugar de trabajo tiene que estar destinada a controlar a los trabajadores en aras de que esas imágenes permitan el ejercicio de las funciones aparejadas a dicho control.

A continuación, el precepto añade que los empleadores "habrán de informar con carácter previo, y de forma expresa, clara y concisa", a los trabajadores y, en su caso, a sus representantes, respecto de los extremos de esta medida de tratamiento de datos. Una vez más, comprobamos que la ley española concreta ciertas obligaciones que se exigen al empleador, y que no se exigen en otros supues-

9 El artículo que examinamos prevé esa obligación de informar a los trabajadores sobre los criterios de utilización de lo s ordenadores de modo más laxo que los arts. 89 y 90, como se comprobará a continuación.

tos de tratamiento de datos de personas-ciudadanas sin la condición de empleadas[10].

Un aspecto no baladí resulta que la LOPDGG no se pronuncia respecto de si esa finalidad "de control" lleva aparejada la posibilidad de que los datos obtenidos sirvan de prueba para sancionar, incluso despedir disciplinariamente al empleado. Con todo, parece que ambas finalidades están estrechamente vinculadas; incluso podría defenderse su idéntico anclaje en el poder de dirección del empresario, aunque se deberá tener en cuenta que si el empleador proyecta el tratamiento ulterior de datos personales sobre un fin que no sea aquél para el que se recogieron, proporcionará al interesado, con anterioridad a dicho tratamiento ulterior, y, en principio, información sobre ese otro fin (véase el art. 13.3 RGPD), obligación que apenas se ha comprobado por los tribunales españoles; y menos aún se ha valorado su ausencia (STC 114/2022).

Si se continúa con la lectura del art. 89 LOPDGDD, el enunciado del artículo prevé que, en el supuesto de que *se haya captado la comisión flagrante de un acto ilícito por los trabajadores*, se entenderá cumplido el deber de informar cuando existiese, al menos el dispositivo que se recoge en el art. 22.4 de la misma ley. Este artículo ha suscitado mucha controversia en los tribunales y en la doctrina científica (Terradillos Ormaetxea, 2023).

En cuanto a la grabación de sonidos de los trabajadores, el apdo. 3 del art. 89 LOPDGDD restringe las posibilidades del empresario, y éste sólo podrá grabar a los empleados cuando resulten relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo. Huelga matizar, por tanto, que la grabación no se permitirá para el control de los trabajadores. El sonido, al captar la voz de las personas, permite identificar más emociones que la imagen, por lo que el régimen para su grabación es más severo que en otros supuestos (AEPD, 2023).

Un grado más elevado de garantías, que impide cualquier grabación de los trabajadores, es el contenido en el apdo. 2 del art. 89 LOPDGDD. Y así, los lugares destinados al descanso o esparcimiento de los trabajadores, como vestuarios, aseos, comedores y análogos, están vetados a la captación de imágenes[11]. Se trata ésta de una prohibición absoluta, que no cede ni cuando se tienen sospechas de la comisión de un acto ilícito. La prohibición de grabar en determinados lugares, para el caso de las imágenes, es extensible igualmente sobre la

10 Nos volvemos a remitir a las normas sobre información básica que recogen tanto el RGPD como la LOPDGDD, y que también se aplicarán a las personas trabajadoras (véanse los art. 12.2 y 13 RGPD; y también el art. 11.3 de la propia LOPDGDD).

11 Véase la S. del Juzgado de lo social de Albacete, nº 65/2023, de 2 de marzo, donde, aplicando analógicamente las sanciones contempladas en la Ley de Infracciones y Sanciones del Orden Social, condena a la empresa a una indemnización de 30.001 euros.

grabación de sonidos. Pero, para el caso de los sonidos, la LOPDGDD incluye todavía más limitaciones, obligando a respetar el principio de proporcionalidad, el de intervención mínima y las garantías previstas en los apartados anteriores.

2.4. Protección de la persona trabajadora frente a la geolocalización

El artículo 90 LOPDGDD vuelve a utilizar el "derecho a la intimidad" para limitar el tratamiento por parte de los empleadores de los datos obtenidos a través del sistema de geolocalización colocado en el vehículo conducido por el trabajador. El esquema que utiliza es muy parecido al dispuesto para la videovigilancia. El principio de limitación se ciñe al ejercicio de las funciones de control de los trabajadores, siempre que esas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo.

