LOS PODERES DE DIRECCIÓN Y DE CONTROL DE LA EMPRESA Y EL DERECHO A LA PROTECCIÓN DE DATOS

THE MANAGEMENT AND CONTROL POWERS OF THE COMPANY AND THE RIGHT TO DATA PROTECTION*

Edurne Terradillos Ormaetxea**
Universidad del País Vasco

SUMARIO: 1. Introducción. –2. Los requisitos y límites del tratamiento de datos personales contemplados en la LOPDGDD, frente a los poderes de dirección y control; 2.1. El contrato de trabajo como apoyo jurídico del tratamiento de datos personales del trabajador; 2.2. La finalidad del tratamiento de datos; 2.3. El deber de información previa o el derecho de los trabajadores a conocer el tratamiento de sus datos, previamente a su recogida; 2.3.1. Las excepciones del deber de información previa en materia de tratamiento de datos personales obtenidos de dispositivos de videovigilancia, cuando se haya captado la comisión flagrante de un acto ilícito: una referencia a las cámaras ocultas. –3. Una aproximación a los límites del tratamiento automatizado de datos. –Bibliografía.

RESUMEN

El trabajo pretende aportar unos criterios que permitan identificar el espacio –y límites– del ejercicio de los poderes de dirección y control empresariales cuando afecten al derecho de protección de datos personales. Las formas de ejercitar los poderes de dirección y control de la empresa están cambiando y se pueden basar en el acceso a los dispositivos electrónicos puestos a disposición del trabajador, en la utilización de videocámaras, en dispositivos de geolocalización o simplemente en grabadoras de sonidos. La regulación jurídica de la grabación de imágenes en las que se capta al trabajador en "comisión flagrante de actos ilícitos" ocupará asimismo un lugar destacado en las páginas siguientes. En tanto que la utilización de algoritmos y el recurso a la inteligencia artificial permite a la empresa realizar un tratamiento automatizado de datos, invasión donde las haya del derecho a la protección de datos, se realizará también una aproximación a su regulación jurídica.

* Recibido 12 de julio de 2022. Aprobado el 19 de septiembre de 2022.
El trabajo ha sido realizado en el contexto del Grupo de Investigación Consolidado del Gobierno Vasco "Un nuevo modelo de Gobernanza empresarial sostenible en la era de la internacionalización y la digitalización" (2022-2025).
** Profesora Titular de Derecho del Trabajo y de la Seguridad Social.

ABSTRACT

The aim of this paper is to provide criteria for identifying the scope –and limits– of the exercise of the company's powers of management and control when they affect the right to personal data protection. The ways of exercising the company's powers of management and control are changing and can be based on access to electronic devices made available to the worker, the use of video cameras, geolocation devices or simply sound recorders. The legal regulation of the recording of images in which the employee is caught in the "flagrant commission of illegal acts" will also occupy a prominent place in the following pages. Insofar as the use of algorithms and artificial intelligence allows the company to carry out automated data processing, an invasion of the right to data protection if ever there was one, an approach to its legal regulation will also be made.

Palabras clave: derecho a la protección de datos personales, tratamiento automatizado de datos, derechos digitales, deber de información previa.

Key words: right to personal data protection, automated processing of data, digital rights, duty of prior information.

1. INTRODUCCIÓN

Las tecnologías de la información y la comunicación y los dispositivos digitales, en general –ordenadores, cámaras de videovigilancia, geolocalizadores…–, se erigen en medios óptimos para la gestión del personal, así como para el desempeño de las facultades del poder de dirección y control. Dichos dispositivos representan una vía destacada en el ejercicio de la actividad laboral, de modo que determinados puestos de trabajo no se conciben actualmente al margen de herramientas. Al mismo tiempo, ciertas terminales digitales facultan el control empresarial de la ejecución ordenada de la actividad laboral. Esos mecanismos no solo son instrumentos facilitadores del cumplimiento laboral, sino que también constituyen hipotéticos medios de prueba a fin de acreditar el incumplimiento de las obligaciones laborales del trabajador. A ello se refería vagamente el art. 20.3 del Estatuto de los Trabajadores (ET), redactado, hasta 2018, desde la óptica empresarial de la fiscalización del cumplimiento laboral o desde la lógica contractual del sometimiento del trabajador al poder empresarial[1]. La actualmente vigente Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD), es la normativa que invoca el nuevo art. 20 bis) ET, titulado –sorprendentemente– "Derechos de los trabajadores a la intimidad en relación con el entorno digital y a la desconexión"[2]. La remisión del ET a la LOPDGDD se hace a su texto completo, lo cual supone que el intér-

[1] MOLINA NAVARRETE, C., "El «trabajador transparente», entre metáfora y realidad, y el «efecto útil» de los derechos de la personalidad en la empresa del siglo XXI". *RTSS. CEF,* 419, 2018, p. 117.

[2] Es importante destacar que el objeto de la normativa española no es únicamente adaptar el ordenamiento jurídico español al reglamento, sino también garantizar los derechos digitales de la ciudadanía, cfr. FERNÁNDEZ DOMÍNGUEZ, J. J., "El marco jurídico de la protección de datos personales: Reglamento UE 2016/679 y Ley Orgánica 3/2018, de 5 de diciembre", *Revista del Ministerio de Trabajo y Economía Social,* n.º 148, 2021, pp. 46 y 47.

prete del Derecho no puede quedarse en los arts. 87 y ss. de la Ley, relativos a las relaciones laborales, sino que, en principio, todo su contenido sería proyectable a este campo específico.

Las herramientas tecnológicas pueden (y suelen) ser utilizadas con un objetivo de control del cumplimiento laboral, y a la postre, con una finalidad disciplinaria. La cuestión reside en realizar una adecuada correspondencia entre el significado etimológico de "dato" –del latín, *"datum"*, lo que se da[3]–, que implica una voluntad positiva del cedente de la información, y los efectos, queridos pero demasiadas veces, involuntarios, de esta nueva revolución digital.

El conflicto entre los poderes de dirección y control de la empresa y la protección de datos puede ser acometido desde muy diversas perspectivas. Por no poder abordarlas todas, en las páginas siguientes nos centraremos en los límites internos del derecho a la protección de datos (DPD, en adelante). No vamos a acometer el estudio de la fina línea que administra las lizas entre derechos (la libertad de empresa y el DPD), porque ese momento pertenece al ámbito de los límites externos de los derechos. No se abordará, pues, el principio de proporcionalidad como clave de bóveda, y los tres juicios que incluye, ya que se parte de la premisa constitucional de que, si no se respetan los límites internos del DPD por parte del poder de dirección empresarial, no ha lugar al examen de la proporcionalidad de la medida empresarial, porque esa medida será ilícita de inicio.

En último lugar, prestaremos atención a otro campo en el que la protección de datos se enfrenta al poder de dirección y control: el tratamiento automatizado de datos, ámbito que sirve a las empresas para gestionar los recursos humanos, desde la selección del personal hasta su despido.

