DERECHOS DIGITALES, PROTECCIÓN DE DATOS Y CONTROL EMPRESARIAL EN ESPAÑA

MARÍA ELISA CUADROS GARRIDO

Profesora Contratada Doctora del Departamento de Derecho del Trabajo y de la Seguridad Social de Facultad de Derecho de la Universidad de Murcia (España).

1. ENFOQUE CONFLICTIVISTA

Las Tecnologías de la información y de la Comunicación (TICs) han puesto en un primer plano la necesidad de que en el desarrollo del contrato de trabajo se respeten los derechos fundamentales de dignidad e intimidad del trabajador y asimismo su derecho a la autodeterminación informativa. Las nuevas tecnologías generan profundas transformaciones en la organización de las empresas y cambios de principios en la práctica laboral, y asimismo llevan a los jueces a adoptar nuevos cánones, gestados y madurados extramuros de las salas en las que los pleitos se convierten en *litis.*

El debate judicial se centra en el conflicto entre los diversos derechos constitucionales del empleado que pueden quedar afectados por el uso de las nuevas tecnologías y que, en su mayoría, pertenecen a la primera generación de derechos fundamentales, que quedó plasmada en las manifestaciones más incipientes del constitucionalismo europeo moderno, aparecidas a lo largo del siglo XIX, como derechos que se caracterizan por reunir el doble requisito de ser de la persona o de la personalidad. Por una parte, pertenecen al trabajador en su condición de tal, aun cuando se ejerzan en el marco del contrato de trabajo, y de otra por ser derechos de libertad, ya que su objeto consiste en la expectativa de la ausencia de intromisiones o interferencias.

Y en el lado contrapuesto, por parte del empleador se encuentran el derecho a la libertad de empresa y el derecho de propiedad, de aparición más tardía, pues surgen ya en el siglo XX a resultas del nuevo pacto social que refundó las relaciones entre Estado y Sociedad.

Los equilibrios y limitaciones que conlleva el contrato de trabajo, para el empresario y el trabajador, suponen que las facultades organizativas

empresariales se encuentran restringidas por los derechos fundamentales del trabajador, quedando el empleador obligado a respetarlos.

Partiendo de la prevalencia de los derechos del trabajador, los límites que quiera poner la empresa. Solo se pueden derivar del hecho de que la propia naturaleza del trabajo contratado implique la restricción del derecho; de tal forma que el ejercicio de las facultades organizativas y disciplinarias del empleador no puede servir en ningún caso de sustento a la producción de resultados inconstitucionales. Y ello porque los derechos constitucionales de cualquier ciudadano *acompañan al trabajador durante toda la vida de la relación laboral, como un veto ínsito a las prerrogativas empresariales*. Por este motivo, el Tribunal Constitucional destaca la necesidad de que las resoluciones judiciales preserven *el necesario equilibrio entre las obligaciones dimanantes del contrato de trabajo y el ámbito modulado de su libertad constitucional*.

En igual sentido, se incide en que precisamente allí donde se plantea una *fuerte tensión dialéctica* es en el lugar de fricción entre los derechos constitucionales del empresario y los fundamentales del trabajador, que disfrutan de una dimensión constitucional diferente.

La doctrina más autorizada señala que el efecto más relevante de las nuevas tecnologías en el ámbito de las relaciones laborales consiste en haber abierto un nuevo escenario conflictivo, en el que las partes siguen siendo los litigantes de siempre, trabajador y empresario, pero la controversia ya no suscita un problema de legalidad o de contractualidad, sino de colisión entre dos categorías de derechos constitucionales (Valdés Dal-Ré, 2009).

A este escenario conflictivo se puede llegar por dos vías, una, por el control que la empresa realiza del uso de las TICs por parte del trabajador, y otra, por el recurso a los adelantos tecnológicos por parte del empleador para controlar al personal contratado (Cuadros Garrido, 2018).

2. DERECHOS DIGITALES

2.1. Normativa

La nueva era digital protagonizada por *Internet de las Cosas* ha supuesto la creación de unos derechos nuevos, que encuentran en parte su fundamento en el derecho preexistente a la protección de datos de la Constitución Española[1] (CE) ubicado en su art. 18.4, pero que implican una adaptación de construcciones clásicas a los requerimientos del avance de la tecnología (Cobacho López, 2019, 226-ss).

Frente al nulo desarrollo que la normativa de protección datos experimentó en el ámbito laboral en España, a nivel europeo el Reglamento General sobre Protección de Datos[2] (RGPD) abrió la posibilidad de intervenir en ese ámbito hasta esa fecha ignorado por la normativa estatal.

El RGPD establece una normativa única, válida en toda la UE y aplicable al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado del tratamiento en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no. El RGPD impuso a los Estados de la UE que adaptaran su normativa a este con la fecha máxima de su entrada en vigor, a saber, en el año 2018.

De este modo, el RGPD incorpora nuevas reglas sobre extraterritorialidad de las normas y se aplicará fuera de la Unión Europea cuando el tratamiento de datos personales de interesados residentes en la Unión se efectúe por responsables o encargados del tratamiento no establecidos en la Unión y las actividades de tratamiento estén relacionadas con dos escenarios:

1 BOE núm. 311, de 29 de diciembre de 1978.

2 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). DOCE 4 mayo de 2016, núm. 119.

1) La oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si se requiere un pago por parte del interesado.
2) El control de su conducta, en la medida en que esta tenga lugar en la Unión Europea.

En el ámbito laboral, los aspectos más relevantes del RGPD son los siguientes:

1. El tratamiento de datos está prohibido cuando revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida o la orientación sexuales de una persona física.
2. El Reglamento da la posibilidad a los Estados miembros de establecer normas más específicas, a través de disposiciones legislativas o de convenios colectivos, para garantizar la protección de los derechos y libertades en relación con el tratamiento de datos personales de los trabajadores en el ámbito laboral, en particular a efectos de contratación de personal, ejecución del contrato laboral, incluido el cumplimiento de las obligaciones establecidas por la ley o por el convenio colectivo, gestión, planificación y organización del trabajo, igualdad y diversidad en el lugar de trabajo, salud y seguridad en el trabajo, protección de los bienes de empleados o clientes, así como a efectos del ejercicio y disfrute, individual o colectivo, de los derechos y prestaciones relacionados con el empleo y a efectos de la extinción de la relación laboral.
3. Las normas que establezcan los Estados deben incluir medidas adecuadas y específicas para preservar la dignidad humana de los interesados, así como sus intereses legítimos y sus derechos fundamentales, prestando especial atención a la transparencia del tratamiento, a la transferencia de los datos personales dentro de un grupo empresarial o de una unión de empresas dedicadas

a una actividad económica conjunta y a los sistemas de supervisión en el lugar de trabajo.

4. La figura del *Delegado de Protección de Datos* fue altamente debatida en todo el proceso regulatorio. Al final, el RGPD ha optado por una solución intermedia, que es la obligatoriedad en la designación de dicha figura, pero sólo para determinados casos concretos, como Administraciones Públicas, entidades cuya principal actividad lleve aparejada la monitorización de datos personales o el tratamiento de datos personales a gran escala y entidades cuya principal actividad lleve aparejado el tratamiento de datos especialmente protegidos a gran escala, así como de antecedentes penales.

Respondiendo al mandato europeo, la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales[3] (LO 3/2018) introdujo en el ordenamiento jurídico español un sistema de garantías de los derechos digitales que, en algunos casos, ya habían sido perfilados por la jurisprudencia europea. Mientras no exista una reforma de la Constitución Española que los eleve a rango constitucional, los derechos digitales quedan recogidos en los arts. 79 a 97 de la LO 3/2018, sin la especial protección que se otorga a los derechos fundamentales[4].

