Primera Parte:
Curso sobre protección de datos CGPJ-AEDTSS

TRATAMIENTO DE DATOS PERSONALES E INTELIGENCIA ARTIFICIAL EN EL MARCO DE LAS RELACIONES LABORALES

PROCESSING OF PERSONAL DATA AND ARTIFICIAL INTELLIGENCE IN THE FRAMEWORK OF INDUSTRIAL RELATIONS*

María Belén Cardona Rubert**
Universidad de Valencia

RESUMEN

Transcurridas tres décadas desde que la primera norma española en materia de protección de datos se promulgó, la LORTAD, y cuando la realidad tecnológico-digital ha superado con creces cualquier previsión futurista es el momento de preguntarse sobre la vigencia el derecho a la protección de datos y la arquitectura legal que le da soporte en el ámbito de las relaciones laborales, tomando como referencia el caso paradigmático de las decisiones algorítmicas que afectan al trabajador.

ABSTRACT

Three decades after the first Spanish data protection law was enacted, the LORTAD, and when the technological-digital reality has far surpassed any futuristic forecast, it is time to ask ourselves about the validity of the right to data protection and the legal architecture

* Recibido el 1 de septiembre de 2022. Aprobado el 19 de septiembre de 2022.
** Catedrática de Derecho del Trabajo y de la Seguridad Social.

that supports it in the field of labour relations, taking as a reference the paradigmatic case of algorithmic decisions that affect the worker.

Palabras clave: Derecho de protección de datos, digitalización, Reglamento General de Protección de Datos (RGPD), Ley de Protección de Datos Personales y Garantía de Derechos Digitales (LOPDGDD), algoritmo, decisiones algorítmicas, inteligencia artificial, transparencia e información, perfiles del trabajador, contrato de trabajo.

Key words: Data Protection, digitization, General Data Protection Regulation (GDPR), Law on the Protection of Personal Data and Guarantee of Digital Rights (LOPDGDD), algorithm, algorithmic decisions, artificial intelligence, transparency and information, employee profiles, employment contract.

1. REFLEXIONES INTRODUCTORIAS

Conceptos como las tecnologías de la información y la comunicación, el ciberespacio, la ciberdelincuencia, las redes sociales, el internet de las cosas, la sociedad digital o el metaverso, han tomado carta de naturaleza en nuestra vida cotidiana. La digitalización está cambiando nuestra forma de comunicarnos y relacionarnos, nuestra forma de trabajar y de crear valor.

El factor que probablemente más ha transformado estas relaciones es el flujo de grandes cantidades de datos relativos a las personas y sus conductas que permite la construcción de perfiles susceptibles de ser tratados con finalidades diversas. Un imparable caudal de información de gran precisión y calidad y que con la incorporación de la técnica de los algoritmos permite, incluso, la previsión de comportamientos futuros y la adopción de decisiones por sistemas expertos basadas en dichas informaciones. Es decir, permite la adopción de decisiones automatizadas, que en el ámbito de la empresa impacta de lleno en el ejercicio de los poderes empresariales, que se abren a la adopción de decisiones algorítmicas basadas en el manejo de *big data*.

La vida ordinaria y profesional de las personas, la actividad productiva, los negocios, la educación, etc. se han visto enormemente facilitadas y agilizadas por la utilización de estas nuevas técnicas, pero estas indudables ventajas no han evitado que su implantación genere numerosas dudas e incertidumbres, puesto que se trata de tecnologías con una nada despreciable potencialidad lesiva para la esfera de los derechos fundamentales. Para empezar, el conocimiento ordenado de datos personales puede dibujar un determinado perfil de la persona o configurar una determinada reputación o fama que es, en definitiva, expresión del honor pero no solo puesto que el haz de derechos fundamentales que puede verse comprometido es amplio, desde la dignidad, el derecho a la intimidad y privacidad, pasando por la protección de datos, la libertad de expresión e información, la integridad física y moral, la libertad ideológica, a la igualdad y no discriminación, hasta los derechos a la libertad sindical y a la huelga, pueden verse comprometidos.

Si hay un entorno en que estas tecnologías ha impactado, definitivamente, es en el de las relaciones de trabajo y el mundo empresarial, hasta el punto de hablarse de Cuarta Revolución Industrial, de la Industria y Sociedad 4.0, de una nueva era, para referirse a los cambios que la digitalización de la economía y la robotización están ocasionando.

Las tecnologías disruptivas abren nuevos horizontes al papel regulador del Derecho. Estamos ante desafíos globales, un cambio de paradigma y de época, en los que las tecnologías digitales abren nuevos escenarios para la ejecución de la prestación laboral.

2. UNA CUESTIÓN NECESARIA: ¿CÓMO SE VEN AFECTADOS LOS DERECHOS FUNDAMENTALES POR LA APLICACIÓN DE LAS TECNOLOGÍAS DISRUPTIVAS?

La aplicación de la informática y de tecnologías afines somete a duro examen la capacidad del ordenamiento jurídico para responder a los nuevos interrogantes que se plantean ya que, en esta situación, son el Derecho y los profesionales del Derecho los llamados a encontrar el equilibrio entre la utilización de las tecnologías y el respeto a los derechos y libertades del individuo. La transformación digital se ha operado paulatinamente, pero de forma contundente y nos ha situado en un escenario de no retorno.

La información sensible crea vulnerabilidad en el titular de los datos pero también en toda la sociedad. La privacidad es una cuestión individual con implicaciones en lo colectivo, en toda la sociedad. La pérdida de privacidad está erosionando la igualdad y facilitando que se instalen en nuestra manera de establecer y mantener relaciones sociales, factores que permiten discriminar a los ciudadanos en función de distintos parámetros, muchos de ellos colectiva e individualmente aceptados. Somos tratados con base en nuestros datos, según la tiranía del algoritmo, según lo que compramos, nuestro género, nuestra salud, nuestra edad o todos estos factores combinados, las posibilidades son casi ilimitadas.