2. LOS REQUISITOS Y LÍMITES DEL TRATAMIENTO DE DATOS PERSONALES CONTEMPLADOS EN LA LOPDGDD, FRENTE A LOS PODERES DE DIRECCIÓN Y CONTROL

Tal como se advertía en la Introducción, la remisión del ET a la LOPDGDD se hace a su totalidad, lo cual supone que el intérprete del Derecho no puede quedarse en los arts. 87 y ss. de la Ley, y que se refieren a las relaciones laborales, sino que todo su contenido es proyectable a este campo. Sentado lo anterior, la premisa –obvia y sencilla, pero nada baladí– de la cual partimos es que la Ley contempla la licitud del tratamiento de datos personales del trabajador por parte de la empresa. Hay que aceptar la intromisión en los datos del trabajador si este quiere seguir participando en el concierto de la vida, también de la empresa. Con todo y con eso, la regulación jurídica del DPD pretende erigirse en la forma de control de las impertinencias, incluso excesos, en los que pueden incurrir los poderes de dirección y control empresariales. Sin embargo, los límites generales a los que se enfrenta el poder empresarial se toparán, en primer lugar, con el contrato de trabajo como interés legítimo que permite la intromisión en los datos del trabajador, con la determinación

[3] Conforme a la Real Academia de la Lengua Española, el término "dato" hace referencia a la "Información sobre algo concreto que permite su conocimiento exacto o sirve para deducir las consecuencias derivadas de un hecho".

de la finalidad del tratamiento, en segundo lugar, y con el deber de información, en último, pero no menos importante, lugar.

Los medios de control digitales que contempla la LOPDGDD se recogen en los arts. 87 y ss., y se concentran en cuatro grupos: el acceso a dispositivos electrónicos –o la monitorización de estos-, la captación de imágenes, la grabación de sonidos y la geolocalización.

2.1. El contrato de trabajo como apoyo jurídico del tratamiento de datos personales del trabajador

No siempre exige la ley que se recabe el consentimiento del titular de los datos para proceder a su tratamiento. Y esa posibilidad se permite en el ámbito de las relaciones laborales dado que "el consentimiento se entiende implícito en la propia aceptación del contrato que implica reconocimiento del poder de dirección del empresario"[4]. No solicitar el consentimiento del trabajador para tratar sus datos supone la primera "atenuación" de la normativa general, en tanto que el art. 6 RGPD invoca, en primer lugar, al consentimiento del afectado aunque, indiscutiblemente, la existencia cualquier otro interés legítimo puede avalar esa afectación.

Con ser legal que únicamente la suscripción del contrato de trabajo permita a la empresa, sin perjuicio de otros límites, la afectación del DPD, llama la atención que no se informe al trabajador del posible tratamiento de datos cuando suscribe el contrato. En efecto, ni la Directiva 91/533/CEE, del Consejo, de 14 de octubre de 1991, relativa a la obligación del empresario de informar al trabajador acerca de las condiciones aplicables al contrato de trabajo o a la relación laboral[5] previó esa información –comprensible, por otra parte, debido a que la digitalización no se encontraba en un estado de desarrollo como el actual–, ni la más reciente Directiva (UE) 2019/1152 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, relativa a unas condiciones laborales transparentes y previsibles en la Unión Europea[6] han contemplado dicha información. En esta nueva directiva, en su Exposición de Motivos (apdo. 3), se invoca al principio n. 7 del pilar europeo de derechos sociales, principio que dispone que los trabajadores tienen derecho a ser informados por escrito al comienzo del empleo sobre sus *derechos y obligaciones* derivados de la relación laboral, incluso en período de prueba. Esa exposición de motivos continúa advirtiendo (apdo. 4) de que, en este entorno laboral cambiante, existe por tanto una creciente necesidad de que los trabajadores dispongan de información completa respecto de sus condiciones de trabajo esenciales, información que debe facilitarse a su debido tiempo y por escrito de una forma de fácil acceso.

A la espera de la transposición al ordenamiento español de la Directiva 2019/1152, cuya fecha límite es el 1 de agosto de 2022, aún tratándose de una Directiva que pretende ac-

---

[4] GARCÍA-PERROTE ESCARTÍN, I. y MERCADER UGUINA, J. R., "La protección de datos se come a la intimidad: la doctrina de la sentencia del Tribunal Europeo de Derechos Humanos de 5 de septiembre de 2017, Gran Sala (caso Barbulescu vs. Rumanía; n.º 61496/08)", *Revista de Información Laboral,* n.º 10, 2017, p. 1.

[5] *Diario Oficial de las Comunidades Europeas,* n.º L 288/32, de 18/10/91.

[6] Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-2019-81159

tualizar los derechos de información a los nuevos tiempos, así como instaurar una serie de contenidos mínimos para los trabajadores con patrones de trabajos con mínima previsibilidad (art. 10 Directiva 2019/1152), extraña bastante que dicha información no se libre al trabajador, fundamentalmente por no haberse contemplado en su texto.

2.2. La finalidad del tratamiento de datos

De la lectura de los arts. 87 y ss. LOPDGDD es fácil diferenciar el distinto alcance o finalidad del tratamiento en función de cuál es el tipo de medio de control que se pretende utilizar por parte de la empresa.

En el supuesto de monitorización de los dispositivos (art. 87), la empresa deberá fundamentar la afectación del DPD en el control de las obligaciones laborales o en la integridad de los dispositivos electrónicos. En parecidos términos se expresa la ley cuando se refiere a la captación de imágenes (art. 89), aunque de manera más restrictiva, porque solo contempla la videovigilancia con la finalidad de controlar el cumplimiento de las obligaciones laborales[7]. Es esa la misma finalidad que legitima la geolocalización del trabajador (art. 90)[8].

Es cierto que la LOPDGDD elige el término de "control", y no otro, para limitar la utilización de dispositivos de videovigilancia. En el campo de las relaciones laborales, es usual distinguir entre el poder de control y el poder disciplinario, diferencia que nos lleva a preguntarnos si la detección de un incumplimiento laboral a través de estos medios puede sustentar un despido disciplinario. Entendemos que la respuesta debe ser positiva dado que no tendría sentido verificar un incumplimiento laboral sin que pueda anudarse ninguna consecuencia al mismo. Además, ambas facultades –de control y de disciplina– se integran dentro del poder de dirección (art. 38 CE y 20 ET).

Además, el art. 5.1 b) del Reglamento, tras ordenar que los datos sean recogidos con fines determinados, explícitos y legítimos, añade que aquellos "no serán tratados ulteriormente de manera incompatible con dichos fines", de donde se puede deducir que la sanción disciplinaria, incluso el despido, puede entenderse como fin compatible con el inicial, esto es, el control del cumplimiento de las obligaciones laborales[9].

Por el contrario, el recurso a la grabación de sonidos cuenta con más limitaciones desde el punto de vista del tratamiento finalístico, en tanto en cuanto solo se recurrirá a esa vía cuando exista un riesgo en la seguridad de las instalaciones de la empresa, bienes y personas. ¿Se incluye en esa acepción el poder de control, incluido el poder disciplinario? El Repertorio OIT "Protección de los datos personales de los trabajadores" (1997)[10], art. 5.2,

---

[7] Más precisión en LÓPEZ BALAGUER, M., "El control empresarial por videovigilancia en la LOPD", *Revista andaluza de trabajo y bienestar social,* n.º 151, 2020, p. 361.

[8] Véase MARÍN MALO, M., "La geolocalización del trabajador. Reflexiones a la luz de la jurisprudencia reciente", *LABOS Revista del Derecho del Trabajo y Protección Social,* n.º 1, 2020, p. 111.

[9] RODRÍGUEZ ESCANCIANO, S., "El derecho a la protección de datos personales en el contrato de trabajo: reflexiones a la luz del Reglamento europeo 2016/679", *Estudios financieros. Revista de trabajo y seguridad social,* n.º 423, 2018, p. 28, exige que sean atendidos todos y cada uno de los fines perseguidos.