3 BOE núm. 294, de 6 de diciembre de 2018. La aprobación de la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales supuso una novedad respecto a la anterior normativa ya que extiende su ámbito material a las relaciones de trabajo. En esta regulación tal y como se establece en sus artículos 87 a 91 dentro del capítulo X, Garantía de los Derechos Digitales, se vienen a considerar lícitos los medios de control empresarial a través de las TICs siempre que respeten los derechos constitucionales superando determinados requisitos.

4 De acuerdo con su ubicación en la Constitución Española de 1978, podemos diferenciar: derechos fundamentales, derechos ordinarios de los ciudadanos y principios económicos y sociales. Tanto los derechos fundamentales como los ordinarios (arts. 30 a 38) son susceptibles de aplicación directa, sin necesidad de desarrollo legal previo, mientras que los principios económicos y sociales (arts. 39 a 52) requieren una regulación previa. Por su parte, los derechos fundamentales son los reconocidos en el Título I, Capítulo II, Sección I de la Constitución Española, todos los cuales están amparados por el máximo nivel de protección constitucional, artículos 14 a 29.

2.2. Derechos digitales

Los derechos digitales, podemos definirlos como derechos y libertades reconocidos a todos los ciudadanos predicables al entorno de Internet, tal tenor literal es la definición de la Exposición de Motivos de la referida LO (Sánchez Trigueros y Cuadros Garrido, 2019, 100-103). Pero tal definición, se nos deviene insuficiente porque el hecho cierto, es que estos nuevos derechos forman un elenco heterogéneo no solo relacionado con la Web.

Gran parte de los derechos digitales carecen de una relación directa con la autodeterminación informativa y se conectan más bien con otros derechos fundamentales de las personas de nuestra Carta Magna, como la dignidad del art. 10 (neutralidad de Internet, acceso universal a la Web[5], seguridad digital[6], educación digital[7], y actualización de informaciones[8]), como la igualdad y no discriminación del art. 14, como los del art. 18.1 la intimidad, el honor o como la libertad de expresión del art. 20 (rectificación en internet[9]) e incluso fuera del texto constitucional, relacionado

5 Art. 81 LO 3/2018. De modo que todos tienen derecho a acceder a Internet independientemente de su condición personal, social, económica o geográfica, y que los poderes públicos quedan obligados a ofrecer un acceso universal, asequible, de calidad y no discriminatorio para toda la población, procurando superar tanto la brecha de género en el ámbito personal y laboral, como brecha generacional mediante acciones dirigidas a la formación y el acceso a las personas mayores, y ofreciendo posibilidades reales en entornos rurales y para las personas que cuenten con necesidades especiales.

6 Art. 82 LO 3/2018. Que implica en esencia seguridad de las comunicaciones que se transmitan y reciban a través de Internet, con el consiguiente deber de los proveedores de servicios de Internet de informar a los usuarios de sus derechos.

7 Art. 83 LO 3/2018. En el sentido de que el sistema educativo deberá garantizar la plena inserción del alumnado en la sociedad digital y el aprendizaje de un uso de los medios digitales que sea seguro y respetuoso con la dignidad humana, los valores constitucionales, los derechos fundamentales y, particularmente con el respeto y la garantía de la intimidad personal y familiar y la protección de datos personales.

8 Art. 85 LO 3/2018. Es un derecho respecto a los medios de comunicación digitales, por el que toda persona tiene derecho a solicitar motivadamente de los medios de comunicación digitales la inclusión de un aviso de actualización suficientemente visible junto a las noticias que le conciernan cuando la información contenida en la noticia original no refleje su situación actual como consecuencia de circunstancias que hubieran tenido lugar después de la publicación, causándole un perjuicio.

9 Art. 84 LO 3/2018. Los responsables de redes sociales y servicios equivalentes deberán

con conceptos jurisprudenciales del Tribunal Constitucional como la privacidad[10] (derecho a la desconexión digital[11]). Si bien otros derechos digitales, forman parte del núcleo duro del derecho a la protección de datos, mereciendo destacarse entre ellos el derecho al olvido en búsquedas de internet[12], derecho al olvido en redes sociales y servicios equivalentes[13], el

adoptar protocolos adecuados para posibilitar el ejercicio del derecho de rectificación ante los usuarios que difundan contenidos que atenten contra el derecho al honor, la intimidad personal y familiar en Internet y el derecho a comunicar o recibir libremente información veraz.

10 STC 12/2012, de 30 de enero. Según el TC reside en derivar los contornos mismos del derecho fundamental a la intimidad del entorno de la privacidad, en su configuración material, es un derecho de exclusión que todo ciudadano tiene de hacerlo valer, frente a los poderes públicos o al resto de la sociedad.

11 La desconexión digital laboral o el derecho a la desconexión laboral es la facultad de los trabajadores a desconectar del trabajo por medios digitales una vez finalizada la jornada laboral convenida. Como precedentes destacables, poner de manifiesto que la figura se encontraba ya regulada en el Derecho francés desde 2016. Fue el supuesto de derechos digitales más mediático, a pesar de que es una norma abierta, pues remite a la negociación colectiva y en todo caso a la autorregulación del empleador, por ello se ha calificado como un derecho formalmente novedoso. Respecto a la aplicabilidad, se extiende a cualquier forma de trabajo incluido el teletrabajo. Son varios los factores que motivan la existencia de este derecho, por un lado, la conciliación de la vida personal y la familiar, por otro lado, la dicotomía entre tiempo de trabajo y de descanso y, finalmente, la prevención del tecnoestrés.

12 Desde que se publicó la conocida STJUE de 13 de mayo de 2014 (Caso Google Spain S.L contra Agencia Española de Protección de Datos) se ha ido configurando el *derecho al olvido*. En dicha sentencia se estimaba la pretensión de un ciudadano español que pedía la cancelación de resultados obtenidos al buscar su nombre en Google, pues mostraba una información desactualizada, en el sentido de *desindexación*; alude al derecho de la persona a dejar de tener un perfil *on line*, es decir, a eliminar de la Red su huella digital. y se ha ido concretado su ejercicio. Art. 93 LO 3/2018. "Toda persona tiene derecho a que los motores de búsqueda en Internet eliminen de las listas de resultados que se obtuvieran tras una búsqueda efectuada 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, teniendo en cuenta los fines para los que se recogieron o trataron, el tiempo transcurrido y la naturaleza e interés público de la información. Del mismo modo deberá procederse cuando las circunstancias personales que en su caso invocase el afectado evidenciasen la prevalencia de sus derechos sobre el mantenimiento de los enlaces por el servicio de búsqueda en Internet".

13 Art. 94 LO 3/2018. "Toda persona tiene derecho a que sean suprimidos, a su simple solicitud, los datos personales que hubiese facilitado para su publicación por servicios de redes sociales y servicios de la sociedad de la información equivalentes, así como a la

derecho de portabilidad[14], o el derecho al testamento digital[15] como de los más relevantes (Sánchez Trigueros y Cuadros Garrido, 2019, 104).

Por lo anterior, la doctrina considera más que plausible un desacuerdo al encaje de esta mezcla de derechos digitales dentro de una Ley Orgánica dedicada a la protección de datos; y aún más criticable es, precisamente,

supresión de los datos personales que le conciernan y que hubiesen sido facilitados por terceros para su publicación por los servicios de redes sociales y servicios de la sociedad de la información equivalentes cuando fuesen inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieren devenido como tales por el transcurso del tiempo, teniendo en cuenta los fines para los que se recogieron o trataron, el tiempo transcurrido y la naturaleza e interés público de la información".

