Facultad de Derecho
Universidad de La Laguna

TRABAJO FIN DE GRADO
Grado en Derecho

Facultad de Derecho

Universidad de La Laguna

Curso 2021/2022

Convocatoria: Julio

EL DERECHO A LA PROTECCIÓN DE DATOS EN EL ÁMBITO LABORAL

THE RIGHT TO DATA PROTECTION IN THE FIELD OF LABOUR LAW

Realizado por la alumna Dª María Martínez Asensio

Tutorizado por el Profesora Dra. Dª Mónica Molina García

Departamento: Derecho Público y Privado Especial y Derecho de la Empresa

Área de conocimiento: Derecho del Trabajo y de la Seguridad Social

ABSTRACT

The right to data protection guarantees a power of disposal and control over the data subject's personal data, as well as over its use and destination with the aim of preventing its unlawful trafficking and/or aim of preventing it being harmful to his or her dignity and rights. Data protection in relation to personnel management raises several questions, even more so with the rise of technology, which has exponentially increased the range of possibilities for processing by the employer.

The aim of this work is to learn about the legal regime of the workers' right to data protection. To do so, I will analyse the different precepts that regulate it, the principles that govern it, the rights that workers have to make their informational self-determination effective and the obligations of the data controller. Finally, I will analyse the criteria followed by case law to determine the legitimacy of the use of video-surveillance cameras to monitor workers.

Keywords: data protection, worker, employer, control, video surveillance.

RESUMEN

El derecho a la protección de datos garantiza un poder de disposición y control sobre los datos personales del interesado, así como sobre su uso y destino con el objetivo de impedir su tráfico ilícito y/o lesivo para su dignidad y derechos. La protección de datos en lo relativo a la gestión del personal plantea diversos interrogantes, más aún con él auge de la tecnología que ha incrementado exponencialmente el abanico de posibilidades de tratamiento por parte del empleador a lo que hay que añadir las potenciales formas de control del trabajador.

Lo que pretendo con este trabajo es conocer el régimen jurídico del derecho a la protección de datos de los trabajadores, para ello analizaré los distintos preceptos que lo regulan con el objetivo de conocer cuáles son los principios que lo inspiran y que derechos tienen los trabajadores para hacer efectiva la autodeterminación informativa además de las obligaciones que tiene el responsable de tratamiento. Por último, analizaré el criterio que sigue la jurisprudencia para determinar la legitimad sobre el uso de cámaras de videovigilancia para controlar a los trabajadores.

Palabras clave: protección de datos, trabajador, empleador, control, videovigilancia.

ÍNDICE

1. EL DERECHO A LA PROTECCIÓN DE LOS DATOS COMO DERECHO FUNDAMENTAL Y AUTÓNOMO Y SUS PRINCIPIOS INSPIRADORES

El derecho a la protección de datos se regula en el artículo 18.4 CE «*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*». La primera norma que desarrolló el derecho a la protección de datos fue la Ley Orgánica 5/1992, de 29 de Octubre, de Regulación del Tratamiento Automatizado de Datos de Carácter Personal. El derecho a la protección de datos es un derecho joven y moderno que fue incorporado a nuestro catálogo de derechos fundamentales a través de la STC 292/2000. Esta Sentencia del TC define al derecho fundamental a la protección de datos como "un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso". (FJ. 7 STC 292/2000)

La STC (Sala Primera) de 20 de julio de1993 (réc. núm. 254/1993), STC (Sala Primera) de 9 de mayo de 1994 (réc. núm.143/1994), STC (Sala Primera) de 13 de enero de 1998 (réc. núm. 11/1998), STC (Sala Segunda) de 4 de mayo de 1998 (réc. núm. 94/1998) y STC (Sala Primera) de 8 de noviembre de 1999 (réc. núm. 202/1999) mencionan a la *«libertad informática»* como un instituto de garantía, con el propósito de dar "respuesta a una forma de amenaza concreta a la dignidad y a los derechos de la persona" (STC 254/1993, FJ. 6), como es el *tratamiento mecanizado de datos*, pues los riesgos que estas operaciones conllevan se han incrementado significativamente debido a las múltiples posibilidades que ofrecen las Tecnologías de la Comunicación y la Información para recoger y tratar datos.