En el ámbito de las relaciones laborales, la inteligencia artificial puede propiciar, por ejemplo, que la combinación de factores como las opiniones vertidas por los clientes, la medición de los tiempos de descanso o del tiempo de desempeño de los encargos, motive la adopción de decisiones empresariales sobre sus trabajadores. Pero, además, los algoritmos pueden albergar sesgos y producir discriminaciones de todo tipo, entre ellas sexistas. Puede suceder, por ejemplo, que se retribuyan más las tareas que requieran mayor esfuerzo físico o que se incluya algún criterio que favorezca a los trabajadores varones, o que la decisión automática produzca un perjuicio a las personas que disfruten de permisos de conciliación familiar, mayoritariamente disfrutados por mujeres.

Todo ello desde la paradoja de que se produce una "renuncia libre a nuestra privacidad"[1], cada vez que realizamos una publicación en Instagram, cada vez que manifestamos nuestras opiniones en redes o simplemente cada vez que solicitamos o compramos un bien de consumo en plataformas digitales. Existe una tendencia a la aceptación de que nuestra esfera privada se reduzca inevitablemente, lo que no deja de ser una falacia. Las consecuen-

[1] El entrecomillado es mío.

cias de dicha tendencia exceden con mucho la mera decisión individual para alcanzar lo colectivo, un riesgo inasumible para las sociedades democráticas, fomentando y contribuyendo a la segmentación y polarización de las mismas.

El filósofo coreano BYUNG-CHUL HAN, expresa claramente esta idea cuando señala a las plataformas como Facebook, Google como los nuevos señores feudales, con respecto a los cuales, desarrollamos una suerte de vasallaje contemporáneo, "labramos sus tierras y producimos datos valiosos de los que ellos luego sacan provecho. Nos sentimos libres, pero estamos completamente explotados, vigilados y controlados. En un sistema que explota la libertad no se crea ninguna resistencia. La dominación se consuma en el momento en el que se encuentra con la libertad…Somos demasiado dependientes de la droga digital y vivimos aturdidos por la fiebre de la comunicación, de modo que no hay ningún basta, ninguna voz de resistencia…El sujeto sometido se imagina que es libre"[2], mientras sigue suministrando de manera continua e inagotable el combustible del que se alimenta el modelo de negocio de estas grandes empresas tecnológicas.

3. EL MARCO REGULATORIO DE LA PROTECCIÓN DE DATOS

La regulación del derecho de protección de datos o derecho de autodeterminación informativa cuenta con una dilatada trayectoria.

A nivel internacional el Convenio n.º 108 del Consejo de Europa, para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal, de 28 de enero de 1981, se remite a los propios Estados firmantes para que desarrollen leyes y adopten medidas en cumplimiento de los principios enunciados en su texto.

A nivel de la Unión Europea, es la Directiva 95/46/CE, del Parlamento y del Consejo de la Unión Europea, de 24 de octubre de 1995, sobre protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, la que introduce el concepto e impone a los Estados miembros su transposición a sus respectivos ordenamientos nacionales.

Con posterioridad otras normas comunitarias han ido incidiendo sobre la regulación del derecho de protección de datos a la par que los nuevos retos tecnológicos y sociales exigían su adaptación a las nuevas realidades. Las Directivas 97/66/CE, de 15 de diciembre de 1997 y 2002/58/CE, de 12 de julio son buena muestra de esto.

El respaldo definitivo a la consideración internacional del derecho a la protección de datos como un derecho independiente respecto al derecho al respeto a la vida privada se obtiene en la Carta de Derechos Fundamentales de la Unión Europea en la que se consagra el derecho fundamental de toda persona a la protección de datos de carácter personal que la conciernen (art. 8).

[2] BYUNG-CHUL HAN, *No-cosas.* Ed. Taurus, Barcelona, 2021, p. 40.

Por su parte, la mayoría de los Estados han llevado a cabo la constitucionalización del derecho a la autodeterminación informativa y, entre ellos, el nuestro, en el art. 18. 4 de nuestra Carta Magna. Aunque existe acuerdo en considerar a este precepto como el fundamento constitucional del derecho, en puridad el artículo se limita a introducir un mandato para el legislador para que garantice los derechos fundamentales frente al uso de la informática. En el año 1992 se produce la primera respuesta legislativa al mandato constitucional a través de la Ley Orgánica 5/1992, de 29 de octubre, de regulación de tratamiento automatizado de los datos de carácter personal (LORTAD) que será sustituida por exigencias de adaptación a la Directiva 95/46/CE, por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos (LOPD).

El punto de inflexión a nivel europeo llega de la mano del Reglamento (UE) 2016/679, de 27 de abril de 2016, General de Protección de Datos (RGPD), que deroga la Directiva 95/46/CE. El RGPD es directamente aplicable en todos los Estados miembro y obligatorio en todos sus elementos, sin necesidad de norma de transposición. Eso sí, a los Estados nacionales se les exige proceder a la depuración de sus ordenamientos, derogaciones de normas incompatibles, cuando proceda; al tiempo que se les incita a completar su regulación y adaptarla a las tradiciones jurídicas propias y al contexto nacional. En el caso español, estas exigencias conducen a la promulgación de una nueva norma de protección de datos, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de Derechos Digitales (LOPDGDD), que junto al RGPD, constituyen el nuevo marco normativo de la protección de datos.

La LOPD queda así derogada por la nueva LOPDGD que es aplicable a cualquier tratamiento de datos personales con independencia de si este se lleva a cabo de manera total o parcialmente automatizada o no y cuyo objeto es, por una parte, adaptar el ordenamiento jurídico español al RGPD y, por otra, garantizar los derechos digitales de la ciudadanía.