14 El art. 17 de la LO 3 /2018 recoge lo siguiente: "El derecho a la portabilidad se ejercerá de acuerdo con lo establecido en el artículo 20 del Reglamento (UE) 2016/679". Este reconocimiento a la portabilidad de los datos supuso una gran novedad del Reglamento Europeo que se recoge en su artículo 20.1:
"El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitad".
Este derecho se aplica cuando el interesado haya facilitado los datos personales dando su consentimiento o cuando el tratamiento sea necesario para la ejecución de un contrato.

15 El art. 96.1 de la LO 3/2019 tiene el siguiente tenor literal:" 1. El acceso a contenidos gestionados por prestadores de servicios de la sociedad de la información sobre personas fallecidas se regirá por las siguientes reglas: a) Las personas vinculadas al fallecido por razones familiares o de hecho, así como sus herederos podrán dirigirse a los prestadores de servicios de la sociedad de la información al objeto de acceder a dichos contenidos e impartirles las instrucciones que estimen oportunas sobre su utilización, destino o supresión. Como excepción, las personas mencionadas no podrán acceder a los contenidos del causante, ni solicitar su modificación o eliminación, cuando la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley. Dicha prohibición no afectará al derecho de los herederos a acceder a los contenidos que pudiesen formar parte del caudal relicto. b) El albacea testamentario, así como aquella persona o institución a la que el fallecido hubiese designado expresamente para ello también podrá solicitar, con arreglo a las instrucciones recibidas, el acceso a los contenidos con vistas a dar cumplimiento a tales instrucciones. c) En caso de personas fallecidas menores de edad, estas facultades podrán ejercerse también por sus representantes legales o, en el marco de sus competencias, por el Ministerio Fiscal, que podrá actuar de oficio o a instancia de cualquier persona física o jurídica interesada. d) En caso de fallecimiento de personas con discapacidad, estas facultades podrán ejercerse también, además de por quienes señala la letra anterior, por quienes hubiesen sido designados para el ejercicio de funciones de apoyo si tales facultades se entendieran comprendidas en las medidas de apoyo prestadas por el designado".

mezclar cuestiones laborales relativas a la intimidad de los trabajadores en el entorno digital, con cuestiones relativas al derecho de acceso a Internet, la seguridad digital, el derecho a la educación digital, el derecho de portabilidad en servicios de redes sociales y equivalentes, o el derecho al testamento digital, materias todas ellas tratadas en el Título X de la LO 3/2018. El único nexo en común que fuerza el legislador es, precisamente, que los derechos y libertades de la Constitución son plenamente aplicables en Internet, de tal modo que, pudiendo afectar las nuevas tecnologías digitales a derechos consagrados constitucionalmente, en especial a la intimidad reconocida en el artículo 18.4 de nuestra Constitución, su encaje de regulación parece un tanto forzado (Quilez Moreno, 2019).

Por otro lado, cabe aludir que el catálogo de derechos digitales laborales implica en sí mismo una regulación *ex novo* de la dicción del artículo 20.3[16] Estatuto de los Trabajadores[17] (ET), la cual se ve además reforzada por la adición de un artículo *20 bis*[18] al texto estatutario, el cual remite de forma íntegra, a la LO 3/18 (Sánchez Quiñonez, 2019).

16 Autoriza al empresario a adoptar *las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana y teniendo en cuenta la capacidad de los trabajadores disminuidos.* Ya en la propia dicción de la norma del 20.3 ET, se apunta la íntima relación existente entre las genéricas facultades empresariales de dirección y de organización que permiten adoptar medidas de supervisión o vigilancia de la actividad laboral al empresario, y la atribución de tales facultades sobre el trabajador; lo que se justifica en las potestades derivadas del contrato de trabajo, cuyo fundamento se encuentra en la libertad de empresa, reconocida en el artículo 38 CE.

17 Texto refundido de la Ley del Estatuto de los Trabajadores**.** Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores. BOE núm. 255, de 24 de octubre de 2015.

18 "Derechos de los trabajadores a la intimidad en relación con el entorno digital y a la desconexión. Los trabajadores tienen derecho a la intimidad en el uso de los dispositivos digitales puestos a su disposición por el empleador, a la desconexión digital y a la intimidad frente al uso de dispositivos de videovigilancia y geolocalización en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales". Si bien con una simple lectura de dicho artículo resultará difícil saber en qué se concreta exactamente el contenido de cada uno de los derechos allí recogidos. La remisión a la normativa sobre protección de datos pone finalmente algo de luz a estas cuestiones de ámbito laboral, que tantas dudas había generado, otorgándose una mayor seguridad jurídica.

2.3. El derecho a la protección de datos

La autodeterminación informativa, protección de datos o libertad informática, como ya se ha aludido, constituye un derecho fundamental reconocido en el art. 18.4[19] de la Constitución Española pero que, en el año 2000, fue *rebautizado* por el Tribunal Constitucional evitando así la obsolescencia del texto constitucional (Sempere Navarro, 2020), en este sentido, el TC ha declarado la libertad informática tiene por objeto especifico garantizar a las personas la potestad de control sobre el uso de los datos propios[20].

El tratamiento automatizado de datos de carácter personal constituye una cuestión objeto de estudio en España y en otros países europeos y a la que las diferentes cortes constitucionales, deben otorgar una respuesta sobre la base de un material normativo que son los preceptos constitucionales respectivos. Desde esta óptica, es sencillo comprender que en ninguna otra rama del Derecho sea el comparatismo tan hacedero (Pérez de los Cobos, 2019).

19 Con el siguiente tenor literal: "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

20 En el inicio del siglo XXI, el proceso de reconocimiento del derecho a la protección de datos como autónomo, marca un precedente importante, con las SSTC 290/2000 y 292/2000. Por un lado, la STC 290/2000, 30 de noviembre se pronunció sobre la constitucionalidad de la ya entonces derogada Ley Orgánica Reguladora del Tratamiento Automatizado de Datos de Carácter Personal de 1992 (LORTAD). Aunque no aborda cuestiones sustantivas sobre el derecho, es muy interesante el voto particular del Magistrado Jiménez de Parga, en el que se expresan las razones por las cuales, a su juicio, *debió afirmarse de modo explícito, en la argumentación de ella, que nuestro Tribunal reconoce y protege ahora un derecho fundamental, el derecho de libertad informática, que no figura en la Tabla del texto de 1978.*
Por su parte la STC 292/2000, de 4 de enero, parte del reconocimiento de un derecho fundamental específico, derecho a la protección de datos o libertad informática, que coexiste con otros derechos. Para el Tribunal Constitucional *la garantía de la vida privada y de la reputación tiene hoy una dimensión positiva que excede el ámbito propio del derecho fundamental a la intimidad*. Y que se traduce en un derecho de control sobre los datos relativos a la propia persona.

La cobertura legal de la protección de datos reviste un perfil muy formalista[21], ya que garantiza a la persona el control activo de las informaciones que le afectan, el derecho a no ser instrumentalizada a través del conocimiento adquirido de aspectos de nuestra personalidad, en la medida en que supone ser informada de quién posee sus datos personales, a qué uso se están sometiendo y la facultad de ejercer los tradicionales derechos ARCO (acceso, rectificación[22], cancelación[23] y oposición[24]) que junto con los nuevos derechos de la LO3/2018 a la portabilidad, al olvido, y a la limitación al tratamiento configuran con los derechos ARCOPOL. Por tanto, el derecho a la protección de datos consta de dos elementos, por un lado, el derecho a decidir y consentir sobre la obtención y uso de los datos, y por otro, el derecho a obtener información puntual y exacta acerca de su tratamiento y trayectoria (García Murcia y Rodríguez Cardo, 2019).