[10] No es una norma imperativa. Disponible en: http://www.oit.org/global/publications/ilo-bookstore/order-online/books/WCMS_PUBL_9223103290_ES/lang--es/index.htm

dispone que no se pueden utilizar los datos obtenidos con el fin de garantizar la seguridad… para controlar el comportamiento de los trabajadores.

Las resistencias por entender que la normativa sobre protección de datos al completo es aplicable al entorno de las relaciones laborales se aprecian en la dirección seguida por la fundamentación jurídica de la STC 160/2021; sentencia donde la doctrina relativa a la amplia irradiación de los derechos fundamentales, a la vez que la interpretación de estos de conformidad con las normas internacionales sobre protección de derechos y libertad públicas queda difuminada. En efecto, los trabajadores –en este caso asesores comerciales de una compañía de telefonía– eran conocedores del hecho de la grabación, pero contaban con un compromiso expreso de la empresa de que, en ningún caso, aquella tendría como objetivo convertirse en un mecanismo disciplinario. Para el TC, la trascendencia constitucional del asunto consistía en determinar la relevancia que para la configuración del derecho a la protección de datos del carácter personal (art. 18.4 CE) tienen las condiciones pactadas entre las partes respecto del uso de los datos de carácter personal obtenidos mediante estas grabaciones. Y en opinión del Tribunal, no existió una vulneración del DPD. Siendo cierto que los hechos a los que atiende la sentencia ocurrieron antes de ser aprobada la LOPDGDD, también lo es que entonces estaba en vigor el RGPD, con referencias muy concretas a los fines del tratamiento en cuestión.

La LOPDGDD dispone este límite en forma de "principio de limitación de la finalidad" y "principio de minimización de los datos". Hacer lo contrario a lo que propugnan esos principios supondría una vulneración del principio de lealtad de los datos, tal como se recoge tanto en el Repertorio OIT (art. 5), como en la Carta de Derechos fundamentales de la UE (art. 8.2), pero también en el Reglamento General de Protección de Datos (art. 5.1 b). En abreviada conclusión, el poder de dirección y control empresarial no se debería ejercitar invadiendo el DPD si aquel se utiliza para una finalidad distinta de las permitidas, ni si se emplea partiendo de una finalidad permitida por el tratamiento pero utilizada después para alcanzar una distinta, no adecuada o no pertinente o que no sea compatible con la originaria (art. 5.1 b) y c) LOPDGDD).

A todo lo anterior se suma que cualquier debate que se origine en relación con ese equilibrio, disputa o lid entre el DPD y el ejercicio de los poderes de dirección y control de la empresa debería partir de la interpretación realizada por el TC[11] en torno a los derechos fundamentales, doctrina que propugna la más amplia irradiación de esos derechos, tal y como postula el art. 10.2 CE.

2.3. El deber de información previa o el derecho de los trabajadores a conocer el tratamiento de sus datos, previamente a su recogida

El tercero, pero nada desdeñable límite al que se enfrenta el poder de dirección antes del tratamiento de datos personales de los trabajadores se refiere al deber de información. Es esencial recordar que la STC 39/2016, 3 marzo (FJ 3) consignó que el deber de información forma parte del contenido esencial del derecho a la protección de datos[12].

---

[11] Doctrina que comienza con la innovadora y trascendental STC 99/1994, de 11 de abril.

[12] Esta doctrina vuelve a recogerse en la más reciente STC 160/2021, 4 de octubre.

El DPD es un derecho fundamental, autónomo, con una regulación propia en el art. 18.4 de la CE, que permite a las personas obtener un poder de disposición sobre sus datos personales y también saber quién posee esos datos y para qué, con la facultad de oponerse a esa posesión y su uso[13].

El supuesto donde esta obligación empresarial resulta menos taxativa es el relativo al art. 87 LOPDGG, referido a la monitorización de los dispositivos digitales. En efecto, el apdo. 3 "in fine" del art. 87 recoge que "Los trabajadores deberán ser informados de los criterios de utilización a los que se refiere este apartado". Al contrario que lo que ocurre en el resto de medios digitales que pueden conculcar el DPD, donde la LOPDGG requiere expresamente que previamente al tratamiento se informe de la medida a los trabajadores y a sus representantes (arts. 89.1 y 90.2 LOPDGDD), en lo relativo al acceso a los dispositivos digitales, la ley es menos concisa[14]. Sin embargo, repárese en que ese mismo art. 87, apdo. 3, exige que en la empresa elabore los criterios de utilización de los dispositivos digitales por parte de los trabajadores, proceso en el que participarán los representantes de los trabajadores.

En este trabajo se defiende que el contenido de esa deber no solo alcanza la información sobre la adopción de la medida empresarial "ad hoc" (grabación, geolocalización…) sino que, en una lectura paralela y sistemática de esos artículos con el resto de la Ley, a la que, recuérdese, el art. 20 bis) ET se remite por completo[15], dicha información deberá albergar el contenido de los derechos ínsitos en el art. 12 RGPD, los llamados derechos ARCO (acceso, rectificación, supresión, limitación del tratamiento y oposición). A mayor abundamiento, el contenido de esa información será diferente en función de que los datos se hayan obtenido o no del interesado; con el apunte añadido de que el deber de información es más exigente y más intenso cuando los datos no se obtienen del interesado, como, por ejemplo, en los casos de videograbación o geolocalización[16] (compárense los arts. 13 y 14 RGPD). Sin embargo, entendemos también que la información que debe librarse a los representantes de los trabajadores no debería ser tan completa como la que se propugna para los propios trabajadores: en la medida en que los representantes no son los titulares del DPD, no tendría sentido informarles de esos derechos que no podrán ejercitar, por no tener la condición de interesados; tampoco la de legitimados. Al contrario, recibir esa información, previamente al tratamiento, es de suma importancia para la persona trabajadora, habida cuenta de que esos derechos forman parte del contenido esencial del DPD. Además, esa información previa cobra un lugar destacado en el ámbito de las relaciones laborales, toda vez que es el contrato de trabajo el título legítimo que habilita al em-

---

[13] VALLE MUÑOZ, F. A., "Control tecnológico empresarial y licitud de la prueba en el proceso laboral" desarrollado en el marco del proyecto de investigación", *Trabajo y derecho: nueva revista de actualidad y relaciones laborales,* n.º 87, 2022, p. 3.

[14] Véase CASAS BAAMONDE, M.ª E. y ÁNGEL QUIROGA, M., "Los derechos fundamentales a la intimidad y a la protección de datos personales en la economía digital. Geolocalización de los trabajadores a través de GPS del vehículo de empresa. Despido procedente". *Revista de jurisprudencia laboral,* Número 9/2020.

[15] Favorable a esa remisión en bloque, véase BAZ RODRÍGUEZ, J., "La Ley Orgánica 3/2018 como marco embrionario de garantía de los derechos digitales laborales. Claves para un análisis sistemático", *Trabajo y Derecho,* n.º 54, 2019, pp. 49 y ss.

[16] Sobre la geolocalización, véase la STS n. 766/2020, de 15 de septiembre.

presario a afectar el DPD de las personas trabajadores, sin que, por ahora, ninguna norma jurídica expresamente obligue a la empresa a informarles de esta cuestión.