4. TREINTA AÑOS DE PROTECCIÓN DE DATOS, ¿TANTO HA CAMBIADO TODO? VIGENCIA DE LA ARQUITECTURA LEGAL DEL DERECHO A LA PROTECCIÓN DE DATOS EN EL NUEVO CONTEXTO SOCIOECONÓMICO

La conocida como economía del dato comporta un escenario de oportunidades de negocio, basado en la analítica de todo tipo de dato y que en el contexto de la Estrategia Digital Europea, necesariamente debe compatibilizar el desarrollo de la tecnología con la garantía de los derechos fundamentales. En este sentido el Plan España Digital 2025 y las líneas estratégicas del Gobierno de España para ejecutar el Plan europeo de Recuperación, Transformación y Resiliencia, se sitúan en la apuesta por la digitalización y generación de servicios públicos y negocios privados basados en datos, siguiendo el modelo europeo, es decir, con respeto al derecho a la protección de datos.

Por otro lado, el gigantesco laboratorio social proporcionado por la emergencia sanitaria mundial ha servido para evidenciar los claros y sombras de los ordenamientos jurídicos, naturalizando definitivamente lo digital en las relaciones económicas y sociales. El impacto de la pandemia ha acelerado la necesidad de transformación digital de empresas e instituciones. Un tránsito obligado por la necesidad de mantener el negocio.

En este escenario se ha puesto de manifiesto que las legislaciones, tanto en el plano de la Unión Europea como en el interno requieren un impulso y sobre todo una interpretación y una aplicación que no desconozca el potencial lesivo de las tecnologías disruptivas para la esfera de los derechos de las personas.

Este año se cumplen 30 años de la primera norma que, en el ámbito nacional, dio cumplimiento al mandato constitucional del art. 18.4 CE e introdujo la regulación legal en materia de protección de datos. Tres décadas desde que la LORTAD[3] se promulgó y los que entonces vaticinaban escenarios que en aquel momento parecían propias del ámbito de la ciencia ficción, hoy se ven superados por una realidad tecnológico-digital que ha superado cualquier previsión y que ni mucho menos ha escrito su último capítulo.

Y en este entorno digital ¿sigue teniendo vigencia el derecho a la protección de datos y la arquitectura legal que le da soporte y contenido o es necesaria una normativa nueva? Existe una tendencia, en mi opinión, excesiva en algunos ámbitos a entender que cada evolución tecnológica requiere una nueva regulación, cuando estamos asistiendo a continuas transformaciones tecnológicas con potencialidad de incidir sobre la esfera de los derechos fundamentales de la persona. Esta interpretación en términos absolutos constituye, sin duda, una falacia puesto que ni todas las innovaciones requieren normativa ad hoc, ni la normativa de protección de datos ha perdido vigencia, ya que la misma tiene vocación de permanencia y ofrece un sistema de principios rectores y reglas suficientes. Ahora bien, ello no empece para que cuando los cambios sean suficientemente relevantes sea aconsejable e, incluso, imprescindible proceder a la interpretación y adaptación a la realidad práctica.

Ciertamente, facilitaría esta conclusión contar con una Jurisprudencia adaptativa y dúctil que interpretara las normas rehuyendo interpretaciones inmovilistas, literales y apegadas a su origen, para abrirse a interpretaciones adaptadas al contexto vigente. No parece ser el caso habitual. Estamos acostumbrados a interpretaciones de la norma apegadas al tenor literal e histórico de la ley, que empujan al legislador a impulsar iniciativas legislativas que den respuestas a las nuevas necesidades, no acogidas inicialmente por la normativa, por mucho que pudiera resultar suficiente una interpretación adaptada a los nuevos tiempos, para preservar su validez.

Dicho lo cual, conviene seguir insistiendo en que la aparición de tecnologías disruptivas dibuja nuevos horizontes para los que hay que hallar soluciones aterrizadas en la realidad concreta y con garantías para los derechos.

4.1. La necesaria revisión del concepto del derecho a la protección de datos

Transcurridas tres décadas desde la promulgación de la LORTAD, la primera norma que ofreció una regulación legal al derecho a la protección de datos es oportuno plantearse la vigencia y actualidad del concepto en el nuevo contexto tecnológico, económico y social,

[3] Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal.

con el trasfondo de un marco normativo nuevo y original como es la combinación de la norma comunitaria de aplicación prioritaria, el RGPD, y la norma nacional, la LOPDGDD, complementaria al RGPD.

El derecho a la protección de datos o derecho a la autodeterminación informativa se concibe como la capacidad y derecho de los individuos de ejercer el control sobre las informaciones que les atañen. Dicho derecho se constituye a partir de la noción de intimidad pero la supera por incluir una función dinámica de control sobre las informaciones que se refieren al individuo. Y es precisamente esta función la que lo configura como un derecho autónomo con respecto al derecho a la intimidad.

El concepto tradicional de intimidad se revela como insuficiente para ofrecer cobertura frente a potenciales lesiones derivadas del uso de las tecnologías que puedan incidir sobre la esfera más privada y reservada de la persona. La posibilidad casi ilimitada de recoger, almacenar, conectar y procesar datos y la gran reducción de costes y tiempo necesarios para realizar tales funciones permiten a quien posea los datos, obtener un perfil de la persona, un perfil completo que puede incluir o del que se pueden deducir informaciones sensibles y que posibilite valoraciones de la misma y decisiones sobre ella.

El derecho a la protección de datos se apoya en un conjunto de derechos subjetivos, deberes, procedimientos y reglas objetivas, mediante las que se permite al individuo definir según MURILLO DE LA CUEVA "la intensidad con la que desea que se conozcan y circulen su identidad y circunstancias, combatir las inexactitudes o falsedades que las alteren y defenderse de cualquier utilización abusiva"[4] que se pretenda hacer de las mismas.

En el derecho a la protección de datos se reconoce una doble vertiente. Por una parte, una dimensión positiva, entendida como derecho de control activo sobre los datos personales; por otra, se reconoce el carácter institucional de garantía-presupuesto del ejercicio de otros derechos constitucionales como el derecho de asociación, libertad ideológica y religiosa, derecho a la no discriminación, derecho al trabajo, derecho a la igualdad, etc., constituyéndose en un derecho instrumental ordenado a la protección de otros derechos fundamentales.

Se trata, por tanto, de un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento de datos (STC 254/1993).