En un entorno globalizado como el tecnológico, la aplicación extraterritorial de las normas constituye un verdadero desafío, pues no tendría demasiado sentido limitarlas a un determinado espacio, por el principio de aplicación territorial de la Ley, o a un concreto conjunto de personas, por imperativo del principio de personalidad. Frente al escaso desarrollo que la normativa de protección datos había experimentado[25], a nivel europeo

21 De modo que una intromisión empresarial, por ejemplo, puede no vulnerar ni la intimidad del trabajador ni el secreto de las comunicaciones, pero, puede estar quebrando su derecho a la protección de datos personales.

22 Art. 14. LO 3 /2018.Tiene el siguiente contenido:" Al ejercer el derecho de rectificación reconocido en el artículo 16 del Reglamento (UE) 2016/679, el afectado deberá indicar en su solicitud a qué datos se refiere y la corrección que haya de realizarse. Deberá acompañar, cuando sea preciso, la documentación justificativa de la inexactitud o carácter incompleto de los datos objeto de tratamiento".

23 Art. 15. LO 3 /2018. Con el tenor literal de a continuación: "1. El derecho de supresión se ejercerá de acuerdo con lo establecido en el artículo 17 del Reglamento (UE) 2016/679".

24 Art. 18. LO 3 /2018. El derecho de oposición, así como los derechos relacionados con las decisiones individuales automatizadas, incluida la realización de perfiles, se ejercerán de acuerdo con lo establecido, respectivamente, en los artículos 21 y 22 del Reglamento (UE) 2016/679.

25 Como antecedentes destacables, el art. 8 del Convenio de Roma protege, en general, el derecho al respeto de la vida privada, pero no contiene referencia alguna a la protección de datos de carácter personal, lo que no puede extrañar si se tiene en cuenta que este

el RGPD se abrió la posibilidad de intervenir en este ámbito hasta ahora ignorado por la normativa estatal española.

3. CONTROL EMPRESARIAL

3.1. Delimitación

Abordando la problemática desde la perspectiva del Derecho del Trabajo, uno de los riesgos del tratamiento de los datos de los empleados por parte del titular de la relación laboral, supone la posible creación de perfiles virtuales con datos subjetivos o bien la utilización de la información para una finalidad distinta de la que se recogió (Rodríguez Escanciano, 2015). En este sentido los datos y la información que el empresario obtiene pueden ser usados con fines legítimos de control de la prestación laboral o bien con intenciones ilegítimas lo que provoca discriminación y un ataque directo a la dignidad de la persona trabajadora (Sierra Hernáiz. 2020).

El derecho a la protección de datos personales que asiste al trabajador, y que conecta en buena medida con su derecho a la intimidad y a la consideración debida a su dignidad como persona (art. 4.2[26] ET), debe

instrumento fue adoptado en 1950. Sin embargo, otros documentos internacionales de ámbito regional europeo se refieren específicamente a la protección de los datos personales. Por su parte de la Carta de Derechos Fundamentales de la Unión Europea (DOCE 30 marzo 2010, núm. 83.) que en su art. 8 consagra el derecho de toda persona "a la protección de los datos de carácter personal que le conciernan", muy ligado por lo demás al derecho al respeto de la vida privada y familiar reconocido en su art. 7.

26 En la relación de trabajo, los trabajadores tienen derecho:
a) A la ocupación efectiva.
b) A la promoción y formación profesional en el trabajo, incluida la dirigida a su adaptación a las modificaciones operadas en el puesto de trabajo, así como al desarrollo de planes y acciones formativas tendentes a favorecer su mayor empleabilidad.
c) A no ser discriminados directa o indirectamente para el empleo, o una vez empleados, por razones de sexo, estado civil, edad dentro de los límites marcados por esta ley, origen racial o étnico, condición social, religión o convicciones, ideas políticas, orientación sexual, afiliación o no a un sindicato, así como por razón de lengua, dentro del Estado español.
Tampoco podrán ser discriminados por razón de discapacidad, siempre que se hallasen en condiciones de aptitud para desempeñar el trabajo o empleo de que se trate.
d) A su integridad física y a una adecuada política de prevención de riesgos laborales.

conectarse con los poderes del empresario y, particularmente, con sus facultades de control y vigilancia (art. 20.3 ET).

Para efectuar la pertinente ponderación entre ambos extremos los tribunales españoles e internacionales habitualmente manejan el principio de proporcionalidad, que es un criterio metodológico que cumple la función de estructurar el procedimiento interpretativo para la determinación del contenido de los derechos fundamentales. Sirve para controlar cualesquiera actos que inciden sobre los intereses de los particulares.

En las alusiones jurisprudenciales más representativas, este principio aparece articulado de tres subprincipios: idoneidad, necesidad y proporcionalidad en sentido estricto. Cada uno expresa determinada exigencia que toda intervención en derechos fundamentales debe cumplir:

- Que la intervención sea adecuada para alcanzar el fin que se propone.
- Que sea necesaria, en cuanto que no quepa una medida alternativa, menos gravosa para el interesado.
- Que sea proporcionada en sentido estricto; que en ningún caso suponga un sacrificio excesivo del derecho. Este último requisito significa que aun cuando la medida sea adecuada y necesaria, deberá considerarse inválida si implica el vaciamiento del derecho en juego.

3.2. El consentimiento

El primer aspecto que procede analizar es el del consentimiento ya que la obtención de este por parte de sujeto del afectado constituye una

e) Al respeto de su intimidad y a la consideración debida a su dignidad, comprendida la protección frente al acoso por razón de origen racial o étnico, religión o convicciones, discapacidad, edad u orientación sexual, y frente al acoso sexual y al acoso por razón de sexo.
f) A la percepción puntual de la remuneración pactada o legalmente establecida.
g) Al ejercicio individual de las acciones derivadas de su contrato de trabajo.
h) A cuantos otros se deriven específicamente del contrato de trabajo.

de las piezas fundamentales en el régimen del tratamiento de los datos de carácter personal. La regulación general se encuentra en el art. 6 LO 3/2018 [27]

En el apartado 2 del art.6 afirma el consentimiento ha de ser otorgado de manera expresa tantas veces como finalidades distintas tenga el tratamiento de datos[28].

Pero en el ámbito laboral el consentimiento del trabajador pasa, como regla general a un segundo plano, pues se entiende implícito en la relación negocial, siempre que el tratamiento de datos de carácter personal sea necesario para el mantenimiento y el cumplimiento del contrato firmado por las partes (Quilez Moreno, 2019).

Por tanto, la prestación del empleado se ejecuta en un entorno físico, la captación de los datos de carácter personal del trabajador deja de constituir un presupuesto indispensable para la ejecución del contrato de trabajo, lo que supone una excepción a la regla general que recoge la normativa en protección de datos (Villalba Sánchez, 2019).

La base jurídica del tratamiento de datos en el trabajo no reside en el consentimiento de los trabajadores[29] debido a la naturaleza de la relación entre empresario y trabajador, basada en la dependencia y la subordinación, que hacen que el consentimiento no pueda calificarse como libre (Preciado Doménech, 2019).

---

27 Que lo define en su apartado 1 de la siguiente manera:"(…) toda manifestación de voluntad libre, específica, informada e inequívoca por la que este acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen".

28 2. Cuando se pretenda fundar el tratamiento de los datos en el consentimiento del afectado para una pluralidad de finalidades será preciso que conste de manera específica e inequívoca que dicho consentimiento se otorga para todas ellas. 3. No podrá supeditarse la ejecución del contrato a que el afectado consienta el tratamiento de los datos personales para finalidades que no guarden relación con el mantenimiento, desarrollo o control de la relación contractual.

29 Art. 6a RGPD.

Una circunstancia importante que debemos tener presente es que en el tratamiento de datos existen una serie de ellos que por su contenido se consideran especiales, son aquellos datos que revelen el origen étnico o racial, ideología política, convicciones sociales, orientación sexual, datos genéticos, datos biométricos, datos relativos a la salud, etc.