Analizada la última jurisprudencia sobre esta cuestión, y a pesar de que los últimos pronunciamientos judiciales no aplican todavía la LOPDGDD, se aprecia cierta resistencia a dirimir los conflictos existentes entre el poder de dirección y de disciplina, por un lado, y el DPD, por otro, a favor del derecho fundamental, esto es, del lado de la preservación del DPD de los trabajadores. O bien porque para los tribunales es irrelevante que el fin del tratamiento no estuviera determinado desde el principio[17], o bien porque hay alguna otra prueba, no determinante, que abunda en la causa disciplinaria del despido[18], o bien porque es irrelevante que no se haya informado al trabajador cuando sí se ha hecho a los representantes de los trabajadores[19], lo cierto es que se aprecian fugas significativas en la doctrina jurisprudencial que propugna la interpretación extensiva (irradiación plena) de los derechos fundamentales.

2.3.1. Las excepciones del deber de información previa en materia de tratamiento de datos personales obtenidos de dispositivos de videovigilancia, cuando se haya captado la comisión flagrante de un acto ilícito: una referencia a las cámaras ocultas

El art. 89 LOPDGDD concierta bastantes dudas sobre el alcance de la información que debe deparar el empleador al trabajador y a sus representantes en un supuesto muy concreto, la captación de la comisión flagrante por el trabajador de un acto ilícito, supuesto en el que ese precepto invoca a lo dispuesto en el art. 22 LOPDGDD.

En circunstancias "normales" ese precepto, 89.1, exige a los empleadores que informen con *carácter previo* a los trabajadores y, en su caso, a sus representantes sobre la medida en cuestión. La sentencia citada de la Gran Sala del Tribunal Europeo de Derechos Humanos (TEDH) de 5 de septiembre de 2017 (Barbulescu II)[20] también se pronunció sobre el particular, declarando que el trabajador es titular de ese derecho informativo de *manera previa* al tratamiento de datos personales.

Pero ante una situación de captación de la comisión flagrante de un acto ilícito, ¿qué regula la ley respecto del deber de información previa del empleador?

El mismo art. 89.1 LOPDGDD provee que en ese supuesto el deber de informar será aliviado siendo suficiente con que exista el dispositivo al que se refiere el art. 22.4 de la Ley orgánica; esto es, será bastante para entender cumplido el deber de información con la colocación por parte de la empresa, de un *dispositivo informativo* en un lugar suficiente-

---

[17] Véase la STS 25/01/2022, rec. ud 4468/2018. Es sintomático que el F.J. 4 de la sentencia citada recuerde que "Solamente era necesario el deber de información del art. 5 LOPD de 1999". Sin embargo, al actor no se le notificó que la realización de captación de su imagen durante el desempeño laboral fuera a utilizarse con una finalidad disciplinaria.

[18] Véase la STC 160/2021, 4 de octubre.

[19] Véase la STS de 30 marzo 2022, rec. ud. 1288/2020.

[20] Recurso n.º 61496/08.

mente visible, identificando, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos en los artículos 15 a 22 del Reglamento (UE) 2016/679 (derechos de acceso, rectificación y supresión, limitación del tratamiento, etc.). También podrá incluirse en el dispositivo informativo un código de conexión o dirección de internet a esta información (sistema de capas). El precepto finaliza recordando que "en todo caso, el responsable del tratamiento deberá mantener a disposición de los afectados la información a la que se refiere el citado reglamento".

La doctrina[21], antes de aprobarse la LOPDGDD, se preguntó si el interés del empresario de sorprender *in fraganti* al empleado justificaría el recurrir a un sistema de videovigilancia que no garantizara la finalidad última para la que puedan ser empleadas las imágenes en un futuro[22], esto es, la sanción o el despido del trabajador[23]. Si el principio de calidad de los datos que recogía la anterior LOPD (art. 4) exigía que los datos de carácter personal solo pueden ser recogidos para el cumplimiento de finalidades determinadas, explícitas y legítimas del responsable del tratamiento, parecería que no cualquier motivo pudiera debilitar ese derecho a la información previa que forma parte del contenido esencial del derecho a la protección de datos[24]; con más razón se exigiría lo anterior en el caso de las relaciones laborales donde no se requiere el consentimiento del trabajador para tratar sus datos personales[25].

Esa posibilidad de limitar el derecho a la protección de datos personales se contempla en el propio RGPD, cuyo art. 23.1 permite que los Estados miembros mediante medidas legislativas, limiten el alcance de los derechos y obligaciones establecidos entre los arts. 12 a 22 del Reglamento, cuando tal limitación respete en lo esencial los derechos y libertades fundamentales *y sea una medida necesaria y proporcionada* en una sociedad democrática para salvaguardar" una serie de bienes jurídicos, que parecen enumerarse a modo de "lista cerrada". Obsérvese que el art. 23.1 RGPD faculta la redacción de un art. 89 LOPDGDD que limita el deber de información previa, pero impide que tal limitación neu-

---

[21] JIMÉNEZ-CASTELLANOS BALLESTEROS, I., "Videovigilancia laboral y derecho fundamental a la protección de datos", *Temas Laborales* n.º 136/2017, pp. 152 y ss.

[22] MIÑARRO YANINI, M., "Impacto del reglamento comunitario de protección de datos en las relaciones laborales: un –pretendido– «cambio cultural»", *RTSS CEF* n. 423, 2018 p. 14, antes de que dispusiéramos del nuevo Título X de la LOPDGDD, opinó que la calificación de la acción de videovigilancia "no informada" sería considerada ilícita pero no se pronunciaba sobre la acción de videovigilancia insuficientemente informada que, a mi modo de ver, sería igualmente ilícita.

[23] Para un caso donde la empresa advirtió de las distintas finalidades que perseguía el sistema de videovigilancia, véase la STSJ Madrid (Social), n. 388/2019, de 24 abril, AS/2019/2350, F.J. 2; o la STSJ Castilla y León, Burgos (Social) n. 319/2019, 15 de mayo, AS 2019/1751, F.J. 1, donde se hacían constar las finalidades disciplinarias de la instalación de las cámaras, información que se libró a través del comité de empresa.

[24] En relación con el deber de información previa como contenido esencial del derecho a la protección de datos personales, véase la pionera STC 292/2000, 30 noviembre. En la doctrina, SERRANO GARCÍA, J. M.ª, "Límites de la ley de protección de datos al poder de dirección del empresario", *La protección de datos y la regulación de las tecnologías en la negociación colectiva y en la jurisprudencia,* Editorial Bormazo, Albacete, 2019, p. 25.

[25] JIMÉNEZ-CASTELLANOS BALLESTEROS, I., "Videovigilancia laboral…", *op. cit.*, anticipó que dicha limitación debería darse en aquellos supuestos en los que se tratara de comprobar ilícitos penales especialmente graves, como el acoso sexual, y para la obtención de pruebas; añadiendo que una interpretación semejante debería exigir que, en cualquier caso, se garantizara el ejercicio de los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición) por parte del trabajador, *op. cit., ult. cit.*

tralice "lo cardinal" de los derechos, como lo es el contenido esencial del derecho a la protección de datos personales; y que dicha medida restrictiva, por ejemplo, la instalación de las cámaras deba ser necesaria y proporcionada. Y todo, en esa secuencia de respetar, en primer lugar, el contenido esencial del derecho fundamental; y, en segundo lugar, y por ese orden, exhortar a la medida restrictiva que cumpla esos tres requisitos ínsitos en el principio de proporcionalidad, mecanismo que administra la intensidad del ejercicio de los derechos cuando entran en liza. Se deberá insistir en que es la medida restrictiva la que debe someterse al cumplimiento de los tres juicios o condiciones que encarna ese principio, medida que en el caso que nos ocupa es adoptada por la parte empresarial[26].