La forma, el tiempo y el modo en que debe librarse la información al trabajador acerca de la existencia y características de esos dispositivos de geolocalización son idénticos al caso de la grabación de imágenes: se hará con carácter previo, de forma expresa, clara e inequívoca y se informará de la existencia y características de esos dispositivos. Ahora bien, nunca antes como en este apartado se ha observado la referencia al derecho de los trabajadores a ser informados acerca del posible ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión. ¿Significa este enunciado que en el resto de supuestos se cancela este deber de información que soporta la empresa? En nuestra opinión, en línea con lo manifestado anteriormente, y en consonancia con las directrices mostradas por el GT29, esta referencia no es más que un recordatorio, que refuerza la necesidad de que la empresa se emplee en dicha información, dado que se trata de un deber general que proviene del art. 12 RGPD y que debe ser respetado en cualquier tratamiento de datos; con la importante excepción del caso de la captación de imágenes de comisión flagrante de "actos ilícitos", por tratarse de una excepción expresamente recogida en la LOPDGDD (aunque con la decisiva reserva de que el RGPD se refiere a "infracciones penales" en su art. 23.1 d).

Por último, se volverá a recordar que, aunque el propietario de los sistemas de geolocalización sea el empresario, el GT29 insistió en que los trabajadores tienen derecho a mantener en secreto los datos de localización relacionados, en el entendimiento de que se excluirán del tratamiento las localizaciones del trabajador que no tengan relación con el trabajo[12].

12 En España, sin embargo, el Tribunal Supremo (TS) se ha pronunciado, en parte, sobre este sistema de control del trabajador, declarando que "geolocalizar" a los trabajadores no supone una invasión de su intimidad si el dispositivo utilizado para ello es propiedad de la empresa (STS sentencia núm. 163/2021, de 8 de febrero).

3. LA TECNOLOGÍA RELATIVA A LA INTELIGENCIA ARTIFICIAL O LA UTILIZACIÓN MASIVA DE DATOS: LA INCIPIENTE REGULACIÓN LEGAL

3.1. La regulación jurídica europea

En el ámbito de los recursos humanos, la información recopilada de distintas fuentes, que cuando alcanza un volumen lo bastante elevado se denomina *big data,* se utiliza para fines muy variados como entrenar algoritmos (o, más genéricamente, inteligencia artificial, IA) capaces de realizar actividades varias, como predicciones relacionadas con el talento y la capacidad de los trabajadores y los candidatos; supervisar, evaluar y estimular el rendimiento; fijar objetivos y valorar los resultados del trabajo; poner en contacto a los trabajadores con los clientes; juzgar estados de ánimo y emociones de los empleados; proporcionar formación modular en el lugar de producción; encontrar patrones de comportamiento dentro de la plantilla, por ejemplo relacionados con las enfermedades, y muchas cosas más, incluida la selección de los trabajadores a despedir.

A la luz de estas innovaciones, en este trabajo explicaremos a grandes rasgos cómo se está introduciendo la IA en los procesos de decisión empresariales e identificaremos los riesgos a los que se enfrentan los trabajadores en la actualidad, riesgos que deben ser reconocidos tanto por los legisladores como por quienes contratan a los trabajadores (UGT, 2021). Esos riesgos se relacionan con la introducción de criterios sesgados en la adopción de los algoritmos, que pueden resultar abiertamente discriminatorios, a pesar de contar con una apariencia inicial de neutralidad (Grupo de Trabajo, 2017). El Libro Blanco sobre IA (Comisión Europea, 2020) identificó riesgos "a futuro" apenas intuidos en este momento (ETUC, 2022).

El debate sobre la necesidad de una regulación legal de los algoritmos en las relaciones laborales está, pues, servido. Y lo está porque hay autores que defienden que la propia resistencia que ofrecen los derechos fundamentales –si acaso, una apelación reforzada de estos–, las directrices emanadas de la estrategia europea en inteligencia artificial, junto con las disposiciones derivadas del RGPD, y con apoyo en la importante función que le corresponde asumir a la negociación colectiva, podrían ser suficientes para frenar las consecuencias indeseadas de la masiva utilización de los algoritmos (García Quiñones, 2023). De hecho, el V Acuerdo para el Empleo y la Negociación Colectiva (AENC), firmado en 2023 por las organizaciones sindicales y empresariales más representativas de España[13], recoge en su Capítulo XVI un apar-

13 BOE 31 de mayo de 2023. La eficacia jurídica de este tipo de acuerdos permitiría incorporar el contenido del mismo a todos los convenios colectivos de ámbito inferior (sectorial, empresarial o infraempresarial) que puedan firmarse a partir de ahora, siempre que se celebren por las organizaciones firmantes de este Acuerdo (art. 83.3 ET).

tado titulado "Inteligencia Artificial y garantía del principio de control humano y derecho a la información sobre los algoritmos".

En realidad, el AENC se remite a los compromisos básicos del Acuerdo Marco europeo sobre digitalización de 2020[14] (control humano, transparencia, información entendible), acuerdo que en concreto alberga un método para abordar los efectos de la transición digital sobre el mercado de trabajo de forma conjunta por los empleadores y los trabajadores y sus representantes (Rodríguez Fernández, 2023), aunque es plausible que dicho acuerdo europeo se haya proyectado en España: sólo así será posible dotar de eficacia jurídica a sus cláusulas, aunque se pronostica que su despliegue en los diferentes Estados miembros no será uniforme (Sepúlveda Gómez, 2021).