La STC 292/2000, de 30 de noviembre del 2000[1] declaró al derecho a la protección de datos como derecho fundamental y autónomo. El hecho de que ostente la condición de derecho fundamental lo hace invocable por vía de amparo o tutela preferente y sumaria ex artículo.53.2 CE, sin necesidad de relacionarlo con otro derecho fundamental.

Esta sentencia permitió desligar al derecho a la protección de datos ex artículo 18.4 CE del derecho a la intimidad ex artículo 18.1 CE. Lo cierto es que ambos derechos "comparten el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar"[2]. Pero poseen distintas funciones, la función del derecho a la intimidad es garantizar el libre desarrollo de la vida privada individual de cada uno, protegiendo aquellos ámbitos personales y familiares que se desean excluir del conocimiento ajeno o de cualquier intromisión indeseada por algún tercero. En cambio, el derecho a la protección de datos otorga al individuo un poder de disposición y control sobre sus datos personales con el objetivo de impedir su tráfico lesivo e ilícito para la dignidad y el derecho del interesado.

Además, el derecho a la protección de datos atribuye al titular unos poderes jurídicos -indispensables para hacer efectivo el derecho a la protección de datos- que permiten imponer a terceros deberes jurídicos, como son: el derecho a un tratamiento licito, el derecho a saber y ser informado sobre el destino y uso de los datos y al conjunto de derechos que permiten acceder, rectificar y cancelar dichos datos.[3]

[1] Para saber más sobre ella. Comentario de la STC 292/2000. Disponible en https://www.madrid.org/usupadron/legislacion/protdatos/protecciondatos.pdf (fecha de última consulta: 9 de junio de 2022)

[2] Disponible en https://archivos.juridicas.uma.mx/www/bjv/libros/12/5669/23.pdf (fecha de última consulta: 9 de junio 2022)

[3] *Ibidem.*

En definitiva, "los trabajadores deben encontrarse informados del tratamiento de sus datos y no pueden ver menoscabado su derecho a la privacidad por el mero hecho de ocupar un puesto de trabajo y desarrollar una relación laboral".[4]

Los principios que regulan la protección de datos "albergan la propia concreción del contenido esencial del derecho a la protección de datos personales",[5] pues "constituyen una verdadera pauta normativa e interpretativa de todas las instituciones que componen la normativa de protección de datos",[6] cuyo propósito no es otro que "informar e integrar la aplicación de todo el conjunto normativo".[7]

En definitiva, tratan de cubrir las lagunas legales que la regulación de la protección de datos pueda presentar y de adecuar la normativa de la protección de dados a las relaciones de trabajo y empleo. Es evidente que el juego de los principios de protección de datos entraña en el ámbito laboral una limitación al poder de ordenación y control del que es titular el empresario.[8]

Principio de lealtad. Este principio se encuentra recogido en el artículo 8.2 CDFUE y el articulo 5.1.a) RGPD, en él se garantiza que los datos tengan un tratamiento legal mediante el obligado respeto de los requisitos, derechos y garantías que establece la normativa de protección de datos.

[4] FERRER SERRANO, R.L: *Guía de protección de datos de los trabajadores*. Ed. Tirant lo Blanch, 2019, pág. 19.

[5] BAZ RODRIGUEZ, J.*: Privacidad y protección de datos de los trabajadores en el entorno laboral,* Ed. Bosch, Madrid, 2019, pág. 98.

[6] *Ibidem.*

[7] *Ibidem.*

[8] FERRER SERRANO, R.L: *op. cit.*, pág. 32-36. MERCADER UGUINA, J.*: Protección de datos y garantía de los derechos digitales en las relaciones laborales*, Ed. Lefebvre, *2019*, pág. 32-37. BAZ RODRIGUEZ, J.: *op. cit.*, pág. 97-106.

El profesor MERCADER define a la lealtad como "la vara de medir la relación entre el interesado y responsable de los datos y se traduce en la transparencia y la confianza en el tratamiento de los datos que el segundo le adeuda al primero".[9]

Principio de transparencia. Este principio supone "un refuerzo transcendental del deber de información que recae sobre el empresario cuando lleve a cabo las operaciones de tratamiento de datos de los trabajadores"[10]. En el mismo sentido BAZ RODRIGUEZ, "El principio de transparencia, desde esta perspectiva, no sería sino un refuerzo de las exigencias de licitud y lealtad, añadiendo elementos de buena fe y confianza en la regularidad del tratamiento"[11].