Si nos detenemos en la lectura de dichas excepciones, o de los fines más elevados que permiten la limitación del derecho a la protección de datos personales, observamos que en el RGPD no hallamos ningún apartado que se refiera particularmente al "control de la actividad laboral": ni siquiera hay un epígrafe que permita tales restricciones -con un enunciado estándar como "para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento", por ejemplo. Lo más cercano al tema que nos ocupa lo encontramos en el apdo. d) del art. 23.1 RGPD, al referirse a "la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales". Este enunciado puede vincularse con la restricción del deber de información previa previsto en el art. 22 LOPDGDD que se refiere a los casos en que se capte la "comisión flagrante de un *acto ilícito*"[27].

De este modo, entendemos que la Ley española se ha excedido respecto de lo permitido por el Reglamento, ya que no es lo mismo "infracción penal" que "acto ilícito". Ante esta comparación entre las dos normativas jurídicas, deberá subrayarse que no nos encontramos ante una norma específica instaurada por la LOPDGDD respecto del RGPD, sino de una contravención a lo dispuesto en este último[28]. De hecho, la AEPD en la denominada "Ficha práctica de videovigilancia" relativa a las cámaras para el control empresarial, señala que las imágenes que se utilicen para denunciar delitos o infracciones se acompañarán a la *denuncia* y deberán conservarse para ser entregadas a las Fuerzas y Cuerpos de Seguridad o a los Juzgados y Tribunales que las requieran; añadiendo que no podrán utilizarse para otro fin[29].

Abunda en lo anterior el hecho de que es el art. 88 RGPD el que permite a los Estados, a través de disposiciones legislativas o de convenios colectivos, el establecer normas *más específicas* en el ámbito laboral; pero no ya para limitar el derecho que nos ocupa, sino

---

[26] En esta línea, véase el Informe Jurídico de la AEPD 2017-0139, disponible en: https://www.aepd.es/es/documento/2017-0139.pdf (último acceso: 13 noviembre 2020). Así también, MIGUEL BARRIO, R., "El juicio de proporcionalidad en la prueba de la videograbación oculta a las personas trabajadoras", *Revista de trabajo y seguridad social,* n.º 461-462, 2021, p. 128.

[27] La cursiva es nuestra. En relación con las dudas que suscita este texto, véase la sentencia núm. 52/2019, del Juzgado de lo social n. 3 de Pamplona, de 18 de febrero, AS 2019\101, F.J. 3.

[28] Desde nuestro punto de vista, ese contenido de la LOPDGDD podría ser motivo de recurso de inconstitucionalidad, de igual manera a como ocurrió en el caso de la sentencia del TC (Pleno) 76/2019, 22 de mayo.

[29] Compruébese en: https://www.aepd.es/sites/default/files/2019-09/ficha-videovigilancia-control-empresarial.pdf (último acceso: 7 julio 2022).

"para garantizar la protección de los derechos y libertades en relación con el tratamiento de datos personales de los trabajadores en el ámbito laboral". Expresado en otras palabras, y dada la naturaleza del Reglamento comunitario como norma de obligado cumplimiento, así como de conformidad con el significado de "específico" contenido en el Diccionario de la Real Academia de la Lengua, el RGPD permite *añadir* más normas al espacio de regulación del Derecho de Trabajo, pero no autorizaría a *modificar* sus normas; menos aún a contravenirlas.

La doctrina sentada por el TEDH en dos sentencias conocidas como López Ribalda I (sentencia n. 1874/13) y II (sentencia n. 6567/13)[30] no ha contribuido a pacificar la polémica de las "cámaras ocultas". Ambas sentencias tratan del mismo caso en el que la empresa informó a los trabajadores acerca de la instalación de las cámaras visibles – que se destinaron a comprobar si los clientes estaban hurtando productos-, pero no de las ocultas – que se proyectaron sobre las cajas registradoras y cintas de los productos. Los fallos a los que llegan sendas sentencias son tan dispares que podemos concluir que se ha desmoronado el denominador común que informaba la doctrina de las anteriores sentencias del TEDH, eso es, que la previa información sobre la vigilancia empresarial forma parte del contenido esencial de los derechos a la vida privada, conforme exige el art. 8 del Convenio Europeo de Derechos Humanos[31]. Con la Sentencia López Ribalda II, el Tribunal recuerda "que la información dada a las personas no es sino uno de los criterios que tener en cuenta para apreciar la proporcionalidad de la medida de videovigilancia en el caso de examen. Si tal información falta, las garantías deducibles de los otros criterios revestirán mayor importancia" (párr. 131 in fine)[32].

Por obra de lo mandatado en el art. 23.1 RGPD, el TEDH del conocido como caso López Ribalda II altera el orden de los factores con un resultado eminentemente dispar del de la sentencia López Ribalda I, imponiendo un decurso único para el deber de información y el juicio de proporcionalidad[33]. El deber de información previa al tratamiento de datos personales encarna una evidente relajación del requisito duro representado por el "consentimiento previo del interesado". Si este falta en el orden penal, por ejemplo, la prueba procesal obtenida mediante el tratamiento de datos personales, por ejemplo, sería *nula*[34].

---

[30] Sobre la STEDH López Ribalda I, me remito a TERRADILLOS ORMAETXEA, E., "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", *RDS*, n.º 80, 2017, pp. 147 y ss.; y en relación con la polémica sentencia López Ribalda II, VALDÉS DAL-RE, F., "La ineludible respuesta legislativa y judicial española a la contratación temporal en el sector público sanitario", *Derecho de las Relaciones Laborales,* n.º 5, 2020, p. 661.

[31] VALDÉS DAL-RE, F., "La ineludible respuesta…", *op. cit.*, p. 655.

[32] La cursiva es nuestra. Esta doctrina se empieza a aplicar en España, véase la STSJ de Andalucía, Málaga (Sala de lo Social, Sección 1.ª) Sentencia núm. 1287/2019 de 10 julio, AS\2020\434 (F.J. 5).

[33] Equiparando los fallos de Barbulescu II y López Ribalda II, y enmarcando el conocimiento previo en el test de proporcionalidad, véase CUADROS GARRIDO, M. E., "La protección de los derechos fundamentales de la persona trabajadora ante la utilización de GPS: ¿reformulación o continuidad?", *Lan Harremanak* n.º 42, 2019, pp. 4 y 11. Entre las sentencias del orden jurisdiccional laboral que empiezan a aplicar esta doctrina, véase, por todas, la STS 5 marzo 2020, rec. ud 256/2017, F.J. 5.

[34] Lo que automáticamente no supone que debe ser así calificado el despido, ver por todas, S. Tribunal Superior de Justicia de Madrid, (Sala de lo Social, Sección 5.ª) Sentencia núm. 739/2014 de 29 septiembre. AS 2014\2981.