Tal como se sostenía más atrás, la doctrina ha subrayado que el RGPD constituye actualmente la normativa más efectiva para garantizar el respeto de los derechos fundamentales en el ámbito de la IA, asegurando una intervención humana tanto en las decisiones automatizadas como en la elaboración de perfiles que determinan consecuencias jurídicas, mediante el establecimiento de un derecho de explicación junto con la evaluación de impacto de la IA sobre la protección de datos, instrumentos ambos relevantes para la preservación de los derechos fundamentales (Sáez Lara, 2020).

En efecto, su art. 22, bajo el título "Decisiones individuales automatizadas, incluida la elaboración de perfiles", reconoce el derecho del interesado (en nuestro caso, el empleado) a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar. Esta prohibición permite, sin embargo, un tratamiento "semiautomático", mientras tanto la intervención humana sea significativa[15]. A ello hay que añadir que el propio art. 22.2 exceptúa lo anterior en tres supuestos, de modo que la decisión automatizada podrá prescindir de la intervención humana cuando: a) sea necesaria para la celebración o la ejecución de un *contrato* (lo que ampararía también los procesos precontractuales), b) cuando esté autorizada por el Derecho de la Unión o de los Estados miembros o, c) cuando se base en el consentimiento explícito del interesado.

Huelga aclarar que la alusión a "contrato" incluye los "contratos de trabajo", por lo que este título jurídico permitiría al empresario recurrir a decisiones automatizadas, que podrán ser adoptadas tras un análisis de una ingente cantidad de datos de los trabajadores. Aun y todo, en el caso del contrato de trabajo, el responsable del tratamiento –o sea, el empresario– adoptará las medidas adecuadas para salvaguar-

14 Acuerdo Marco europeo sobre digitalización de 2020 https://www.ceoe.es/sites/ceoe-corporativo/files/content/file/2020/12/22/110/acuerdo_marco_interlocutores_sociales_europeos_digitalizacion_2020.pdf.

15 Artículo 22.3 del RGPD.

dar los derechos y libertades y los intereses legítimos del interesado, como mínimo, el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión (art. 22.3).

Por otra parte, una lectura sistemática y más integrada del RGPD conduce a exigir que esta dispensa sea interpretada de forma restrictiva. La lectura del Dictamen elaborado por el GT29 es también útil, en la medida en que la excepción procedería cuando la intervención humana fuese impracticable por el gran volumen de datos a procesar, o cuando no existiera un método menos intrusivo e igualmente efectivo. La elevada cantidad de datos utilizada por la IA ha conducido a aprobar una nueva normativa en la UE.

3.1.1. El Reglamento europeo sobre Inteligencia Artificial

Con parecer adecuada la excepción analizada, sin embargo, los dos factores que permiten acudir a la misma, esto es, la cantidad intensiva de datos y la inexistencia de medidas más eficaces, parece que van a crecer y decrecer, respectivamente, en un corto o medio plazo. En una sociedad en la que proliferan los datos y donde se espera que sigan creciendo, parece lógico pensar que el recurso a la automatización –cada vez más mejorado, en tanto que se nutre de datos, con los que se entrena– se va a imponer sobre cualquier otra medida, y va a dar lugar a decisiones que, aunque no sean completamente automatizadas, están influenciadas por los procesos y resultados de un sistema basado en la IA (Olmos Parés, 2023).

De la anterior premisa, y de otras, surgió la necesidad de elaborar un Reglamento relativo a la Inteligencia Artificial, aplicable en la UE[16]. Los modelos de IA que pretenden sustituir la inteligencia humana a base de la regla "prueba-error" se dedican a utilizar la experiencia humana, previa transformación de ésta en datos, para predecir comportamientos o eventos o para extraer conclusiones que sirvan para elaborar recomendaciones o buscar soluciones (Rivas Vallejo, 2023). Para ello, esos sistemas de IA utilizan, fundamentalmente, datos masivos. A tal fin emplean, entre otros, principalmente el método del aprendizaje automático (sistema que aprende de la actividad realizada y de sus propios errores, a la vez que extraen conocimiento, que puede proceder de datos masivos).

La secuenciación de un determinado proceso para adoptar una decisión puede también funcionar sin alimentación por datos, en cuanto simplemente requiera del análisis de cada caso y no de un espectro amplio, por lo que tal sistema podrá diseñarse para exigir el cumplimiento de determinadas condiciones como un modelo binario (sí/no) capaz de determinar en cada supuesto si lo que se somete a su consideración cumple la expectativa exigible previamente tasada (p.e., los requisitos para el acceso a una prestación o beneficio público). Obviamente, las implicaciones del uso de una tipología u otra (referidas a mecanismos habitualmente utilizados en el

16 La última versión publicada se corresponde con las enmiendas aprobadas por el Parlamento Europeo, el 14 de junio de 2023 (COM (2021)0206-C9-0146/2021-2021/0106(COD)). Las referencias al Reglamento IA se harán respecto de esta versión.