A lo que se refiere por tanto este principio es a la manera en que han de cumplirse las obligaciones de informar al trabajador sobre los elementos del tratamiento de sus datos personales. Para hacer efectivo este principio es necesario que la identificación del responsable, los fines del tratamiento, los derechos que le asisten y la forma de ejercerlos, además de los riesgos derivados del tratamiento, todos estos extremos deben ser formulados y emitidos "en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo". [12]

En consecuencia, la información que los trabajadores deben conocer acerca del tratamiento de sus datos personales está minuciosamente detallada desde el punto de vista material como temporal en los artículos 13 y 14 RGPD. En cambio, la norma comunitaria no determina cual son los medios a través de los cuales se debe canalizar la información.

[9] MERCADER UGUINA, J.: *op. cit.*, pág. 32.

[10] BAZ RODRIGUEZ, J.*: op. cit.*, pág. 98.

[11] BAZ RODRIGUEZ, J.: *op. cit.*, pág. 102.

[12] MERCADER UGUINA, J.*: op. cit,*. pág. 32.

En este caso lo recomendable es optar por procedimientos o medios de información que permitan constatar que el trabajador ha sido correctamente informado de todos los términos mencionados anteriormente. Es habitual añadir al contrato laboral una cláusula-tipo o entregar un formulario al trabajador que contenga toda la información necesaria en relación a la normativa de protección de datos. Esta última forma otorga mayor garantía al trabajador, que incluir una cláusula-tipo, porque el trabajador en un documento separado va a poder comprender mucho mejor el alcance de los derechos de los que es titular a causa del tratamiento de sus datos personales en la relación laboral y va a poder ejercer un verdadero poder de control sobre sus datos personales.

Frente a la normativa rigurosa marcada por el RGPD, la normativa interna ha optado por un sistema denominado *«información por capas»* ex articulo 11 LOPD, sistema que resulta polémico porque el RGPD no prevé la posibilidad de clasificar la información en distintos niveles y por esta razón parece más que objetable la interpretación que la normativa interna ha hecho del RGPD.

Mediante este sistema al interesado se le suministra únicamente la información básica junto con un correo electrónico u otro medio que le permita acceder a la información restante de forma sencilla e inmediata. Este sistema según BAZ RODRIGUEZ, "suscita dudas fundadas sobre su corrección y aptitud para cumplir el deber de información en los términos previstos reglamentariamente, al menos en el ámbito de la relación laboral". [13]

El principal interrogante de este mecanismo es la denominada *«información básica»* que supone una *devaluación* del deber de transparencia informativa, porque la información se reduce a la identidad del responsable, la finalidad de tratamiento y la posibilidad de ejercer sus derechos.

[13] BAZ RODRIGUEZ, J.*: op. cit.*, pág. 105.

En el entorno laboral a la hora de cumplir eficazmente con el principio de transparencia debe garantizarse que el trabajador recibe una información completa antes de suscribir el contrato de trabajo. Esto quiere decir que la información básica debe de proporcionarse con carácter previo a la firma del contrato para que el trabajador pueda acceder a la información adicional con el propósito de que llegado el día de la fecha de la firma del contrato el trabajador disponga de la información completa.

En definitiva, mediante este mecanismo de información por capas no podemos garantizar que el deber de información se cumpla en el inicio de una relación laboral si no se establece un procedimiento de información que evidencie que el trabajador es conocedor de todos los extremos que señala la norma.

Principio de limitación de la finalidad. Este principio como su propio nombre indica dispone que los datos personales deben ser recogidos con "fines determinados, explícitos y legítimos". Es decir que la finalidad del tratamiento tiene que estar perfectamente determinada antes del inicio del tratamiento "sin poderse confundir con cualquier interés del empresario"[14].

Principio de minimización de datos. Este principio significa que los datos han de ser adecuados, pertinentes y limitados en relación con el fin que legitima el tratamiento. El en ámbito laboral el tratamiento de datos de los trabajadores debe estar limitado "a lo necesario para satisfacer las finalidades empresariales del tratamiento en cuestión"[15].