Este tipo de datos requieren un tratamiento más cuidadoso por su especial sensibilidad. Por este motivo en la relación laboral se debe justificar su tratamiento por parte del responsable[30] (Ortega Jiménez, 2019).

El criterio de los órganos de la jurisdicción social ha sido restrictivo en materia de obtención del consentimiento para el tratamiento de los datos personales de los trabajadores, cediendo exclusivamente en aquellos aspectos vinculados al ejercicio de la potestad disciplinaria basada en el art. 20.3 ET (Sánchez Quiñonez, 2019).

En términos generales el criterio a seguir por parte de la empresa recomendaría valorar una íntima conexión entre los datos solicitados y el ejercicio de las acciones derivadas del contrato de trabajo, siguiendo un criterio restrictivo y eminentemente actualizado, evitando la solicitud de datos que no guardan relación en el momento actual con el desempeño del trabajo o con las necesidades inmediatas organizativas y/o productivas de la empresa (Sánchez Quiñonez, 2019).

Recordemos la doctrina al respecto de la STC 98/2000, de 10 de abril, la grabación del sonido constituye una intromisión *en la propia esfera de desenvolvimiento del individuo*[31] quizás sirva para interpretar el precepto.

30 En este sentido si la empresa necesita obtener datos especiales de sus trabajadores podrá recabarlos sin necesidad del consentimiento de los trabajadores únicamente cuando: 1) El tratamiento sea necesario para proteger intereses vitales del trabajador. 2) Sea necesario para el cumplimiento de obligaciones del responsable en ámbito del Derecho laboral y de la seguridad social. 3) Para fines de medicina preventiva o laboral, evaluación de la capacidad laboral de trabajador, diagnóstico médico, etc. En el resto de los supuestos se requiere el consentimiento del trabajador.

31 En el caso de las grabaciones del Casino de la Toja, el TC consideró que tal grabación suponía una *intromisión ilegítima en el derecho a la intimidad,* pues la empresa con el sistema de audición y grabación captaba comentarios privados de los clientes y de los trabajadores, que eran ajenos al interés empresarial y por tanto irrelevantes desde la pers-

3.3. Información previa

3.3.1. Panorámica general

El uso de dispositivos digitales facilitados por el empresario a los trabajadores supone la obligación patronal de información previa sobre el uso privado permitidos de los mismos (tiempo y forma de utilización), pudiendo ser legítimo el control de estos a los solos efectos de controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la integridad de dichos dispositivos (Purcalla Bonilla, 2019).

El correo electrónico e Internet y otros recursos tecnológicos que la empresa pone a disposición del trabajador (como son también el ordenador personal, *smartphone*, *tablets,* etc.) cabe caracterizarlos, por un lado, como herramientas de trabajo habituales y básicas de la mayoría de las empresas, que agilizan y mejoran los servicios a sus clientes; por otro lado, como instrumentos de comunicación, y como tales, susceptibles de un uso social.

A menudo, los medios tecnológicos son utilizados por los empleados para buscar o transmitir información con fines particulares, ajenos a los intereses de la empresa. En caso de ausencia de norma expresa, se parte del reconocimiento tácito por parte del empresario del derecho a un uso social de los medios informáticos a favor del trabajador, concibiéndose esta conducta como inocua.

La STS 28 de junio de 2006 fue la primera sentencia del Alto Tribunal que abordó el problema del uso de las herramientas informáticas para fines particulares. Marcó un antes y un después, al hilo de una progresiva evolución del ámbito de la intimidad del trabajador en el marco de las nuevas tecnologías. La referida sentencia, asumió la posición de la Sala de lo Social del TSJ del País Vasco, que partía de un razonamiento según el cual *la falta de prohibición específica* por parte de la empresa respecto a un

pectiva de control de las obligaciones laborales. La actividad que se pretendía controlar por parte de la empresa declaró el TC, se encontraba en lo que ha denominado la *propia esfera de desenvolvimiento del individuo* por lo cual se rebasan las funciones de control en la prestación laboral, que legalmente le concede el ET.

uso privado de las herramientas informáticas equivalía a *autorización*, y la carga de la prueba de la existencia de una prohibición la tenía el empresario.

Este derecho al uso social tolerable de la Red, no obstante, podría ser limitado o casi eliminado mediante una regulación unilateral o bilateral, en su caso. Por lo que mientras que no haya una orden o una regulación empresarial, o no se demuestre que exista, ni existe incumplimiento por el mero uso de las tecnologías, ni el empresario puede acceder sin más a los datos del correo y los archivos temporales de Internet del trabajador, ya que estos quedan protegidos por el derecho a la intimidad, como consecuencia de la doctrina europea.

Es una circunstancia para tener en cuenta la existencia de la generalización de una cierta tolerancia con respecto al uso moderado de los medios de la empresa. El art. 3 del Código Civil[32] afirma que las normas deben interpretarse desde la realidad social del tiempo en que son aplicadas; en este sentido la doctrina viene admitiendo cierta tolerancia social sobre el uso de estas herramientas de trabajo, incluso de manera extralaboral.

Incluso, por las dificultades prácticas de establecer una prohibición absoluta, es recomendable no establecerla; piénsese, por ejemplo, en el acceso a Internet desde el teléfono particular del trabajador, lo que llevaría, al emplear la videovigilancia para verificar el cumplimiento de las órdenes, dada la imposibilidad de fiscalizar el móvil particular.

La doctrina constitucional española, ha reconocido reiteradamente que la garantía del derecho a la intimidad personal y a la protección de datos impone, como regla general un deber de información respecto al trabajador que protege frente a intromisiones ilegítimas del empresario. Este deber es más relevante si cabe en el derecho a la protección de la autodeterminación informativa, al formar parte de su núcleo esencial el derecho del afectado a ser informado de quien posee los datos personales y con qué fin (Cuadros Garrido, 2019).

32 Real Decreto de 24 de julio de 1889 por el que se publica el Código Civil. Gaceta de Madrid núm. 206, de 25 de julio de 1889.

3.3.2. Información previa sobre el uso de dispositivos digitales

La LO 3/2018, reconoce expresamente el derecho de los trabajadores a la protección de su intimidad en el uso de los dispositivos digitales puestos a disposición por la empresa. Restringe el acceso del empleador a sus contenidos a los solos efectos de controlar obligaciones laborales o estatutarias y de garantizar la integridad de los dispositivos. Establece el mandato al empleador de fijar los criterios de uso de los dispositivos con la participación de los representantes de los trabajadores, siendo los trabajadores informados de esos criterios.

Como aspecto positivo, hay que destacar la correcta elección del término dispositivo digital, cuya amplitud hace referencia a que se entienden incluidos en el mismo tanto los dispositivos digitales actuales en uso (ordenadores, teléfonos móviles, tablets, etc.), como los posibles futuros.

Como primer punto crítico, hay que apuntar que no se recogen de manera expresa los derechos fundamentales del art. 18.3 y del 18.4 CE, como derechos de especial protección dado que también potencialmente junto al 18.1 CE pueden resultar vulnerados. Como segunda objeción, se han dejado fuera de regulación los dispositivos propiedad del trabajador que cada vez se llevan más al trabajo son usados con fines laborales, de acuerdo con tendencia anglosajona BYOD[33].

Con respecto al uso de estos dispositivos merece apuntarse la doctrina aplicable que emana de la STEDH de 5 de septiembre de 2017, conocida como *Barbulescu II, en ella* el TEDH reflexiona sobre varios aspectos para resolver sobre si se ha vulnerado o no el art 8 del Convenio de Roma, con las siguientes cuestiones:

33 Siglas de *Bring Your Own Device* (Trae tu propio dispositivo). Con este acrónimo, se describe una nueva tendencia tecnológica en la que la política empresarial permite a los trabajadores utilizar sus propios dispositivos personales para usos profesionales. Asimismo, cuando el empleado además utiliza y comparte aplicaciones y tratamientos poniéndolos a *trabajar* en las funciones de su actividad en la empresa el término se amplia y se habla de BYOT que abarca programas, aplicaciones, plataformas propias o compartidas en el concepto de utilización en común, etc.