ámbito de la gestión del trabajo o las prestaciones públicas) son muy dispares entre sí, pues, mientras en el modelo alimentado por datos masivos los riesgos pueden ser de diverso origen (incorporación de sesgos perjuicios, además de errores en la selección o etiquetado de los datos, entre otros), en el segundo modelo tales riesgos son también menos complejos, pero no por ello inexistentes.

Y así, a finales de 2023, la Presidencia del Consejo de la UE (España) y los negociadores del Parlamento Europeo alcanzaron un acuerdo provisional sobre la propuesta relativa a normas armonizadas en materia de inteligencia artificial[17]. Recientemente, se ha aprobado el Reglamento de Inteligencia Artificial[18], norma que tiene por objeto garantizar que los sistemas de IA introducidos en los mercados europeos y utilizados en la UE sean seguros y respeten los derechos fundamentales y los valores de la UE. La idea principal de esta futura regulación jurídica se sustenta en un enfoque basado en los riesgos: a mayor riesgo, normas más estrictas[19].

Es importante subrayar que los sistemas de IA identificados como de alto riesgo en el nuevo Reglamento (Anexo III, apdo. 4) incluyen la tecnología de IA utilizada para la contratación o la selección de personas físicas, en particular para publicar anuncios de empleo específicos, analizar y filtrar las solicitudes de empleo y evaluar a los candidatos; o para tomar decisiones que afecten a las condiciones de las relaciones de índole laboral o a la promoción o rescisión de relaciones contractuales de índole laboral, para la asignación de tareas a partir de comportamientos individuales o rasgos o características personales o para supervisar y evaluar el rendimiento y el comportamiento de las personas en el marco de dichas relaciones.

Conforme al Reglamento IA (art. 27), los sistemas de IA de alto riesgo estarán sujetos a obligaciones estrictas antes de que puedan comercializarse. Así, por ejemplo, en lo que se refiere a los riesgos apreciados en el campo de las relaciones laborales, la norma europea apuesta por una mejor protección de los derechos mediante la obligación de que los implementadores de sistemas de IA de alto riesgo lleven a cabo una evaluación del impacto en los derechos fundamentales antes de poner en marcha un sistema de IA. Esa evaluación integrará una serie de tareas: una descripción de los procesos del responsable del despliegue en los que se utilizará el sistema de IA de alto riesgo en consonancia con su finalidad prevista; una descripción del período de tiempo durante el cual se prevé utilizar cada sistema de IA de alto riesgo y la frecuencia con la que está previsto utilizarlo; las categorías de personas físicas y

17 https://ec.europa.eu/commission/presscorner/detail/es/ip_23_6473 (último acceso: febrero 2024).

18 Resolución legislativa del Parlamento Europeo, de 13 de marzo de 2024, sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo, por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)) .

19 La información se ha obtenido de https://digital-strategy.ec.europa.eu/es/policies/regulatory-framework-ai (último acceso: enero de 2024)

grupos que puedan verse afectados por su utilización en el contexto específico; los riesgos de perjuicio específicos que puedan afectar a las categorías de personas físicas y grupos determinadas; una descripción de la aplicación de medidas de supervisión humana, de acuerdo con las instrucciones de uso; y las medidas que deben adoptarse en caso de que dichos riesgos se materialicen, en particular, los acuerdos de gobernanza interna y los mecanismos de reclamación.

Además, una vez realizada la evaluación a que se refiere el apartado 1 del presente artículo, el responsable del despliegue notificará sus resultados a la autoridad de vigilancia del mercado.

A fin de comprobar la relación tan íntima que existe entre el RGPD y esta nueva normativa, el nuevo Reglamento dispone que, si ya se cumple cualquiera de las obligaciones establecidas en el presente artículo como resultado de la evaluación de impacto relativa a la protección de datos, la evaluación de impacto relativa a los derechos fundamentales a que se refiere el apartado 1 del presente artículo complementará dicha evaluación de impacto relativa a la protección de datos.

Asimismo, en el contexto del empleo y la protección de los trabajadores, se advierte que el presente Reglamento no debe afectar al Derecho de la Unión en materia de política social ni a la legislación laboral nacional –conforme al Derecho de la Unión– relativa a las condiciones de empleo y de trabajo, incluidas la salud y seguridad en el trabajo y la relación entre empleadores y trabajadores. Se añade que el Reglamento tampoco debe afectar, en modo alguno, al ejercicio de los derechos fundamentales reconocidos en los Estados miembros y a escala de la Unión, incluidos el derecho o la libertad de huelga o de emprender otras acciones contempladas en los sistemas de relaciones laborales específicos de los Estados miembros y el derecho a negociar, concluir y hacer cumplir convenios colectivos o a llevar a cabo acciones colectivas conforme a la legislación nacional (considerando nº 10).