El derecho a la autodeterminación informativa se convierte en la defensa eficaz para la esfera privada del individuo frente al peligro de procesamiento de los datos personales. En este contexto, la protección de datos personales proporciona los instrumentos destinados a limitar y racionalizar la utilización de las tecnologías de la información y comunicación, para impedir los perjuicios que el uso incontrolado de aquellas pueda ocasionar a las personas.

---

[4] MURILLO DE LA CUEVA, P. L., *El derecho a la autodeterminación informativa.* Ed. Tecnos, Madrid, 1990, p. 174.

La Jurisprudencia del Tribunal Constitucional ha reforzado el reconocimiento del derecho a la protección de datos como un derecho autónomo y, particularmente, en sus sentencias 290/2000 y 292/2000, en las que establece la diferenciación entre el derecho a la intimidad y a la protección de datos personales. Según estas "la función del derecho fundamental a la intimidad del art. 18.1.CE es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad (…) En cambio, el derecho fundamental a la protección de datos persigue garantizar a esa persona 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".

En esta jurisprudencia se acotan los perfiles y el contenido del derecho fundamental a la protección de datos, considerándolo como un derecho autónomo e independiente en nuestro sistema constitucional, de manera coincidente con la LOPDGDD.

El derecho a la protección de datos puede definirse como el poder de disposición y de control sobre los datos personales, que habilita a la persona a determinar qué datos y a decidir en qué medida cuales de estos datos proporciona “a un tercero, sea el Estado o un particular, o cuales puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso" (STC292/2000). Se trata, en definitiva, de un derecho horizontal que puede ser ejercido frente a todos, de un derecho de toda persona al tratamiento leal y lícito de sus datos, para finalidades concretas y con su consentimiento previo.

En definitiva, el derecho a la autodeterminación informativa o a la protección de datos confiere al titular de los datos la facultad de conocer y controlar cuantas transacciones y operaciones se realicen con sus datos, así como la de decidir sobre dichas operaciones, a través del otorgamiento informado de su consentimiento, poniendo en sus manos cuantos instrumentos válidos de defensa prevea el ordenamiento, convirtiéndolo en el principal garante de su privacidad. Y este concepto sigue siendo válido en el actual contexto tecnológico y económico social.

El concepto de autodeterminación informativa, por tanto, es un concepto vigente cuyos perfiles, eso sí, han variado de manera matizada para hacer frente a las nuevas exigencias de tutela de la información personal del titular de los datos procesados, en un mundo digitalizado.

El gran reto es proteger y garantizar el derecho fundamental a la protección de datos en un contexto público-privado de aceleración de la innovación, transformación digital, de fomento de la economía de datos y de generalización de aplicación de la inteligencia artificial.

5. LA NUEVA DIMENSIÓN DEL DERECHO A LA PROTECCIÓN DE DATOS A TRAVÉS DEL CASO PARADIGMÁTICO DE LAS DECISIONES ALGORÍTMICAS EN LAS RELACIONES LABORALES: LA NECESARIA ADAPTACIÓN A LOS CAMBIOS CONTEXTUALES

Un caso paradigmático en este último sentido es el de la generalización de la utilización de los algoritmos para gestionar las relaciones laborales.

La imparable y progresiva automatización en la toma de decisiones relativas al núcleo de los poderes empresariales y, en consecuencia, de mayor trascendencia laboral, que obliga a identificar y evaluar la solidez de los mecanismos de protección jurídica de los derechos fundamentales de los trabajadores ante aquellos.

El derecho a la protección de datos sin un contenido que le dote de efectividad no sería más que una mera entelequia, por ello incluye una serie de garantías y derechos que otorgan a la persona titular de los datos la posibilidad de determinar el nivel de protección frente a posibles invasiones en la esfera de sus derechos. En este contenido efectivo es en el que se han producido las principales adaptaciones de los perfiles del derecho a las nuevas realidades.

Es aquella la sede en la que es posible identificar las verdaderas transformaciones del derecho que ha ido adaptándose y haciendo frente a los retos contextuales de la digitalización, mediante la atribución de más incisivos instrumentos a través de los cuales hacer efectivo y real el derecho a la protección de datos. Puesto que la protección efectiva de los datos personales exige que se refuercen y especifiquen los derechos de los interesados y las obligaciones de quienes tratan y determinan el tratamiento de los datos de carácter personal.

Como señala el RGPD en su Considerando 6, la evolución tecnológica y la globalización han planteado nuevos retos para la protección de datos personales. “La magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa”, ya que tanto las empresas privadas como las propias administraciones utilizan datos personales en “una escala sin precedentes” y las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial. Este escenario exige compaginar la facilitación de la libre circulación de datos personales en la Unión Europea y la transferencia a terceros países, con un elevado nivel de protección de datos personales.

El nuevo orden legal proporciona nuevas respuestas en el fondo y la forma a los retos de la era de la disrupción digital. En términos generales, se redimensionan los derechos del interesado, a través de su fortalecimiento y diversificación, respetando el esquema inicial de los principios de protección de datos.

La introducción de los algoritmos en la gestión del personal ha impactado de lleno en las relaciones laborales. Decisiones sobre promociones profesionales, modificaciones de las condiciones de trabajo o despidos pueden adoptarse a través de algoritmos que no requieren la voluntad humana inmediata.

La inteligencia artificial puede propiciar, por ejemplo, que la combinación de factores como las opiniones vertidas por los clientes, la medición de los tiempos de descanso o del tiempo de desempeño de los encargos, motive la adopción de decisiones empresariales sobre sus trabajadores. Pero, además, los algoritmos pueden albergar sesgos y producir discriminaciones de todo tipo, entre ellas sexistas. Puede suceder, por ejemplo, que se retribuyan más las tareas que requieran mayor esfuerzo físico o que se incluya algún criterio que favorezca a los trabajadores varones, o que la decisión automática produzca un perjuicio a las personas que disfruten de permisos de conciliación familiar, mayoritariamente disfrutados por mujeres.

Ya señalábamos que la progresiva automatización en la toma de decisiones relativas al ejercicio de los poderes empresariales obliga a identificar los mecanismos de protección de los derechos de los trabajadores en este contexto.