– ¿Se ha informado al empleado de la posibilidad de que el empleador tome medidas para controlar su correspondencia y otras comunicaciones, así como de la aplicación de esas medidas? La información debe en principio ser clara en cuanto a la naturaleza de la vigilancia y anterior a su puesta en práctica y en el supuesto enjuiciado no lo ha sido (Cuadros Garrido, 2017).
– ¿Cuál fue el alcance de la vigilancia llevada a cabo por el empleador y el grado de intromisión en la vida privada del trabajador? No se detalla, si el empresario hubiera podido valerse de medios menos intrusivos de fiscalización de la cuenta del trabajador, pues se afirma que existen varios tipos de control, unos muy intrusivos sobre el contenido de las comunicaciones electrónicas y otros menos invasores que analizan el tráfico generado sobre el número de las comunicaciones. No se justifica por qué se opta por la vigilancia más intrusiva y no se explica si al mismo resultado de hubiera podido llegar con otros métodos menos invasivos. No se especifica tampoco durante cuánto tiempo se ha llevado a cabo la vigilancia y cuántas personas han podido acceder al contenido de tales informaciones (Cuadros Garrido, 2019).
– ¿Han existido motivos legítimos, debidamente acreditados por el empleador, para justificar la vigilancia y el acceso a los contenidos de las comunicaciones? Se afirma que no se justifica cuáles son las razones concretas que determinan la fiscalización y monitorización de la cuenta del trabajador, por otro lado tampoco y, en fin, si el acceso al contenido de las comunicaciones hubiera sido posible sin su conocimiento (Cuadros Garrido, 2019).

Se concluye por el TEDH que los tribunales nacionales no verificaron si el trabajador había sido advertido con anterioridad de la vigilancia que iba a llevarse a cabo de sus comunicaciones electrónicas efectuadas desde la cuenta profesional, ni tampoco hasta qué punto se ha producido una intromisión en la vida privada del trabajador en el ámbito de la relación

de trabajo que hubiera podido alcanzarse por vías menos invasivas. Se considera que no se ha protegido de manera adecuada el derecho del trabajador al respeto de su vida privada, y desde ese momento, no han realizado una ponderación justa de los intereses en juego y han vulnerado la normativa en protección datos.

3.3.3. Información previa sobre el uso de dispositivos de videovigilancia permanente

El art. 89.1 LO 3/18 regula sobre videovigilancia permanente respecto a la que se exige información previa expresa, clara e inequívoca. El legislador español considera lícito el uso de la videovigilancia fundamentando el procesamiento de imágenes en el control de la prestación por parte del empresario para verificar su efectivo cumplimiento (art. 20.3 ET), como hasta entonces había venido entendiendo la jurisprudencia.

Si acaso, anotemos que la doctrina aplicable de la STC 29/2013, de 11 febrero[34], caso del empleado de la Universidad de Sevilla marcó el cénit de la protección constitucional, negando la posibilidad de que el empleador utilizara imágenes grabadas por las cámaras de seguridad existentes en sus instalaciones cuando previamente no lo ha advertido. Se afirma que el

34 El Tribunal Constitucional anuló las sanciones impuestas a un subdirector técnico sancionado por una institución universitaria tras ser controlado con cámaras de videovigilancia para conocer si cumplía con su jornada laboral. La Sala consideró lesionado su derecho a la protección de datos. Afirmó que la actuación de la Universidad no podía justificarse por el hecho de que hubiera distintivos para advertir de la instalación de cámaras, sino que era necesario que se informase a los trabajadores de forma previa, precisa y clara de las grabaciones y de su objetivo. En la base de su fundamentación aparece el siguiente relato: *En el caso enjuiciado, las cámaras de videovigilancia instaladas en el recinto universitario reprodujeron la imagen del recurrente y permitieron el control de su jornada de trabajo; captaron, por tanto, su imagen, que constituye un dato de carácter personal, y se emplearon para el seguimiento del cumplimiento de su contrato. De los hechos probados se desprende que la persona jurídica titular del establecimiento donde se encuentran instaladas las videocámaras es la Universidad de Sevilla y que ella fue quien utilizó al fin descrito las grabaciones, siendo la responsable del tratamiento de los datos sin haber informado al trabajador sobre esa utilidad de supervisión laboral asociada a las capturas de su imagen. Vulneró, de esa manera, el art. 18.4 CE* (FJ 8.º).Se establece además que la información a los trabajadores había de ser previa y expresa sobre la finalidad de control de la actividad laboral a la que esa captación podía ser dirigida.

poder de control sobre los propios datos personales nada vale si el afectado desconoce qué datos son los que se poseen por terceros, quiénes los poseen, y con qué fin: por ello se precisa una *información previa y expresa, precisa, clara e inequívoca (...) de la finalidad de control de la actividad laboral a la que esa captación podía ser dirigida*.

La STC 29/2013, de 11 de febrero, constituyó un hito por dos motivos fundamentales; el primero, porque estableció un canon de control de constitucionalidad más rígido que el que la jurisprudencia constitucional venía aplicando respecto al otros derechos fundamentales como el derecho a la intimidad; como segundo motivo, porque rechazó la existencia de norma legal en las relaciones laborales que autorizara restricciones del derecho a la información sobre el tratamiento de datos personales, no considerando hábil a tal fin el art. 20. 3 ET. Desde esta máxima, por tanto, negada la validez constitucional de restricciones al derecho fundamental de los trabajadores *ex* art. 18.4 CE, quedaba en consecuencia impedida la ponderación de la medida empresarial.

3.3.4. Información previa en relación con dispositivos de grabación del sonido

La utilización de sistemas de grabación de sonidos en el lugar de trabajo se admite únicamente cuando resulten relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo y siempre respetando el principio de proporcionalidad, el de intervención mínima y las garantías previstas en los apartados anteriores. La supresión de los sonidos conservados por estos sistemas de grabación se realizará en el plazo máximo de un mes como regla general, en los términos del art. 22.3 LOPD.

La norma no determina qué se entiende por tal riesgo, quizás el legislador podía haber concretado especificando qué determinadas actividades son de riesgo, piénsese en determinadas zonas restringidas de una central nuclear, por ejemplo.

3.3.5. Ausencia de información previa sobre el uso de dispositivos de videovigilancia oculta

El art. 89.1 LO 3/18 regula la videovigilancia encubierta[35] que se permite únicamente en los supuestos de flagrante delito y cuya obligación de información es prácticamente inexistente.

La doctrina aplicable y más reciente al respecto emana de la STEDH de 17 de octubre de 2019[36] conocida como *López Ribalda II,* valida la

35 En el supuesto de que se haya captado la comisión flagrante de un acto ilícito por los trabajadores se entenderá cumplido el deber de informar cuando existiese al menos el cartel informativo conforme a la instrucción núm.1/2006 de la AEPD. Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras. «BOE» núm. 296, de 12 de diciembre de 2006.