Por último, algunos usos de la IA entrañan riesgos que se consideran inaceptables, por lo que su uso en la UE quedará prohibido (art. 5). Entre esos ejemplos se encuentra la introducción en el mercado, la puesta en servicio para este fin específico o el uso de sistemas de IA que tengan los siguientes efectos: que creen o amplíen bases de datos de reconocimiento facial mediante la extracción no selectiva de imágenes faciales de internet o de circuitos cerrados de televisión; o que sirvan para inferir las emociones de una persona física en los lugares de trabajo y en los centros educativos, excepto cuando el sistema de IA esté destinado a ser instalado o introducido en el mercado por motivos médicos o de seguridad. También estará prohibida la introducción en el mercado, la puesta en servicio para este fin específico o el uso de sistemas de categorización biométrica que clasifiquen individualmente a las personas físicas sobre la base de sus datos biométricos para deducir o inferir su raza, opiniones políticas, afiliación sindical, convicciones religiosas o filosóficas, vida sexual u orientación sexual.

3.1.2. La Directiva europea relativa a la mejora de las condiciones laborales en las plataformas digitales

Es conocido que la persona que presta sus servicios a través de plataformas se ve sometida a un intenso control laboral, debido en particular a la aplicación informática sustentada en la IA que permite esa relación de servicios. Por eso es bienvenida esta norma comunitaria, norma que constituye el primer acto legislativo de la UE que regula la gestión algorítmica en el lugar de trabajo y establece normas mínimas de la UE para mejorar las condiciones laborales de millones de trabajadores de plataformas en toda la UE (Cardona Rubert, 2024).

La nueva directiva europea prevé que los Estados miembros dispongan de procedimientos administrativos o judiciales para clasificar como personas trabajadoras por cuenta ajena a aquellas que trabajan en alguna de estas plataformas digitales, por lo que la transposición de la Directiva permitiría ampliar el ámbito de aplicación de la presunción de laboralidad a todas las plataformas digitales, y no sólo a las de reparto, como ocurre en la legislación española (Cardona Rubert, 2024).

La norma regula, de forma extensa, las posibilidades que tienen las plataformas de procesar los datos personales de forma automatizada para monitorizar o tomar decisiones que afecten a las personas trabajadoras (Todolí Signes, 2024). Su contenido, amplio, reproduce las garantías del Reglamento IA, respecto de distintas cuestiones como (i) la obligación de realizar –con consulta a los representantes de los trabajadores– una evaluación de impacto (art. 8), o (ii) el impedimento de que las plataformas realicen una serie de usos prohibidos (art. 7) relacionados con el control de datos emocionales o psicológicos de las personas trabajadoras, el respeto de la privacidad de sus conversaciones privadas, la predicción del ejercicio de derechos fundamentales –incluyendo la sindicación, la huelga, o los derechos de consulta o negociación colectiva–. El procesamiento de datos biométricos también está prohibido. El art. 9 (iii) prevé obligaciones de transparencia de la plataforma respecto al uso del algoritmo, de modo que la norma europea elabora una lista detallada de la información que debe trasmitirse tanto a las personas que prestan servicios como a sus representantes, y que debe hacerse antes de la introducción de dicha tecnología en la empresa. Asimismo, (iv) se establece la obligación de que los Estados miembros garanticen una supervisión humana de todos estos sistemas automatizados (art. 11). Por último, (v) la norma prohíbe que el algoritmo determine la finalización de la relación contractual, exigiendo que dicha decisión la tome una persona humana (art. 10.5). Como ha manifestado la doctrina, "la Directiva arma un sistema cuya finalidad es proporcionar garantías a la posición del trabajador de plataformas digitales, rebajando, en la medida de la posible, la excesiva vulnerabilidad frente a la plataforma" (Cardona Rubert, 2024).

3.2. La regulación jurídica española relativa al empleo de la IA en el lugar de trabajo

3.2.1. El trabajo prestado a las plataformas digitales de reparto de comida: la presunción de laboralidad de sus trabajadores

La conocida como "ley rider"[20] fue acordada en marzo de 2021 entre el Gobierno español, la patronal y los sindicatos más representativos. Previamente, el Tribunal Supremo (STS 805/2020, de 25 de septiembre) había declarado la condición de asalariados a los trabajadores que prestaban sus servicios en plataformas digitales de reparto de comida a domicilio, concretamente, a repartidores de la plataforma Glovo.

La norma jurídica permitió introducir una Disposición Adicional 23 en el texto del ET, donde actualmente se recoge que se presume incluida en el ámbito de esta ley, la actividad de las personas que presten servicios retribuidos consistentes en el reparto o distribución de cualquier producto de consumo o mercancía, por parte de personas empleadoras que ejercen las facultades empresariales de organización, dirección y control de forma directa, indirecta o implícita, mediante la gestión algorítmica del servicio o de las condiciones de trabajo, a través de una plataforma digital.