Dicha protección se construye a partir de la aproximación de reglas sobre las relaciones entre la gestión algorítmica de las decisiones empresariales y el derecho a la privacidad y el adecuado tratamiento de datos personales. No es un equilibro fácil, pues las decisiones automáticas pueden proyectarse sobre datos que afectan a la vida íntima de las personas –y que revelan informaciones tan privadas como sus relaciones personales, su religión, sus convicciones o su orientación sexual, entre otros muchas– y para garantizar dicho equilibrio, la normativa de protección de datos ha ido introduciendo medidas concretas.

Las herramientas jurídicas de las que disponemos para compaginar estos dos aspectos son pocas. La protección más importante proviene de la normativa en protección de datos, el Reglamento (UE) 2016/679, de 27 de abril de 2016, General de Protección de Datos (RGPD) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de Derechos Digitales (LOPDGDD). Y, en concreto, de la prohibición general sobre las decisiones basadas, únicamente, en un tratamiento automatizado de sus datos de carácter personal, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar y su derecho a oponerse a ella (art. 22 RGPD).

Con esta previsión se establece a favor de los interesados el derecho de no verse sometidos a una decisión con efectos jurídicos sobre ellos o que les afecte de manera significativa que esté basada únicamente en un tratamiento automatizado de datos, destinado a evaluar determinados aspectos de su personalidad, tales como su rendimiento laboral, fiabilidad o conducta.

Se trata de una garantía sustancial que se coloca en las manos del interesado, en este caso del trabajador, una garantía que le permite evitar los efectos perniciosos que sobre su persona o vida personal o profesional pueda tener una decisión fundada exclusivamente en una valoración de su persona, producto de una elaboración informática.

La contundencia de dicha prohibición, sin embargo, se diluye en el ámbito de las relaciones laborales, puesto que el propio art. 22.2.a) RGPD admite las decisiones automatizadas, que pueden ser transcendentales en la fase de selección y contratación, pero también durante toda la vigencia del contrato, al excluir expresamente de aquella la decisión automatizada necesaria para la celebración o la ejecución de un contrato. No obstante, y en todo caso, el procedimiento de gestión empresarial que prevea la adopción de decisiones algorítmicas debe articular mecanismos para garantizar la intervención humana, si la persona afectada lo solicita, la expresión del trabajador afectado y el derecho a impugnar la decisión (art. 22.3 RGPD), permitiéndole así contrarrestar los efectos perniciosos que sobre su persona o vida profesional pueda tener una decisión fundada exclusivamente en una valoración de su persona, producto de una formulación informática.

5.1. Derechos de transparencia e información

En este ámbito cobran particular relevancia los derechos de transparencia e información previstos en los arts. 11 LOPDGDD y 12-14 RGPD ya que resulta de la máxima importancia garantizar la transparencia y el derecho de información de los trabajadores afectados sobre los sistemas de gestión algorítmica que se utilicen para el control y seguimiento de la prestación laboral, así como para la adopción de decisiones que afecten a sus condiciones de trabajo.

El derecho de información en el sentido en el que es regulado en los artículos 12, 13 y 14 RGPD, aparece en primer término como concreción del principio de transparencia que obliga al responsable del tratamiento a facilitar la información prevista en los arts. 13 y 14 y cualquier comunicación relativa al tratamiento (arts. 15 a 22 y 34) y a hacerlo en forma concisa, transparente e inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cuando la información se dirija a menores.

Otras de las vertientes del derecho de información y, no menos importante, es la de considerarlo como fase o requisito previo al otorgamiento del consentimiento (art. 4.11RGPD).

El derecho a la información, obviamente, mantiene una estrecha relación con el principio de transparencia y permite al sujeto ejercer un verdadero control sobre sus datos personales, confiriendo validez a la prestación del consentimiento tras haber ejercido el derecho de información. Un consentimiento otorgado sin que se hayan cumplido, de forma adecuada, por parte del responsable del tratamiento las obligaciones de información, es un consentimiento que carece de validez. El derecho de información tiene en el ámbito laboral una importancia central puesto que el art. 6.1.b) RGPD excluye, como ya hiciera su predecesora, la LOPD, los tratamientos de datos en el ámbito laboral, en concreto, cuando el tratamiento sea necesario para la ejecución de un contrato en el que el interesado es parte. Se puede afirmar que, en el caso de los contratos de trabajo, el peso de la tutela del derecho a la protección de datos se traslada al derecho de información.

La información se facilitará por escrito o por otros medios, incluidos, los electrónicos. Cuando lo solicite el interesado, la información podrá facilitarse verbalmente siempre que se demuestre la identidad del interesado por otros medios (art. 12 RGPD y art. 11 LOPDGDD).

La información que debe facilitarse por el responsable del tratamiento sobre la recogida, tratamiento, uso, plazo de conservación y destino varia ligeramente en función del origen de los datos personales, según se hayan recabado del interesado o no (arts. 13 y 14 RGPD y 11LOPD).

El contenido previsto en ambos casos es extenso y prácticamente coincidente. Así sería preciso informar sobre: la identidad y contacto del responsable y de su representante; del del delegado de protección de datos; de los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento; los destinatarios o las categorías de destinatarios de los datos personales; la intención, en su caso, de transferir datos perso-

nales a un tercer país u organización internacional; el plazo de conservación de los datos; los derechos que puede ejercer el interesado; cuando la comunicación de datos sea un requisito legal o contractual, la obligación de prestar el consentimiento y consecuencias de no hacerlo; la existencia de decisiones automatizadas y elaboración de perfiles; en el caso de preverse tratamiento ulterior de los datos con un fin distinto del inicial, deberá proporcionar información sobre dicho fin.

En el supuesto en el que los datos personales no hubieran sido recabados del afectado, además de la información anterior, se tendrá que incluir la referida a las categorías de datos objeto de tratamiento y a las fuentes de las que procedieran los datos.