36 STEDH de 17 de octubre de 2019 (JUR 2019, 289974). El caso López Ribalda y otras contra el Reino de España, resuelve sobre una pretendida vulneración del art. 8 CEDH por lesionar la prueba videográfica el derecho a la privacidad de las cinco demandantes, antiguas empleadas de MERCADONA, en su día despedidas, por haber cometido diversos hurtos. Los hechos transcurren del siguiente modo: en un supermercado de la cadena antes mencionada, se realizó una auditoría de los últimos meses de facturación que desprendió un importante descuadre contable. Para detectar el origen de las anomalías, se decidió instalar varias cámaras de vigilancia oculta en la línea de caja, para fiscalizar la actividad de los empleados, que junto que a las cámaras permanentes en el área de entrada y de cuya existencia conocían los trabajadores, fiscalizaron la totalidad de la actividad de la plantilla. En el Juzgado de lo Social y en la Sala del TSJ Cataluña se consideraron los despidos como procedentes y la prueba videográfica que no era nula. El TS inadmitió los recursos unificación doctrina e igual respuesta dio el TC a través de auto de inadmisión. Agotada la vía judicial en España, las demandantes acudieron al TEDH, basaron su postulación en una infracción del art. 6 por no haberse garantizado el derecho a un juicio justo y 8 CEDH por vulneración del derecho a la privacidad. Interesante resulta en este caso el voto particular del magistrado Dedov. El citado magistrado considera que con la instalación de las cámaras ocultas no se había producido merma de derecho fundamental alguno y ello habida cuenta de que: 1) las cámaras se encontraban situadas en espacios públicos y no privados por lo que la "expectativa razonable de privacidad" debía ser considerada menor, 2) porque aun cuando los empleados no habían sido informados expresamente de la instalación de las cámaras, el hecho de que algunas de ellas se encontraban explícitamente visibles hacía evidente la instalación de un sistema de seguridad, y 3) porque aunque no existían sospechas concretas contra una persona determinada (como ocurría, por ejemplo, en el caso Kopke vs Alemania) es indudable que dada cuenta del enorme montante de perdidas ocurridas en el establecimiento, resultaba razonable para el empresario considerar que era más de una persona el autor del ilícito lo que, consecuentemente, justificaba la adopción de la medida de seguridad considerada

videovigilancia oculta arbitrada por la empleadora, al considerar que la medida interpuesta por la empresa estaba justificada por la necesidad al haberse producido irregularidades en la actuación profesional de las demandantes. Al efecto, y en función de la doctrina actual de Estrasburgo, son decisivos como factores a tener en cuenta los siguientes:

a) El grado de intromisión del empresario.

b) La concurrencia de legítima razón empresarial justificativa de la monitorización.

c) La inexistencia o existencia de medios menos intrusivos para la consecución del mismo objetivo.

d) El destino dado por la empresa al resultado del control.

e) La previsión de garantías para la persona trabajadora

La cuestión especialmente crucial es la ausencia de información de la existencia de cámaras ocultas el Tribunal europeo incide en que el suministro de información exacta sobre la colocación de las cámaras hubiera frustrado la finalidad de estas. Aunque es cierto que no se cumplieron totalmente las exigencias derivadas del deber de información pues no se notificó la colocación exacta de cada cámara de seguridad, también lo es que se proporcionó una cierta información (existía un distintivo conforme

"indiscriminada" por el Tribunal. Finalmente, el magistrado realiza unas muy relevantes consideraciones sobre la protección que el derecho a la intimidad ha de tener respecto a aquellos que se prevalecen de la misma para la comisión de hechos delictivos.
Una primera STEDH 9 de enero de 2018 *López Ribalda I* (TEDH 2018, 1) estimó lesionado el derecho a la privacidad de las demandantes por incumplimiento de la normativa nacional, puesto el derecho al respeto a la vida privada y familiar, implica un conocimiento previo de la fiscalización de la actividad de las trabajadoras a través de la videovigilancia, y respecto de las cámaras instaladas *ad hoc*, no existía pues no se había facilitado información previa. La segunda sentencia dictada en Gran Sala, estima el recurso del abogado del Estado en nombre de España y considera que no se ha vulnerado el derecho a la privacidad de las demandantes, la medida estaba justificada por un objetivo legítimo que no podía lograrse con otras medidas, dado que se parte de unas sospechas de irregularidades fundadas en unas importantes pérdidas que llevan a la empresa a arbitrar cámaras ocultas en los puestos de caja lugares en los que se insiste que eran de acceso público y a mayor abundamiento, únicamente se grabó durante diez días, en consecuencia, la intrusión muy está limitada en el tiempo.

a la Instrucción núm.1/2006) por lo que la existencia de dicho sistema de seguridad no pasaba desapercibida para los trabajadores.

En base a ello, considera el TEDH que aunque el derecho a la información tiene naturaleza fundamental, dicha exigencia constituye solo un criterio a tener en cuenta más para evaluar la proporcionalidad de la adopción de la medida de control por lo que, en el presente caso, y teniendo en cuenta tanto las circunstancias anteriormente expuestas, así como el incontestable hecho de que se había aportado una información general sobra la existencia de videocámaras de seguridad, no puede entenderse que se haya producido una injerencia ilegitima y desproporcionada en la intimidad de los trabajadores afectados y, consecuentemente, debía considerarse la medida adoptada plenamente válida. De ello cabe deducir que la obligación de información previa no es un requisito sobre el que calibre, únicamente, la determinación de si una prueba puede ser utilizada, o no, en el ámbito de un procedimiento judicial, sino, al contrario, un criterio más a valorar sobre la proporcionalidad de la medida (Zaragoza Tejada, 2020).

3.3.6. Información previa sobre el uso de dispositivos de geolocalización

Se establece un deber de información previo a la fiscalización del GPS, que detalle de manera expresa, clara e inequívoca. Se reconocen los derechos de acceso, rectificación, limitación del tratamiento y supresión. El derecho que resulta más afectado aquí es la autodeterminación informativa (art. 18.4 CE), por su relación instrumental con el derecho a la intimidad este segundo derecho (art. 18.1 CE) también es objeto de protección, pero no de una manera colateral por lo que la redacción del precepto no es del todo afortunada.

4. LA PROTAGONISTA AUSENTE: LA NEGOCIACIÓN COLECTIVA

La regulación por parte de la LO 3/2018 en materia laboral con los arts. 97 a 91, supone un gran avance significativo, pero no ha respondido a las expectativas (. El papel de la negociación colectiva en esta materia

adquiere el rol de protagonista[37], pero las tareas encomendadas por el momento no se están realizando, (Sánchez Trigueros y Cuadros Garrido, 2019, 124-127) el nivel de inclusión en los textos convencionales es del todo escaso (Pérez de los Cobos, 2019).

La ley propone que el contenido de la negociación colectiva se concentre en definir *garantías adicionales* a las que la norma ha previsto en la definición del tratamiento de datos y los derechos digitales en las relaciones de trabajo, recordando implícitamente que no es posible la disponibilidad colectiva de estos derechos fundamentales individuales (Baylos Grau, 2019).

Es casi unánime en la doctrina la crítica al legislador español que ha relegado el papel de la negociación a este ámbito tan reducido de acotar los límites al poder de control y vigilancia empresarial e implementar los derechos digitales de la parte trabajadora con respecto a las TICs (Llorens Espada, 2020). En este sentido se apunta que los márgenes que el precepto europeo reconoce a la legislación y negociaciones colectiva internas son amplísimos, por ello resulta incongruente el parco artículo de la Ley española. Las normas más específicas podrían haber abarcado cualquier secuencia en el tiempo de la relación laboral, desde la contratación hasta la extinción del contrato y desde la perspectiva de contenido, medidas que preserven la dignidad humana, los derechos fundamentales e intereses legítimos de los trabajadores (Pérez de los Cobos, 2019).

La actuación de la negociación colectiva está condicionada por el enfoque que escoge la regulación de estos derechos digitales en la LO[38].

37 El art. 91 LO 3/2018, prescribe que "los convenios colectivos podrán establecer garantías adicionales de los derechos y libertades relacionados con el tratamiento de los datos personales de los trabajadores y la salvaguarda de derechos digitales en el ámbito laboral". Este precepto incluso por algunos autores se considera innecesario ya que pese a su enfática rúbrica recoge una obviedad. Por ello debe de integrarse con en el art. 88 del RGPD que contempla una visión más amplia a desempeñar por la negociación colectiva en este ámbito.