La ley ha sido bienvenida y ha servido de marco para la elaboración de la Directiva sobre plataformas digitales, recientemente aprobada. Con todo, sólo se aplica al sector del reparto de comida, y su efectividad no ha sido la esperada porque la empresa principal del sector, Glovo, sigue contratando a trabajadores autónomos[21]. La empresa fue sancionada con multas astronómicas por el incumplimiento de la normativa anterior, pero sigue sin abonarlas[22]. En efecto, en el último Informe de Delivery Hero[23], la empresa "madre" de Glovo, se da cuenta de las dificultades que asolan a esta empresa.

3.2.2. Las funciones de los representantes colectivos de los trabajadores en la elaboración de los algoritmos que afecten a las relaciones de trabajo, incluida la elaboración de perfiles

En el ámbito del diálogo social tripartito español, se acordó incorporar, en el Real Decreto-Ley 9/2021, de 11 de mayo, por el que se modifica el texto refundido de la Ley

20 Real Decreto-ley 9/2021, de 11 de mayo, por el que se modifica el texto refundido de la Ley del Estatuto de los Trabajadores, para garantizar los derechos laborales de las personas dedicadas al reparto en el ámbito de plataformas digitales.

21 https://elpais.com/economia/2023-05-07/dos-anos-de-la-ley-rider-rebeldia-en-el-sector-del-delivery-que-ignora-las-multas-millonarias-de-trabajo.html# (último acceso: febrero 2024).

22 https://efe.com/portada-espana/2024-04-10/trabajo-remite-fiscalia-informe-actuacion-glovo-repartidores/ (último acceso: abril de 2024).

23 https://www.eleconomista.es/retail-consumo/noticias/12786432/04/24/glovo-lograra-beneficios-operativos-en-el-segundo-semestre-por-primera-vez-en-diez-anos.html (último acceso: abril de 2024).

del Estatuto de los trabajadores, una letra d) al artículo 64.4 ET relativa al derecho a la información sobre 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, acceso y mantenimiento del empleo, incluida la elaboración de perfiles. Cierto es que entre las funciones que pueden desempeñar los representantes legales de los trabajadores, la de recibir información es la más endeble.

Tampoco podemos desdeñar que países del Derecho comparado, como Alemania (European Agency for Safety and Health at Work, 2024), señalan varios cambios legislativos para empoderar a los trabajadores, como garantizar la codeterminación y el derecho de los comités de empresa a participar en los procesos de introducción y uso de la IA en el lugar de trabajo. En dicho país se prevé también modificar la legislación pertinente para garantizar que el derecho ya existente a codeterminar los criterios de selección utilizados para la contratación, reasignación, promoción/demisión y despido de trabajadores también se aplique cuando se utilice la IA.

4. CONCLUSIONES

El Reglamento (UE) 2016/679, 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, constituye la primera norma jurídica que integra las relaciones laborales en el ámbito de protección del DPD. Antes, la CE de 1978, en su art. 18.4, preveía un derecho a la protección frente a la informática. No obstante, el marco de las relaciones laborales, basado en la subordinación y la dependencia del trabajador, era prácticamente ajeno a su ámbito de protección; con la excepción de la interpretación realizada por los tribunales de las postrimerías del siglo XX, favorable a la persona trabajadora. En desarrollo del citado Reglamento europeo se aprobó la Ley Orgánica 3/2018, de protección de datos personales y garantía de los derechos digitales, con un importante Título X dedicado a proteger la intimidad y el DPD de los trabajadores por cuenta ajena y de los empleados públicos.

Los mandatos de la LOPDGDD específicos que regulan los derechos de los trabajadores afectados por la tecnología y la digitalización se corresponden con los arts. 87 a 91 de la ley (Título X). Sin embargo, esta matización no es obstáculo para subrayar que, tanto el contenido general del RGPD, aplicable a las personas que no son trabajadoras, como el contenido general del resto de títulos de la LOPDGDD se proyectan también sobre los trabajadores.

No obstante, los tribunales del orden jurisdiccional social, encargados de aplicar el Derecho, no reparan con la debida atención en la protección brindada por el Reglamento, que debe ser leído en paralelo e integrado con la LOPDGDD[24]. De ello resulta

24 Esta conclusión se comprueba fácilmente con el acceso a cualquier base de datos de jurisprudencia, donde es imposible encontrar, salvo alguna excepción –como la STSJ Madrid nº 893/2022, de 5 de octubre–, una sentencia del orden jurisdiccional laboral que aplique el RGPD.

que la garantía brindada en ciertas sentencias a los trabajadores sea menor que la que resultaría de la aplicación apropiada del Derecho (Terradillos Ormaetxea, 2023).