Principio de exactitud. En virtud de este principio los datos tienen que ser exactos y deben estar actualizados de manera que reflejen fielmente la situación real del interesado, ex artículo 5.1.d) RGPD y 4 LOPD.

[14] MERCADER UGUINA, J.*: op. cit.*, pág. 32.

[15] BAZ RODRIGUEZ, J.*: op. cit.*, pág. 99.

Se deben adoptar todas las medidas razonables para que los trabajadores puedan acceder e incidir sobre el tratamiento de sus datos (Considerando Nº139 RGPD), especialmente para que puedan rectificar o complementar sin dilación los datos personales que no sean exactos en relación con el fin del tratamiento.

Por tanto, este principio de minimización de datos "requerirá que se asegure la capacidad del trabajador de obtener, a partir de su requerimiento, en intervalos razonables y sin excesiva demora, la confirmación del tratamiento de datos relativos a su persona, siempre de un modo respetuoso con el principio de transparencia"[16]. Con este propósito se articularán procedimientos que permitan al responsable realizar una actualización continua de los datos, de forma que sea exactos y se ajusten a la realidad del trabajador.

Principio de limitación del plazo de conservación. Este principio establece un límite temporal al tratamiento de los datos personales, pues estos deben ser mantenidos el tiempo estrictamente necesario para el fin del tratamiento. Para ello será necesario aplicar medidas técnicas y organizativas adecuadas.

Este principio presenta interrogantes cuando el tratamiento de los datos se plantea en un contexto laboral porque a la hora de fijar un plazo de conservación nos vamos a encontrar con la divergencia entre los plazos que cubren las responsabilidades derivadas del tratamiento de los datos y, por otro lado, los plazos vinculados a la prescripción de acciones derivadas de los negocios jurídicos. A esta problemática se le suma la diversidad de datos personales pueden ser tratados por la empresa que originan una pluralidad de regímenes en cuanto a plazos de conservación.

No hay una solución concreta pero sí que existe una regla general. Una vez finalice el contrato laboral nace el derecho del trabajador a la supresión de los datos personales que le conciernen ex articulo 17 RGPD.

[16] BAZ RODRIGUEZ, J.*: op. cit.*, pág. 100.

Aunque los plazos de prescripción de las acciones que se derivan del contrato laboral pueden justificar que el plazo se extienda más allá de la extinción del contrato laboral.

Principio de integridad y confidencialidad. Los datos personales deben ser tratados de forma que se garantice una seguridad adecuada incluyendo la protección contra el tratamiento no autorizado o ilegal. Estos principios constituyen una garantía de seguridad para los datos personales. Se regulan en el artículo 5.1.f) RGPD y artículo 5 LOPD. Para cumplir con los parámetros de seguridad que marcan estos principios se deberán adoptar los medios tecnológicos necesarios y las medidas técnicas y organizativas apropiadas para evitar cualquier perdida, destrucción o daño accidental.

2. RÉGIMEN JURIDICO

2.1. EL DERECHO EUROPEO

El derecho a la protección de datos es "un derecho emergente, pero ya central en nuestro tiempo".[17] Se encuentra recogido en el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea, en este sentido "conviene poner de relieve el cambio sustancial en la función socio-política de la privacidad que la Carta Comunitaria vino a consagrar, sobrepasando ampliamente la esfera privada, para conformarse como elemento constitutivo de la ciudadanía digital".[18]

[17] FERNÁNDEZ DE MARCOS, E.D.: *Él Reglamento Europeo de Protección de Datos y la LOPDGDD: Todo lo que necesitas saber,* Ed. La Ley, 2020, pág. 89.

[18] BAZ RODRIGUEZ, J.: *Los nuevos derechos digitales laborales de las personas trabajadoras en España: vigilancia tecnificada, teletrabajo, inteligencia artificial, Big Data.* Ed. CISS, Madrid, 2021, pág. 24.

La Organización Internacional del Trabajo se hizo eco de la causa muy tempranamente, pues en 1997 elaboró una serie de recomendaciones prácticas para la protección de los datos personales de los trabajadores.[19]

En materia de protección de datos han sido muy utilices determinados instrumentos comunitarios que han colaborado eficazmente en la aplicación efectiva del derecho a la protección de datos en el ámbito laboral. Es interesante mencionar la Recomendación del Comité de ministros del Consejo de Europa sobre el tratamiento de datos personales en el contexto de empleo, de 1 de abril de 2015, en ella se aborda con ánimo de garante diversos aspectos que afectan al tratamiento de los datos de los trabajadores y también a los candidatos a los puestos de trabajo.