Se observa, por tanto, en la actual configuración del derecho de información que, con la finalidad de asegurar que el consentimiento del interesado se otorgue con mayores garantías de validez, aquel se ha extendido hasta abarcar un número mayor de informaciones que las exigidas de acuerdo con el anterior marco legal. La cuestión es si esta redimensión del derecho de información es adecuada y compatible con la obligación de proporcionar la información de forma clara, sencilla y accesible, es decir, con las exigencias de la transparencia (art. 12 RDGPD) ya que en la práctica se puede ocasionar una sobrecarga informativa que confunda al interesado a la hora de prestar su consentimiento y, en definitiva, reste intensidad efectiva al cumplimiento de los deberes de información que recaen sobre el responsable del tratamiento.

El GT29 en relación con estas eventuales contradicciones que pueden producirse entre el deber de proporcionar información completa y la de hacerlo de forma concisa y clara, introduce la posibilidad de proporcionar la información por capas o niveles. Así en el Considerando 36 del Documento WP260 rev. 01 se establece un orden y una priorización de la información que se debe facilitar a los interesados[5]. No se trata de prescindir de proporcionar la plenitud de la información legalmente prevista pero sí de proporcionarla en niveles o capas en función de su relevancia para el interesado, garantizando así que la misma se proporciona de forma transparente, es decir, de forma clara, sencilla y accesible. Así, por ejemplo, el primer nivel, al que hace referencia el Considerando 36, incluiría información relativa a los fines, la identidad del responsable y una descripción de los derechos del interesado.

Por lo que, en definitiva, parece conveniente que la información se proporcione modularmente, mediante niveles o capas, para garantizar que el interesado aprehende dicha información de manera correcta y adecuada para acabar otorgando un consentimiento debidamente informado y, por lo tanto, válido. Y sin que en ningún caso eso comporte renunciar a acceder al conjunto de las informaciones que prevén las normas[6].

---

[5] Documento WP 260 rev.01 del Grupo de Trabajo del art. 29 (GT29) "Directrices sobre la transparencia en virtud del Reglamento (UE) 2016/679", de 29 de noviembre de 2017, revisado y adoptado el 11 de abril de 2018. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

[6] Esta información por niveles es la recomendada en la Guía para el cumplimiento del deber de informar, elaborada por la AEPD, la Agencia Vasca de Protección de Datos y la Agencia Catalana de Protección de Datos, https://www.aepd.es/sites/default/files/2019-09/guia-modelo-clausula-informativa.pdf

Las decisiones algorítmicas en el ámbito de las relaciones laborales no suponen una excepción y la información proporciona debe ser suficiente, entendible y transparente (arts. 11 LOPDGDD y arts. 12-14 RGPDD). En esta línea es conveniente, también, establecer con claridad los datos que necesariamente deberían quedar al margen de la gestión algorítmica en contextos laborales. Datos que puedan revelar emociones o estados de ánimo o los que se refieren a conversaciones privadas de las personas trabajadoras nunca deberían ser usados por las empresas, amén de con carácter general, las categorías especiales de datos incluidos en el art. 9 RGPD, es decir, datos personales que revelen el origen étnico o racial, opiniones políticas, convicciones religiosas o filosóficas, afiliación sindical, tratamiento de datos genéticos, vida sexual, orientación sexual, etc.

Con carácter previo, es exigible al responsable del tratamiento que:

– utilice procedimientos matemáticos o estadísticos adecuados para la elaboración de perfiles;

– aplique medidas técnicas y organizativas apropiadas para garantizar que se corrijan los factores que introduzcan inexactitudes en los datos personales y se reduzca al máximo el riesgo de error;

– que se aseguren los datos personales de forma que se tengan en cuenta los posibles riesgos para los intereses y derechos del interesado;

– y que se impidan, entre otras cosas, efectos discriminatorios por motivos de raza u origen étnico, opiniones políticas, religión, creencias, afiliación sindical, condición genética o estado de salud, orientación sexual (art. 9 RGPD).

Se requiere, además, asegurar un régimen adecuado de rendición de cuentas en el que las personas que representen a la empresa revisen y expliquen dichas medidas. Por tanto, deben existir procedimientos adecuados para que sea factible discutirlas e impugnarlas, por lo tanto, es importante que con carácter previo se establezcan mecanismos precisos y claros para la revisión de esas decisiones, exigiéndose a tal fin la existencia de recursos personales suficientes.

En este ámbito resulta muy relevante garantizar la adecuada participación de los representantes de los trabajadores y la apertura de estas cuestiones a la negociación colectiva y al diálogo social. La normativa laboral básica recoge una previsión específica relativa a la intervención de los representantes de los trabajadores y la gestión empresarial algorítmica. Así se reconoce en el art. 64.4.d) del Estatuto de los Trabajadores[7], que consagra su derecho a ser informados por la empresa 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. Previsión que no resulta baladí, aunque pro-

[7] Sobre el derecho de información algorítmica del art. 64.4.d) ET, *vid. in extenso* LOSADA CARREÑO, J., "Inteligencia artificial e información algorítmica en el ámbito laboral. Especial referencia al art. 64.4.d) del Estatuto de los Trabajadores", en *Revista General de Derecho del Trabajo y de la Seguridad Social,* n.º 61, 2022, pp. 418 y ss.

bablemente sea insuficiente para garantizar un papel activo en la defensa de los derechos de los trabajadores y haya que aspirar a modelos que tengan más en consideración los derechos colectivos de trabajadores y trabajadoras y, por tanto, su acción sea más trascendente. Modelos como el de la empresa Just Eat en el que se ha constituido una comisión del algoritmo, interpretan la transparencia en la gestión algorítmica como un factor que más allá de responder a criterios legales, contribuye al buen desempeño, a la mejora del rendimiento de los trabajadores y a la construcción de un mejor clima laboral.

El derecho europeo va en dicha dirección y particularmente la Propuesta de Directiva de mejora de las condiciones de trabajo en el entorno de las plataformas digitales, publicada el pasado 9 diciembre de 2021, aunque referida a dichos entornos, introduce una serie de previsiones dirigidas a acotar la incidencia del algoritmo sobre la relación laboral y, lo que es más importante, sobre las personas trabajadoras y cuyo pilar central es la necesaria intervención humana en la adopción de decisiones basadas únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente, en coherencia con el Reglamento Europeo de Protección de Datos (UE) 2016/679 (art. 22) y la propia normativa española en protección de datos (arts. 21 y 22 LOPDGDD).