A mayor abundamiento, al analizar el tratamiento que la LOPDGDD dispone respecto de la captación de datos personales a través de los distintos instrumentos digitales (monitorización del ordenador, videocámaras, grabación de sonidos y geolocalización), observamos que la ley española recoge más garantías para el trabajador que para el resto de los ciudadanos. En muchos casos, pero no en todos, el legislador se preocupa por que la finalidad del tratamiento se justifique en la relación laboral, estando el fin de "controlar el cumplimiento de las obligaciones laborales" en el frontispicio de casi todos los casos. La grabación de sonidos, sin embargo, se exceptúa de lo anterior, ya que únicamente será posible en circunstancias tan extraordinarias como que existan riesgos relevantes en la seguridad de las instalaciones, bienes y personas.

Nos encontramos, pues, ante un escenario normativo complejo, desde el momento en que existen fuentes procedentes de la UE, del Consejo de Europa y de España. Con todo, el sistema de fuentes obliga a aplicar conjuntamente el RGPD y la LOPDGDD, aunque debe llamarse también la atención sobre el hecho de que hay veces en los que la ley española no ha desarrollado convenientemente el Reglamento.

En base a una lectura coordinada de la legislación mencionada, por ejemplo, tecnologías que permanentemente graban al trabajador, o recogen datos sobre su geolocalización o monitorizan su ordenador, serían contrarias a la legislación sobre protección de datos. Así como la legislación permite el tratamiento de datos personales, prohíbe también el exceso de recogida de datos del trabajador porque ese control se convertiría en invasivo; de ahí, además, se podría crear el riesgo de un tratamiento posterior incompatible. Este axioma conduce a que la legislación sobre protección de datos prohíba la grabación continuada del trabajador, porque permitiría un control detallado de su vida y de sus pautas de comportamiento. A pesar de que la finalidad inicial de dicha grabación fuera legítima, otros principios que alumbran el DPD, como el principio de subsidiariedad –que existan medios menos invasivos de la privacidad para obtener el mismo resultado– harían decaer la libertad empresarial para proceder así. Otro ejemplo sería el relativo a la finalidad del tratamiento de datos, que debe estar perfectamente identificada en la información que debe suministrarse al trabajador y a sus representantes; y que, de cambiarse, debería, de nuevo, ser motivo de información posterior. Todo ello, a riesgo de que el tratamiento devenga invasivo, consecuencia que prevé el RGPD.

Para finalizar, tal como se ha visto, la aplicación masiva de la IA en los lugares de trabajo va a suponer otra tecnología disruptiva, con muchos efectos todavía desconocidos para los trabajadores. La aplicación de los sistemas IA a las relaciones laborales se ha clasificado como de alto riesgo por el Reglamento IA, lo cual compor-

tará una serie de obligaciones y compromisos para los empleadores. Es evidente que el Derecho no va a poder frenar todas las posibles colisiones entre la tecnología IA y los derechos de los trabajadores, pero debe ser bienvenida esta primera reacción jurídica de la UE, así como la calificación de "alto riesgo" de la introducción y uso de la IA sobre el empleo y las relaciones laborales. Esa evaluación de impacto sobre los derechos fundamentales de los trabajadores que exige el Reglamento en esos casos, en tanto que se trata de una medida preventiva, es donde radica la piedra angular de este nuevo edificio. Esas cautelas y garantías son también adoptadas por la nueva Directiva sobre las plataformas digitales, aprobada en 2024, que se sitúa en línea con la "filosofía" del Reglamento IA.

El Real Decreto 817/2023, de 8 de noviembre (BOE 9 de noviembre), que establece un entorno controlado de pruebas para el ensayo del cumplimiento de la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial, es un instrumento útil y que puede servir de prueba-error para cuando entre en vigor el Reglamento europeo (2026); pero, también puede ser un instrumento válido para la futura y esperada ley española que complemente el Reglamento IA. Asimismo, en el siguiente bienio esperamos ser testigos de la transposición de la Directiva sobre plataformas digitales. Confiemos, pues, en que esas eventuales leyes españolas consignen las posibles limitaciones que la tecnología IA puede entrañar sobre los derechos fundamentales de los trabajadores con certeza y previsibilidad. Los flancos dejados por la actual LOPDGDD, y la interpretación equivocada llevada a cabo por algunos tribunales debe hacernos mejorar en aras de lograr, frente a la IA, la irradiación plena de los derechos fundamentales en la empresa.

REFERENCIAS BIBLIOGRÁFICAS

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (2023): Guía de la AEPD sobre tratamientos de control de presencia mediante sistemas biométricos, 2023. Disponible en: https://www.aepd.es/guias/guia-control-presencia-biometrico.pdf [Consultado: febrero 2024].

BAYLOS GRAU, A. (2019): "El papel de la negociación colectiva en la ley de protección de datos personales y garantía de derechos digitales en España", *Labour & Law Issues*, 5. Disponible en http://www.soluzionilavoro.it/2020/01/30/labour-law-issues-n-1-2019/ (último acceso: marzo 2024).