Por otro lado, también es importante nombrar al Grupo de Trabajo del Artículo 29 (The Articule 29 Working Party) que fue creado por la Directiva 95/46/CE como órgano consultivo independiente que se encarga de estudiar toda cuestión relativa a la aplicación de las disposiciones nacionales en materia de protección de datos, así como emitir dictámenes, documentos y formular recomendaciones sobre cualquier asunto relacionado con la protección de datos en la Unión Europea. [20]

En relación al ámbito laboral es necesario destacar el *Dictamen 8/2001 sobre el tratamiento de datos personales en el contexto laboral*; *Documento de trabajo relativo a las comunicaciones electrónicas en el lugar de trabajo de 2002* y *el Dictamen 2/2017 sobre el tratamiento de los datos en el trabajo*, en él se realiza una revaluación del

[19] Disponible en http://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/normativeinstrument/wcms_112625.pdf (fecha de última consulta: 12 de junio de 2022)

[20] GARCÍA COCA, Olga, 2016, *La protección de datos de carácter personal en la gestión de los recursos humanos de la empresa* (en línea). Tesis doctoral. Sevilla: Universidad Pablo de Olavide, pag. 22-30. (fecha de última consulta: 12 de Junio de 2022). Disponible en: https://rio.upo.es/xmlui/bitstream/handle/10433/3054/garcia-coca-tesis16.pdf?sequence=1&isAllowed=y

equilibrio entre los intereses legítimos de los empresarios y las expectativas razonables de privacidad de los trabajadores, describiendo los riesgos que plantean las nuevas tecnologías y evaluando la proporcionalidad de una serie de escenarios en los que podrían aplicarse.

La evaluación que hace el Dictamen 2/2017 de las diversas cuestiones que afectan al tratamiento de datos de los trabajadores se realiza principalmente en relación con la Directiva 95/46/CE todavía en ese momento vigente, pero también tuvo en cuenta las obligaciones con arreglo al Reglamento 2016/679. El GT 29 dejo de operar el 29 de Mayo de 2018 al mismo tiempo que el RGPD entraba en vigor.

La Directiva 95/46/CE, de 24 de octubre, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, únicamente hace referencia a la protección de datos en el ámbito laboral en el artículo 8.2.b), pues el articulo 8.1 prohíbe el tratamiento de datos sensibles -como puede ser, origen étnico, sexualidad, etc.- y dentro de las excepciones que se recogen en el artículo 8.2, una de ellas es el apartado b), determina la excepción a la regla general de prohibición en el ámbito laboral.

El derecho a la autodeterminación informativa presenta peculiaridades en el contexto de una relación laboral que desborda a la regulación genérica de la protección de datos contenida en la Directiva 95/46/CE, pues la aplicación del régimen general suscita incógnitas en muchos aspectos, pues es difícil cohonestar el régimen jurídico de la protección de datos con la mecánica de la relación laboral, pues "el intérprete se ve obligado a ir desgranando los derechos y obligaciones de la ley y adecuarlos al marco de un contrato de trabajo o una relación de empleo". [21]

[21] ALAMEDA CASTILLO, M.T.: "Él necesario replanteamiento del marco comunitario de los datos personales de los trabajadores": *Los mercados laborales y las políticas sociales en Europa XX Congreso Nacional de Derecho del trabajo y de la seguridad Social*, Ed. Ministerio de Trabajo e Inmigración, Madrid, 2009, pág. 293.

La Comisión Europea de Empleo y Asuntos Sociales es consciente de que durante los últimos años se ha producido un importante progreso tecnológico y globalización que revelan la necesidad de realizar una reflexión sobre una protección idónea de los datos personales de los trabajadores que partiendo del marco general se tuvieran en cuenta las especificaciones propias de la relación laboral pero lamentablemente hasta el momento no se ha reunido el consenso suficiente para redactar una normativa laboral en materia de protección de datos.