Es importante reseñar que en el ámbito de la Unión Europea se halla actualmente en tramitación la propuesta de Reglamento 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. Dicha norma pretende afrontar además la opacidad, la complejidad, el sesgo, cierto grado de imprevisibilidad y un comportamiento parcialmente autónomo de ciertos sistemas de IA, para garantizar su compatibilidad con los derechos fundamentales y facilitar la aplicación de las normas jurídicas, sin que ello implique, en ningún caso, obstaculizar el desarrollo tecnológico y ni aumentar de manera desproporcionada el coste de introducir soluciones de inteligencia artificial en el mercado[8].

5.2. La redimensión de los derechos ARCO

Desde los conocidos como derechos ARCO (derechos de acceso, rectificación, cancelación y oposición) configurados como derechos personalísimos a favor del titular de los datos, previstos en la LOPD, hemos alcanzado el horizonte de su actual configuración en el RGPD y la LOPDGDD, en el que aparecen reforzados de manera significativa.

Estos derechos se encuentran regulados en los arts. 15 a 22 RGPD y en los arts. 12 a 18 LOPGDD. Constituyen un haz relevante de derechos a través de los que el interesado puede ejercer eficazmente su derecho a la protección de datos[9]. Son medios de auto tutela del titular de la información tratada por el responsable. Derechos cuya vigencia en el con-

---

[8] https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52021PC0206&from=ES
Dicha propuesta culminaría un proceso precedido por el Libro Blanco de la Inteligencia Artificial, de 19 de febrero de 2020 (https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_es.pdf) y la Guía de directrices éticas para una inteligencia artificial fiable (https://op.europa.eu/es/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1)

[9] *Vid. in extenso*, CARDONA RUBERT, M. B., "Contenido y elementos principales del derecho a la protección de datos", *Revista del Ministerio de Trabajo y Economía Social,* n.º 148, 2021, pp. 97-112.

trato de trabajo están fuera de toda discusión y de cuyo redimensionamiento se beneficia en primer término el trabajador y por ende titular de la información tratada[10] y no comporta una excepción que el trabajador sea objeto de decisiones algorítmicas, al contrario, cobra en este espacio mayor relevancia la reivindicación del ejercicio de dichos derechos.

El Tribunal Constitucional indicaba ya en su Sentencia 292/2000 que el núcleo esencial del derecho a la autodeterminación informativa se haya no sólo en el consentimiento informado sino que también lo integran esas otras facultades que confieren al titular de los datos personales un poder de disposición sobre la información a él relativa y, en consecuencia, de configurar su propia privacidad.

El Tribunal Constitucional en esta sentencia hacía referencia a los derechos reconocidos al afectado según la legislación vigente, es decir, los derechos de acceso, rectificación, cancelación y oposición al tratamiento, los derechos ARCO. A ellos hay que sumar el derecho al olvido y los derechos de portabilidad y de limitación del tratamiento.

El responsable del tratamiento estará obligado a informar al afectado sobre los medios a su disposición para ejercer dichos derechos, medios que deberán ser accesibles y gratuitas las acciones que permitan dar satisfacción a las solicitudes para su ejercicio.

El derecho de acceso es, sin duda, uno de los derechos más interesantes en cuanto permite la tutela de los propios datos personales de un modo directo, al facilitar el control del sujeto afectado sobre la información tratada. Consiste en la facultad que se le reconoce al afectado de solicitar y obtener del responsable del tratamiento información sobre los datos que le conciernan, con el fin de conocer y verificar la licitud del tratamiento.

El trabajador tiene derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en su caso, derecho de acceso a los datos personales y a la siguiente información: fines del tratamiento; categorías de datos personales tratados; destinatarios o categorías de destinatarios a los que se comunicaron o serán comunicados los datos; plazo previsto de conservación o criterios para su determinación; la existencia de ejercicio de los derechos de rectificación, supresión, limitación del tratamiento u oposición; derecho a presentar una reclamación ante una autoridad de control; si no se obtuvieron los datos del titular, información sobre su origen; la existencia de decisiones automatizadas, incluida la elaboración de perfiles (art. 15 RGPD).

Por su parte, Los derechos de rectificación y supresión, completan al derecho de acceso, puesto que una vez ejercido este, el titular de los datos tratados puede identificar si son inexactos, incorrectos o incompletos.

El derecho de rectificación tiene por objeto obtener la corrección de aquellos datos que resulten incorrectos o incompletos, abriendo a favor del afectado la facultad de exigir la modificación y actualización de la información que está desfasada (art. 16 RGPD y art. 14 LOPDGDD).

[10] Guía de la AEPD "La protección de datos en las relaciones laborales", mayo 2021, pp. 12-15: https://www.aepd.es/es/documento/la-proteccion-de-datos-en-las-relaciones-laborales.pdf

Estas previsiones se entrelazan con las obligaciones impuestas al responsable del tratamiento de velar por la exactitud y actualización de los datos personales tratados y de adoptar todas las medidas razonables para que se supriman o rectifiquen, sin dilación, la inexactitud de los datos personales, con respecto a los fines para los que se tratan (art.4 LOPDGDD, art. 5.1.d) RGPD).

El derecho de supresión, por su parte, tiene por objeto eliminar del fichero aquellos datos personales que sean inadecuados o excesivos. El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, cuando los datos ya no sean necesarios en relación con los fines para los que fueron recogidos; el interesado retire el consentimiento en que se base el tratamiento; el interesado se oponga al tratamiento; los datos hayan sido tratados ilícitamente; los datos deban suprimirse para el cumplimiento de una obligación legal; los datos se hayan obtenido en relación con la oferta de servicios de la sociedad de la información.