Entendemos que el mismo calificativo debe depararse a la inexistencia de la información previa en el ámbito de las relaciones laborales. La integración de este deber en el principio de proporcionalidad, como hace la sentencia citada del TEDH, no se comparte: el test anudado al principio de proporcionalidad no valora la legalidad de la *finalidad* del tratamiento de datos, sino que comprueba su presencia, por lo que ese test o examen tampoco es apto para pronunciarse sobre el incumplimiento de una obligación recogida en el reglamento europeo. Si acudimos al RGPD, su art. 5 es meridanamente claro al distinguir entre el principio de transparencia y el principio de proporcionalidad (art. 5.1). Y el principio de transparencia, que exige que toda *información* dirigida al público o al interesado sea concisa, fácilmente accesible y fácil de entender, y que se utilice un lenguaje claro y sencillo, y, además, en su caso, se visualice[35], reclama que todo tratamiento de datos personales deba ser lícito y leal. Por eso, para las personas físicas debe quedar totalmente claro que se están recogiendo, utilizando, consultando o tratando de otra manera datos personales que les conciernen, así como la medida en que dichos datos son o serán tratados. Solo si el tratamiento es lícito y leal podrá ser transparente[36]. Por su parte, se insistirá en que el principio de proporcionalidad se sitúa en otro estadio, en el del interventor que administra el nada infrecuente conflicto entre derechos fundamentales[37], una vez preservados sus respectivos límites internos.

Volviendo a los parámetros de la LOPDGDD, se aclarará, además, que la "atenuación" del deber de información previa en supuestos de comisión flagrante de un acto ilícito, no significa que la información solicitada en el campo de las relaciones laborales pueda ser menos extensa que la exigida en el Reglamento[38]. Es cierto que la Ley –art. 22.4[39]– apela al "dispositivo informativo" en lugar de mencionar el deber de información previa pero ya se ha analizado cómo se traduce este sintagma en la práctica.

Y, además, si se utilizan cámaras ocultas, esto es, no existiendo información o siendo esta insuficiente, entendemos que se invalidaría esa prueba de conformidad con el art. 11.1

---

[35] Apdo. 58 de la EM del RGPD. Un buen ejemplo del cumplimiento escrupuloso de esta obligación que advertir la instalación de las videocámaras y de informar sobre el derecho a la protección e datos en Sentencia del Tribunal Superior de Justicia de Madrid, (Sala de lo Social, Sección 1.ª), núm. 322/2020 de 30 abril. JUR 2020\207752.

[36] Apdo. 39 de la EM del RGPD. Para THIBAULT ARANDA, J., "La vigilancia del uso de Internet en la empresa y la protección de datos personales", *Revista crítica de teoría y práctica,* n.º 1, 2009, p. 219, el principio de transparencia requiere que toda la información y comunicación sea accesible y de fácil entendimiento, con un lenguaje sencillo y claro; de tal forma que si no se dan todos los requisitos exigidos y el trabajador no es alertado de manera completa sobre las circunstancias particulares, el procedimiento deberá entenderse ilegal.

[37] Para una aplicación exquisita de lo comentado, véase la STC 29/2013, 11 febrero, F.J.7 y F.J.8. En otro sentido las Ss. Tribunal Superior de Justicia de Madrid de 30 septiembre 2020; y Tribunal Superior de Justicia de Castilla León/Burgos de 17 septiembre 2020, F.J. 3.º. Por el contrario, no compartimos el fallo de la STS 1 junio 2022, Rec. ud. 1993/2020, donde el principio de proporcionalidad ni siquiera se tiene en cuenta, cuando la sentencia del TSJ Cataluña 7 febrero 2020 (relativa al mismo caso) había denunciado la falta de ese principio en el ejercicio del poder directivo.

[38] Critica esa reducción del contenido de la información, por reducirse a un "cartel informativo", CUADROS GARRIDO, M. E., "La protección de los derechos fundamentales…", *op. cit.*, p. 7.

[39] Dispone ese apartado que "El deber de información previsto en el artículo 12 del Reglamento (UE) 2016/679 se entenderá cumplido mediante la colocación de un dispositivo informativo en lugar suficientemente visible identificando, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos en los artículos 15 a 22 del Reglamento (UE) 2016/679. También podrá incluirse en el dispositivo informativo un código de conexión o dirección de internet a esta información".

de la Ley Orgánica del Poder Judicial, generándose responsabilidades para el empresario[40]. A mayor abundamiento, la Agencia Española de Protección de Datos (AEPD) ofrece una ficha práctica de videovigilancia de cámaras para el control empresarial donde se lee que *"En todos los casos* se deberá informar de la existencia de un sistema de videovigilancia" [41]; y añade que "A este fin de colocará un cartel suficientemente visible en los accesos a las zonas vigiladas, que indicará de forma clara la identidad del responsable de la instalación, ante quién y dónde dirigirse para ejercer los derechos que prevé la normativa de protección de datos, y dónde obtener más información sobre el tratamiento de los datos personales". No solo lo anterior, sino que la AEPD exige que "se pondrá a disposición de los afectados el resto de la información a la que se refiere el artículo 13 del RGPD".

En conclusión, pues, debemos diferenciar entre la videovigilancia oculta y la que se realiza con conocimiento de la persona trabajadora. Como sentencia de referencia contamos con el *"obiter dicta"* de la citada STS de 15 de enero 2019[42]. En ella se trata de remarcar la idea plasmada en la STC 39/2016[43], en el sentido de que el deber de información previa forma parte del contenido esencial del DPD, por lo que las medidas de videovigilancia deben ser informadas con carácter previo y puestas en conocimiento de la parte trabajadora[44].

Por todo lo expuesto en los anteriores epígrafes, cabe concluir que la licitud o no de las cámaras de videovigilancia como medio de prueba, dependerá en última instancia del respeto a los límites antes descritos. En un primer momento, se debe examinar si la prueba incumple alguno de los límites internos del derecho fundamental y el cumplimiento del deber de información previa en toda su extensión ya que, en caso contrario, la prueba se debería considerar ilícita. Solo después de cumplir con estas dos fases previas podríamos pasar a analizar los límites externos, y acudir al triple test de proporcionalidad[45]. Llegados a este punto, si el juez determina en el momento de valorar la prueba, que la medida empresarial adoptada incumple alguno de los límites (falta de necesidad, idoneidad, proporcionalidad, utilización indiscriminada o inexistencia de sospechas razonadas que justifiquen su utilización[46]), estaríamos ante una prueba ilícita[47].

Como consecuencia de calificar una prueba como ilícita, el juez tendría que inadmitir la prueba debido a su obtención a través de la vulneración de derechos fundamentales, por

---

[40] MIÑARRO YANINI, M., "Impacto del reglamento comunitario…", *op. cit.*, p. 14. La autora entiende que la redacción del art. 88 RGPD indica que la regulación legal en cada Estado miembro debe existir en todo caso.
[41] La cursiva es nuestra.
[42] STS 15 de enero 2019, Rec.341/2017, FJ.3.
[43] Un comentario de esta sentencia en GOÑI SEIN, J. L., "Sentencia del Tribunal Constitucional 39/2016, de 3 de marzo. Instalación de cámaras de videovigilancia para la obtención de pruebas y deber de información", *Ars Iuris Salmanticensis,* n.º 2, 2016, p. 288.
[44] STS 15 de enero 2019, Rec.341/2017, FJ.3.
[45] TERRADILLOS ORMAETXEA, M. E., "El principio de proporcionalidad…", *op. cit.*, p. 152.
[46] En relación con la aplicación de esos tres juicios del principio de proporcionalidad en esta materia, cfr. MIGUEL BARRIO, R., "El juicio de proporcionalidad en la prueba de la videograbación oculta a las personas trabajadoras", *Revista de trabajo y seguridad social,* n.º 461-462, 2021, p.1 28; y GUDE FERNÁNDEZ, A., "La videovigilancia en el ámbito laboral y el derecho a la intimidad", *Revista general de derecho constitucional*, n. 20, 2015, p. 9.
[47] MIGUEL BARRIO, R., "El juicio de proporcionalidad…", *op. cit.*, p. 134.

lo que, en el caso de ser la única prueba de cargo que justifique la sanción impuesta al trabajador –o la principal– por haber infringido la buena fe contractual, generalmente el despido, debería conllevar la declaración de nulidad de la misma[48].