CARDONA RUBERT, M.B. (2024): "La aprobación de la Directiva relativa a la mejora de las Condiciones Laborales en las Plataformas Digitales: una buena noticia". *NET21,* 17. Disponible en https://www.net21.org/condiciones-laborales-en-las-plataformas-digitales (último acceso: 23 de marzo de 2024)

CCOO INDUSTRIA (2016): *La digitalización de la industria*. [en línea]. Disponible en: https://industria.ccoo.es/c3c747b1b9a7fb841a6a6b72032c2138000060.pdf [consulta: febrero 2024].

COMISIÓN EUROPEA (2018a): Employment and social developments in Europe (ESDE). Disponible en: https://ec.europa.eu/commission/presscorner/detail/es/IP_18_4395

— (2018b): Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones Inteligencia artificial para Europa. COM/2018/237 final. [en línea] Disponible en: https://eur-lex.europa.eu/legalcontent/ ES/TXT/?uri=COM%3A2018%3A237%3AFIN. [Consultado: febrero 2024].

COMISIÓN EUROPEA LIBRO BLANCO SOBRE LA IA (2020): https://commission.europa.eu/system/files/2020-02/commission-white-paper-artificial-intelligence-feb2020_en

ETUC (2022): European Trade Union Confederation Resolution calling for an EU Directive on Algorithmic Systems at Work [en línea]. Disponible en: https://www.etuc.org/en/document/etuc-resolution-calling-eu-directive-algorithmicsystems-work [consulta: febrero 2024].

EUROPEAN AGENCY FOR SAFETY AND HEALTH AT WORK (EU-OSHA) (2024): Worker management through AI- From technology development to the impacts on workers and their safety and health. Disponible en: https://osha.europa.eu/en/publications/worker-management-through-ai-technology-development-impacts-workers-and-their-safety-and-health (último acceso: abril 2024).

GARCÍA QUIÑONES, J.C. (2023): "Inteligencia artificial y relaciones laborales: entre la significación creciente de los algoritmos y el desmentido de su neutralidad aparente", *Temas laborales*, 167: 75-126.

GOÑI SEIN, J.L. (2018): *La nueva regulación europea y española de protección de datos y su aplicación al ámbito de la empresa (incluido el Real Decreto-Ley5/2018)*, Bomarzo.

GRUPO DE TRABAJO DEL ARTÍCULO 29 (2017): Dictamen 2/2017 sobre el tratamiento de datos en el trabajo, adoptado el 8 de junio de 2017 (Disponible en: https://www.aepd.es/documento/wp249es.pdf

OLMOS PARÉS, I. (2023): "No soy un robot… soy el empresario". [en línea]. Madrid: Comisión de lo Social de Juezas y Jueces para la Democracia, octubre 2023, n.º 248, pp. 10-36. Disponible en: https://www.juecesdemocracia.es/wp-content/uploads/2023/11/Revista-Jurisdiccion-Social-Octubre-2023.pdf [consulta: enero de 2024].

RIVAS VALLEJO, P. (2023): "Decisiones automatizadas y discriminación en el trabajo", *RGDTSS*, 66: 3 y ss.

RODRÍGUEZ FERNÁNDEZ, M.L. (2023): "La participación de las personas trabajadoras en la gobernanza de la transición digital: las experiencias de la UE y de España", *RDS*, 101: 106-140.

SÁEZ LARA, C. (2020): "Algoritmos y discriminación en el empleo: un reto para la normativa antidiscriminatoria", *Nueva Revista Española de Derecho del Trabajo*, 232: 83-126.

SEPÚLVEDA GÓMEZ, M. (2021): "El Acuerdo Marco Europeo sobre Digitalización. El necesario

protagonismo de la norma pactada", *Temas Laborales*, 158: 213-244.

TERRADILLOS ORMAETXEA, E. (2017): "El principio de proporcionalidad como referencia garantista de los derechos de los trabajadores en las últimas sentencias del TEDH dictadas en materia de ciberderechos: un contraste con la doctrina del Tribunal Constitucional español", Revista de Derecho Social, 80: 139-162.

— (2023): "La video-vigilancia de la persona trabajadora en la empresa: protección de datos personales y prueba ilícita", *Revista de Derecho Social*, 102: 57-89.

TODOLÍ SIGNES, A. (2024): "La Directiva para la mejora de las condiciones laborales en plataformas digitales de trabajo. Contenido y propuestas para la trasposición". Disponible en: https://www.aedtss.com/la-directiva-para-la-mejora-de-las-condiciones-laborales-en-plataformas-digitales-de-trabajo-contenido-y-propuestas-para-la-trasposicion/ (último acceso: 23 de marzo de 2024).

UGT (2021): "Las decisiones algorítmicas en las relaciones laborales", *Servicios de Estudios de la Confederación/Análisis y Contextos*.