38 El legislador considera los sistemas tecnológicos como instrumentos de vigilancia y control al servicio del poder de dirección del empresario y por consiguiente los ha encajado en la amplísima definición que de esta facultad efectúa el art. 20.3 ET y que se reitera

En este lugar el empleador es el sujeto determinante por lo que se impide que el punto de vista normativo se sitúe en la primacía de los derechos fundamentales del trabajador a su intimidad y a la protección de datos en la valoración del perímetro de licitud dentro del cual se debe contener el poder de control tecnológico del empresario, como debería ser lo correcto. Este será el contexto en el que tiene que actuar la negociación colectiva en los tres aspectos fundamentales: control de las comunicaciones electrónicas del trabajador, vigilancia a distancia por cámaras, grabación de sonidos y dispositivos GPS y derecho de desconexión digital (Baylos Grau, 2019).

El primer interrogante por tanto se refiere a si la negociación colectiva puede cambiar este enfoque prioritariamente asentado sobre una suerte de presunción de intromisión legítima del empleador en la confidencialidad de los datos y en la esfera privada de los trabajadores, e invertir por tanto los actuales criterios derivados de una jurisprudencia permisiva (Baylos Grau, 2019).

Tiene más relevancia, el papel de la negociación colectiva en el desarrollo del derecho de desconexión digital y es, es lo más sugerente de los derechos digitales en el ámbito laboral. Las condiciones de ejercicio de este derecho se enuncian de manera genérica y se trata por tanto de un derecho cuya realización está plenamente condicionada a su desarrollo en convenio colectivo o acuerdo informal de empresa. Aunque se remite el desarrollo de este tema a una *política interna* de empresa que debe simplemente consultarse con los representantes de los trabajadores, es evidente que el convenio colectivo debe abordar *las modalidades de ejercicio del derecho a la desconexión y las acciones de formación y de sensibilización del personal sobre un uso razonable de las herramientas tecnológicas que evite el riesgo de fatiga informática*, y en particular, ha de preservar *el derecho a la desconexión digital en los supuestos de realización total o parcial del trabajo a distancia así como en el domicilio del empleado vinculado al uso con fines laborales de herramientas tecnológicas* (Baylos Grau, 2019).

explícitamente en los casos de videovigilancia y geolocalización.

5. REFLEXIONES FINALES

Primera.- A punto de cumplir dos años la LO 3/2018 cabe observar que la negociación colectiva en esta materia ha sido nula, produciéndose la misma situación que antes de ella, la labor de fiscalización a través de las TICs por parte del empresario es sometida como última ratio al control judicial, otorgándose al magistrado de lo Social un papel cuasilegislativa que no es su función propia.

Segundo.- Respecto al terreno legislativo en materia de TICs y control laboral, cabe vaticinar que siempre va a ser *movedizo*, ante un avance de la realidad tecnológica a pasos de gigante, que ha hecho emerger el derecho a la protección de datos como protagonista autónoma en las relaciones laborales en España desde la STC 29/2013, con tan solo siete años, a lejos de alcanzar la mayoría de edad, podríamos afirmar que sus perfiles son difusos y quedan perfilados por la doctrina europea como observamos con la doctrina López Ribalda, pero no se encuentran limitados, por lo que afirmamos que estamos ante un derecho emergente o en alza.

Tercero.- Cabe proponer una reforma de la Constitución Española que introduzca a los Derechos Digitales en su texto, pues algunos precisan de protección preferente y todos han de ser redefinidos pues la situación es confusa, distinguiendo dentro de ellos dos categorías de derechos algunos que deberían tener protección constitucional como derechos fundamentales (el derecho al olvido y el derecho a la desconexión digital) y otros como ordinarios.

BIBLIOGRAFÍA

Baylos Grau, Antonio: "Los derechos digitales y la negociación colectiva", *Diario La Ley*, núm. 9331, 2019.

Cobacho López, Ángel: "Reflexiones en torno a la última actualización del derecho al olvido digital", *Revista de Derecho Político*, núm. 104, 2019.

Cuadros Garrido, María Elisa:

- La protección de los derechos fundamentales de la persona trabajadora ante la utilización de GPS ¿reformulación o continuidad?" *Lan harremanakRevista de relaciones laborales*, núm. 42, 2019.
- *Trabajadores Tecnológicos y Empresas Digitales*, Aranzadi, 2018.

"La mensajería instantánea y la STEDH de 5 de septiembre de 2017", *Revista Aranzadi Doctrinal*, núm. 11, 2017.

García Murcia, Joaquín y Rodríguez Cardo, Iván: "La protección de datos personales en el ámbito del trabajo: una aproximación desde el nuevo marco normativo", *Revista Española de Derecho del Trabajo*, núm. 216, 2019.

Llorens Espada, Julen: "Los derechos digitales en la negociación colectiva", *Trabajo y Derecho*, núm. 11, 2020.

Sánchez Quiñonez, Luis: "El marco legislativo de la protección de datos en el ámbito laboral. Especial referencia al consentimiento del trabajador", *Diario La Ley,* núm. 9377, 2019.

Sánchez Trigueros Maria Del Carmen y Cuadros Garrido, María Elisa: "Autodeterminación informativa: un derecho en alza", *Revista Galega de Dereito Social*, núm. 8. 2018.

Quilez Moreno, Jose María: La garantía de Derechos Digitales en el ámbito laboral: el nuevo artículo 20 bis del Estatuto de los Trabajadores, *Revista Española de Derecho del Trabajo* núm. 217, 2019.

Ortega Jiménez, Alfonso: Cuestiones prácticas laborales *Revista Española de Derecho del Trabajo*, 216, 2019.

Pérez De Los Cobos Orihuel, Francisco:

- "Poderes del empresario y derechos digitales del trabajador", *Trabajo y Derecho: nueva revista de actualidad y relaciones laborales*, núm. 59. 2019.
- "La interpretación de la Constitución", *Revista Española de Derecho del Trabajo,* núm. 169, 2014.

Preciado Doménech, Carlos Hugo: *Los Derechos Digitales de las Personas Trabajadoras*, Aranzadi, 2019.

Purcalla Bonilla, Miguel Ángel: "Control tecnológico de la prestación laboral y derecho a la desconexión de los empleados: Notas a propósito de la Ley 3/2018, de 5 de diciembre", *Revista Española de Derecho del Trabajo* núm. 218, 2019.

Rodríguez Escanciano, Susana: *El derecho a la protección de los datos personales de los trabajadores: nuevas perspectivas,* Ed. Bomarzo, 2009.

Sierra Hernáiz, Elisa: "Protección de datos y derechos de maternidad en el ámbito laboral", *Revista Española de Derecho del Trabajo,* núm. 228, 2020.

Sempere Navarro, Antonio Vicente y San Martin Mazzucconi, Carolina: *Las TIC's en el ámbito laboral*, Dykynson, 2015.

Sempere Navarro, Antonio Vicente: "Un apunte sobre la grabación mediante cámaras al hilo de la STS-VI 600/2019 de 7 de noviembre)", *Revista Aranzadi Doctrinal*, núm. 2, 2020.

Villalba Sánchez, Ana: "El principio de transparencia en la ejecución automatizada del contrato de trabajo: una aproximación jurídica a la tecnología "blockchain" y a la inteligencia artificial", *Revista Española de Derecho del Trabajo,* núm. 224, 2019.

Zaragoza Tejada, Javier Ignacio: "La prueba obtenida por videocámaras de seguridad tras la STEDH del 17 de octubre del 2019. Caso López Ribalda vs España" *Revista Aranzadi Doctrinal,* núm. 2, 2020.