Por último, conviene destacar que esta tesis no ha sido secundada por el TC en la STC 61/2021, de 15 de marzo, alejándose de su jurisprudencia anterior, ya que descarta la nulidad del despido tras haberse declarado nula una prueba obtenida por el empresario habiendo vulnerado el derecho a la intimidad y el secreto de las comunicaciones de un trabajador, considerando de aplicación el art. 55.5 del ET respecto al despido improcedente, aunque la videograbación fuera la única prueba que fundamentaba la carta de despido.

En palabras de la STC citada (F.J. 3), "Dicho, en otros términos, no existe un derecho constitucional a la calificación del despido laboral como nulo, por lo que la pretensión de la actora no puede tener sustento en una vulneración de los derechos reconocidos en el art. 18.1 y 3 CE. Tampoco puede imputarse a la resolución impugnada una conculcación de los derechos de la recurrente a la intimidad y al secreto de las comunicaciones, máxime cuando han sido los órganos judiciales quienes han reconocido que dicha vulneración se produjo con la monitorización del ordenador de la trabajadora"

El TC distingue por tanto los supuestos en que la decisión extintiva vulnera un derecho fundamental, de aquellos otros en los que el empresario, al intentar comprobar el comportamiento de su empleada y obtener pruebas de algunos de sus incumplimientos para tratar de justificar un despido, ha vulnerado los derechos fundamentales de la trabajadora. El máximo intérprete de la Constitución indica que no puede confundirse el despido con violación de derechos fundamentales, con el despido en el que ha habido una lesión de los derechos fundamentales en el proceso de obtención de la prueba; algo inaudito que quizás requiera de la intervención del legislador[49].

3. UNA APROXIMACIÓN A LOS LÍMITES DEL TRATAMIENTO AUTOMATIZADO DE DATOS

El análisis de recursos humanos, que en inglés también se conoce como *human analytics,* se define a grandes rasgos como el uso de datos individualizados sobre personas para ayudar a directivos y a profesionales de Recursos Humanos a tomar decisiones en materia de contratación: seleccionar candidatos, evaluar a los trabajadores, considerar posibles ascensos, identificar cuándo hay riesgo de que las personas dejen su empleo y seleccionar futuros líderes. El análisis de recursos humanos se utiliza también para gestionar

---

[48] En el ámbito doctrinal, sin embargo, existen dos grandes tesis Como señala VALLE MUÑOZ, F. A., "Las cámaras de videovigilancia…," *op. cit.*, p. 43, una de las tesis se basa en calificar el despido disciplinario como nulo, ya que la nulidad de la prueba tiene efectos directos en el despido u otra decisión adoptada por el empresario.
Otro sector de la doctrina científica como SEMPERE NAVARRO, A. V. y GIL PLANA, J., y parte de la doctrina judicial [STSJ 5464/2009,de 17 de julio, Madrid, Rec.2831/2009; STSJ 1889/2017 de 21 de marzo, Comunidad Valenciana, Rec.3904/2016. STSJ Cataluña 18 de enero 2021], apoyan la idea de que el despido o sanción impuestos por el empresario al trabajador basada en la prueba ilícita cuya obtención ha vulnerado derechos fundamentales, conlleva la improcedencia del despido o el carácter injustificado de la sanción.

[49] Véase el exquisito voto particular planteado en la sentencia.

el rendimiento de los trabajadores. Son estas materias normalmente identificadas con el poder de dirección empresarial[50]. De acuerdo con las Conclusiones relativas al Plan Coordinado sobre la Inteligencia Artificial del Consejo de la UE, de 11 febrero 2019 (disponible en: https://data.consilium.europa.eu/doc/document/ST-6177-2019-INIT/es/pdf. El Consejo reconocía ya el efecto perturbador y el potencial transformador que la inteligencia artificial tendrá en el mercado laboral actual, por ejemplo, en los sectores industriales, y pedía a un Grupo de expertos, con intervención de los interlocutores sociales, que reflexionaran sobre el particular (véase el documento citado de 2018 de dicho Grupo de expertos).

La Inteligencia Artificial (IA) es actualmente el ámbito más novedoso y prometedor para la gestión de los entornos laborales y de los trabajadores. El 40% de los departamentos de Recursos Humanos de las empresas grandes y pequeñas (sobre todo estadounidenses, pero también europeas) utilizan aplicaciones mejoradas mediante IA. En el ámbito de los recursos humanos, la información recopilada, que cuando alcanza un volumen lo bastante elevado se denomina *big data*, se utiliza para entrenar algoritmos capaces de realizar predicciones relacionadas con el talento y la capacidad de los trabajadores y los candidatos; para supervisar, evaluar y estimular el rendimiento; para fijar objetivos y valorar los resultados del trabajo; para poner en contacto a los trabajadores con los clientes; para juzgar estados de ánimo y emociones; para proporcionar una formación modular en el lugar de producción… Expresado en una sola oración, los algoritmos se utilizan como conductas empresariales de dominio, de creación de "perfiles incontrolables", que pueden llegar a violentar la dignidad, la libertad y la igualdad de las personas[51].

El art. 4. 4) del Reglamento UE 2016/679 define la «elaboración de perfiles» como toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física[52].

El art. 22 Reglamento UE 2016 reconoce el derecho de todo interesado "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"[53]. Con todo, su apdo. 2 excepciona lo manifestado y permite ese tratamiento cuando

---

[50] Con más profundidad, véanse PROYECTO TECHNOS "Inteligencia artificial y su impacto en los recursos humanos y en el marco regulatorio de las relaciones laborales". Cuatrecasas. Instituto de Estrategia Legal en RRHH (Del Rey Guanter), pp. 75 y ss.; VALVERDE ASENCIO, A. J., *Implantación de sistemas de inteligencia artificial y trabajo.* Editorial Bomarzo, 2020, pp. 22 y ss.

[51] Véase el documento "Información algorítmica en el ámbito laboral". *Guía práctica y herramienta sobre la obligación empresarial de información sobre el uso de algoritmos en el ámbito laboral.* Ministerio de Trabajo y Economía Social, mayo 2022.

[52] Además, la opacidad y la autonomía de esos sistemas inteligentes podrían dificultar la trazabilidad de acciones específicas hasta decisiones humanas específicas en su diseño o en su funcionamiento. Por esta y otras cuestiones, el Parlamento europeo aprobó tres informes, de entre los cuales se destacará el que estudia cómo regular la inteligencia artificial para impulsar el respeto de estándares éticos (2020/2012(INL), "Framework of ethical aspects of artificial intelligence, robotics and related technologies").

[53] GOÑI SEIN, J. L., "Controles empresariales. Geolocalización, correo electrónico, Internet, videovigilancia y controles biométricos", *Justicia laboral: revista de Derecho del Trabajo y de la Seguridad Social,* n.º 39, 2009, p. 11.

la decisión individualizada automatizada "es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento"; aunque a continuación condiciona dicho tratamiento a la adopción de las "medidas adecuadas para salvaguardar 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".