El derecho de supresión lógicamente no es un derecho absoluto y de hecho no se podrá materializar cuando el tratamiento sea necesario para ejercer el derecho a la libertad de expresión e información; para el cumplimento de una obligación legal impuesta; por razones de interés público en el ámbito de la salud pública o por alguna otra de las razones previstas en el art. 17. 3 RGPD.

En relación con el derecho al olvido el RGPD se refiere a él, pero lo hace a penas de soslayo e induciendo a que ambos se interpreten como derechos equivalentes, puesto que el art. 17 los utiliza como términos sinónimos, "derecho de supresión (derecho al olvido)". Si bien en su apartado 2 aunque no menciona expresamente el derecho al olvido, sin embargo, incluye una evidente manifestación del mismo. En concreto, cuando prevé que si se hubieran hecho públicos los datos y el responsable estuviera obligado a suprimirlos, se deberán adoptar medidas razonables, incluidas técnicas, para informar a los responsables que estén tratando los datos personales, de la solicitud del interesado, para en alguna medida limitar el impacto de esta difusión[11].

Más explícito es el legislador nacional que dedica sendos artículos al derecho al olvido, en concreto, en búsquedas en internet (art. 93 LOPDGDD) y en servicios de redes sociales y servicios equivalentes (art. 94 LOPDGDD), abrazando la doctrina del Tribunal de Justicia de la Unión Europea, en su sentencia de 13 de mayo de 2014, en el asunto C-131/12 (Google contra España).

En virtud de dicha regulación se proclama el derecho de toda persona a que los motores de búsqueda e internet eliminen de las listas de resultados obtenidas a partir de su nombre los enlaces publicados que contuvieran información relativa a esa persona, cuando fuesen inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieren devenido como tales por el transcurso del tiempo. También podrá ejercerse este derecho al olvido

[11] RALLO LOMBARTE, A., "Del derecho de protección de datos a la garantía de nuevos derechos digitales", en AA.VV. *El Reglamento General de Protección de Datos. Un enfoque nacional y comparado.* Ed. Tirant lo Blanch, Valencia, 2019, p. 147.

cuando las circunstancias personales invocadas por el afectado evidencien la prevalencia de sus derechos sobre el mantenimiento de los enlaces generados por el servicio de búsqueda (art. 93).

Ahora bien, si existe algún ámbito en el que resultaba especialmente pertinente reconocer el derecho al olvido ese es, sin duda, el de las redes sociales. El legislador recoge en el art. 94 LOPDGDD el derecho al olvido en redes sociales y establece que toda persona dispone del derecho a que los datos que hubiese facilitado para su publicación por redes sociales o servicios de la sociedad de la información equivalentes sean suprimidos "a su simple solicitud" (art. 94). Se suprimirán los datos cuando sean inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieren devenido así por el transcurso del tiempo, teniendo en cuenta los fines para los que se recogieron o trataron y el tiempo transcurrido.

La supresión procederá igualmente, cuando sin concurrir las circunstancias anteriores, las circunstancias personales invocadas evidencien la prevalencia de los derechos del titular de los datos sobre el mantenimiento de los datos por el servicio.

Se trata, en resumen, de proporcionar un derecho al interesado que contribuya eficazmente a la defensa del derecho a la autodeterminación informativa.

En relación con el derecho a la limitación del tratamiento, la legislación nacional remite directamente a la regulación establecida en el RGPD sin matiz ninguno (art. 16 LOPDGDD). Según el art. 18 RGPD el interesado tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos cuando se cumplan algunas de las condiciones previstas y que son que el interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable su verificación; que el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en cambio la limitación de su uso; que el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, ejercicio o defensa de reclamaciones; y, por último, que el interesado se haya opuesto al tratamiento en tanto se verifica si los motivos.

6. CONCLUSIÓN

La conclusión parece clara el futuro Estatuto del Trabajo propio de las relaciones laborales del siglo XXI no puede quedarse atrás y debe considerar la perspectiva digital y los derechos digitales en relación al uso generalizado de la inteligencia artificial, como uno de los retos más importantes que está obligado a contemplar. La arquitectura legal de la protección de datos sigue gozando de buena salud y resiste el envite de la digitalización, ahora bien, requiere una interpretación y adaptación acorde a los retos que plantea garantizar el derecho fundamental a la protección de datos en un contexto público-privado de aceleración de la innovación, transformación digital, de fomento de la economía de datos y de generalización de aplicación de la inteligencia artificial en la gestión de las relaciones laborales.

BIBLIOGRAFÍA

CARDONA RUBERT, M. B., "Contenido y elementos principales del derecho a la protección de datos", *Revista del Ministerio de Trabajo y Economía Social,* N.º 148, 2021.

COMISIÓN EUROPEA, *Libro Blanco de la Inteligencia Artificial,* COM(2020) 65 final,19 de febrero de 2020. Bruselas, https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_es.pdf

COMISIÓN EUROPEA, Grupo de expertos de alto nivel sobre inteligencia artificial, Guía de directrices éticas para una inteligencia artificial fiable. Bruselas, 8 de abril de 2019, https://op.europa.eu/es/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1

COMISIÓN EUROPEA, del Grupo de Trabajo del art. 29 (GT29) Documento WP 260 rev.01 "Directrices sobre la transparencia en virtud del Reglamento (UE) 2016/679", de 29 de noviembre de 2017, revisado y adoptado el 11 de abril de 2018. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

AEPD, Guía "La protección de datos en las relaciones laborales", mayo 2021, https://www.aepd.es/es/documento/la-proteccion-de-datos-en-las-relaciones-laborales.pdf

LOSADA CARREÑO, J., "Inteligencia artificial e información algorítmica en el ámbito laboral. Especial referencia al art. 64.4.d) del Estatuto de los Trabajadores", en *Revista General de Derecho del Trabajo y de la Seguridad Social,* n.º 61, 2022.

RALLO LOMBARTE, A., "Del derecho de protección de datos a la garantía de nuevos derechos digitales", en AA.VV. *El Reglamento General de Protección de Datos. Un enfoque nacional y comparado.* Ed. Tirant lo Blanch, Valencia, 2019.