Un estudio, no nuevo, de Deloitte[54] concluyó que el 71 % de las compañías internacionales consideran que el análisis de recursos humanos es una de las prioridades de sus organizaciones porque, y no solo proporcionará ideas valiosas para el negocio, sino que también ayudará a gestionar lo que se ha dado en llamar el «problema de las personas».

En España, el Informe elaborado por el Ministerio de Trabajo y Economía Social[55], recuerda el derecho individual a obtener información sobre las decisiones íntegramente automatizadas sobre las personas trabajadoras de conformidad con distintos fundamentos jurídicos del RGPD; así como que todas las empresas tienen la obligación suministrar esa información individual cuando sean requeridas para ello.

Desde la premisa de que el acopio de datos es la antesala de la propia parametrización de cualquier sistema inteligente, deben garantizarse los principios y derechos básicos de dicha normativa[56]. En conclusión, por tanto, lo anteriormente expuesto en relación con los límites que el poder de dirección y control encuentra cuando se topa con el DPD es totalmente aplicable al ámbito de las decisiones automatizadas de datos.

BIBLIOGRAFÍA

BAZ RODRÍGUEZ, J., "La Ley Orgánica 3/2018 como marco embrionario de garantía de los derechos digitales laborales. Claves para un análisis sistemático", *Trabajo y Derecho,* n.º 54, 2019.

CASAS BAAMONDE, M.ª E. y ÁNGEL QUIROGA, M., "Los derechos fundamentales a la intimidad y a la protección de datos personales en la economía digital. Geolocalización de los trabajadores a través de GPS del vehículo de empresa. Despido procedente". *Revista de jurisprudencia laboral,* n.º 9, 2020.

COLLINS, L.; FINEMAN, D. R. y TSUCHIDA, A., «People Analytics: Recalculating the Route», Deloitte Insights. 2017. Disponible en: https://www2.deloitte.com/insights/us/en/focus/human-capital-trends/2017/people-analytics-in-hr.html (última apertura 28 junio 2022).

CUADROS GARRIDO, M. E., "La protección de los derechos fundamentales de la persona trabajadora ante la utilización de GPS: ¿reformulación o continuidad?", *Lan Harremanak* n.º 42, 2019.

Este autor alerta de que la IA se trata de una herramienta que permite crear una base de datos de información personal y obtener perfiles sociales de los trabajadores afectado.

[54] Collins, L.; Fineman, D. R. y Tsuchida, A. (2017): "People Analytics: Recalculating the Route", Deloitte Insights. Disponible en: https://www2.deloitte.com/insights/us/en/focus/human-capital-trends/2017/people-analytics-in-hr.html (última apertura 28 junio 2022).

[55] Véase, de nuevo, el documento "Información algorítmica en el ámbito laboral…", *op. cit.*, pp. 9 y 10.

[56] VALVERDE ASENCIO, A. J., *Implantación…, op. cit.,* p. 82.

FERNÁNDEZ DOMINGUEZ, J. J., "El marco jurídico de la protección de datos personales: Reglamento UE 2016/679 y Ley Orgánica 3/2018, de 5 de diciembre", *Revista del Ministerio de Trabajo y Economía Social,* n.148, 2021

GARCÍA-PERROTE ESCARTÍN, I. y MERCADER UGUINA, J. R., "La protección de datos se come a la intimidad: la doctrina de la sentencia del Tribunal Europeo de Derechos Humanos de 5 de septiembre de 2017, Gran Sala (caso Barbulescu v. Rumanía; n.º 61496/08)", *Revista de Información Laboral,* n.º 10, 2017.

GOÑI SEIN, J. L., "Controles empresariales. Geolocalización, correo electrónico, Internet, videovigilancia y controles biométricos", *Justicia laboral: revista de Derecho del Trabajo y de la Seguridad Social,* n.º 39, 2009.

_____. "Sentencia del Tribunal Constitucional 39/2016, de 3 de marzo. Instalación de cámaras de videovigilancia para la obtención de pruebas y deber de información", *Ars Iuris Salmanticensis,* n.º 2, 2016.

GUDE FERNÁNDEZ, A., "La videovigilancia en el ámbito laboral y el derecho a la intimidad", *Revista general de derecho constitucional,* n.º 20, 2015.

INSTITUTO CUATRECASAS (DIR. EL REY GUANTER, S.), *Inteligencia artificial y su impacto en los recursos humanos y en el marco regulatorio de las relaciones laborales.* Cuatrecasas. Instituto de Estrategia Legal en RRHH, 2018.

JIMÉNEZ-CASTELLANOS BALLESTEROS, I., "Videovigilancia laboral y derecho fundamental a la protección de datos", *Temas Laborales* n.º 136, 2017.

LÓPEZ BALAGUER, M., "El control empresarial por videovigilancia en la LOPD", *Revista andaluza de trabajo y bienestar social,* n.º 151, 2020.

MARÍN MALO, M., "La geolocalización del trabajador. Reflexiones a la luz de la jurisprudencia reciente", *LABOS Revista del Derecho del Trabajo y Protección Social,* n.º 1, 2020.

MIGUEL BARRIO, R., "El juicio de proporcionalidad en la prueba de la videograbación oculta a las personas trabajadoras", *Revista de trabajo y seguridad social,* n.º 461-462, 2021.

MINISTERIO DE TRABAJO Y ECONOMÍA SOCIAL, *Guía práctica y herramienta sobre la obligación empresarial de información sobre el uso de algoritmos en el ámbito laboral,* mayo 2022. Disponible en: https://www.mites.gob.es

MIÑARRO YANINI, M., "Impacto del reglamento comunitario de protección de datos en las relaciones laborales: un –pretendido– «cambio cultural»", *RTSS CEF* n.º 423, 2018.

MOLINA NAVARRETE, C., "El «trabajador transparente», entre metáfora y realidad, y el «efecto útil» de los derechos de la personalidad en la empresa del siglo XXI". *RTSS. CEF,* n. 419, 2018

RODRÍGUEZ ESCANCIANO, S., "El derecho a la protección de datos personales en el contrato de trabajo: reflexiones a la luz del Reglamento europeo 2016/679", *Estudios financieros. Revista de trabajo y seguridad social,* n.º 423, 2018.

SERRANO GARCÍA, J. Mª., "Límites de la ley de protección de datos al poder de dirección del empresario", *La protección de datos y la regulación de las tecnologías en la negociación colectiva y en la jurisprudencia,* Editorial Bormazo, Albacete, 2019.

TERRADILLOS ORMAETXEA, E., "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,* n.º 80, 2017.

THIBAULT ARANDA, J., "La vigilancia del uso de Internet en la empresa y la protección de datos personales", *Revista crítica de teoría y práctica,* n.º 1, 2009.

VALDÉS DAL-RÉ, F., "La ineludible respuesta legislativa y judicial española a la contratación temporal en el sector público sanitario", *Derecho de las Relaciones Laborales,* n.º 5, 2020.

VALLE MUÑOZ, F. A., "Control tecnológico empresarial y licitud de la prueba en el proceso laboral" desarrollado en el marco del proyecto de investigación", *Trabajo y derecho: nueva revista de actualidad y relaciones laborales,* n.º 87, 2022.

VALVERDE ASENCIO, A. J., *Implantación de sistemas de inteligencia artificial y trabajo.* Editorial Bomarzo, 2020.