Actualmente, está vigente el Reglamento UE/2016/679, 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 (en adelante, RGPD), con él la UE "apuesta por su potencial para convertirse en líder mundial, al menos, de la inteligencia artificial, precisamente por contar con un marco reglamentario sólido basado en los derechos humanos y fundamentales".[22] No todo son opiniones buenas en torno al RGPD, pues el Letrado REQUEJO, considera que "el RGPD ofrece una imagen muy distinta, hasta el punto de aparecer antes como un problema constitucional que como un instrumento al servicio del constitucionalismo".[23]

Dicho esto, El RGPD ha intentado abordar la problemática de la materia solventando las principales carencias que anterior normativa acarreaba, como son: La *idea de un derecho de protección de datos trasversal.* El objetivo pretendido es que el derecho al tratamiento de datos deje de ser considerado meramente un requisito burocrático y que por el contrario se integre y esté presente en todas las decisiones relacionadas con el tratamiento.[24]

[22] BAZ RODRIGUEZ, J.*: op. cit*., pág. 24.

[23] REQUEJO PAGÉS, J.L.: "La protección de datos, en la encrucijada entre el derecho de la Unión y la Constitución Española", en AA.VV (CASAS BAAMONDE, M.E., Coord.): *El derecho a la protección de datos personales en la sociedad digital*, ed., Monografías fra, 2020, pág. 27.

[24] FERNÁNDEZ VILLAZÓN, L.A.: *Derecho y las nuevas tecnologías.* Ed. Aranzadi, Pamplona, 2020, pág. 207.

Por otro lado, *conseguir una progresiva conciencia sobre este derecho.* La normativa comunitaria ha establecido como contenido esencial del derecho a la protección de datos la exigencia de que la información que se proporcione a las personas titulares de los datos objeto del tratamiento ha de ser transmitida "en forma concisa, transparente, inteligible, y de fácil acceso, con un lenguaje claro y sencillo"[25].

Lo que se pretende es hacer más accesible y comprensible la información para el ciudadano medio, pues si el trabajador no comprende el alcance o el margen de actuación que le otorga su derecho a la protección de datos difícilmente podrá hacer efectivo el derecho a la autodeterminación informativa. [26]

En lo que respecta al ámbito laboral es la primera vez que un precepto proclama la plena aplicación de la normativa de protección de datos en el ámbito de las relaciones de trabajo. Él articulo 88 RGPD y Considerando Nº155 son los puntos de referencia que tomaran los Estados Miembros para elaborar sus normativas nacionales en materia de protección de datos en relación al ámbito laboral. [27]

El articulo 88.1 ofrece la posibilidad de regular normas más específicas con el fin de garantizar la protección de los derechos y libertades en relación con el tratamiento de datos personales de los trabajadores. Esta tarea se podrá llevar a cabo por disposiciones legislativas o mediante convenios colectivos. Así mismo el legislador menciona con carácter abierto una serie de situaciones es los que sería conveniente establecer una regulación más específica: 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

[25] *Ibidem.*

[26] *Ibidem.*

[27] FERRER SERRANO, R.L: *op. cit.*, pág. 22-24

o clientes; El ejercicio y disfrute, individual o colectivo, de los derechos y prestaciones relacionados con el empleo y a efectos de la extinción de la relación laboral.

La razón por la que el legislador no establece un marco común en materia laboral se debe a "la profunda diversidad institucional en materia laboral en las diversas experiencias nacionales, junto a la propia inviolabilidad político-legislativa de otras alternativas, operaron quizá como factores decisivos en la postura abstencionista del legislador eurocomunitario, que optó por efectuar una vaga e incorrecta alusión a una serie de materias". [28]

El articulo 88.2 en cambio se redacta en términos impositivos, porque de darse una regulación más específica, esta tiene que obligatoriamente preservar la dignidad humana, intereses legítimos y sus derechos fundamentales. "Lo que parece exigir cuanto menos, una reflexión ponderada del estado miembro sobre si esa protección en el ámbito laboral requiere de medidas específicas".[29]

El artículo 88.3 establece la obligación de notificar cualquier disposición legal que se adopte en relación a la materia por cualquier estado miembro, con el objeto de comprobar si cumple con los parámetros marcados por el marco común europeo.

El organismo con competencias en materia de protección de datos que se responsabiliza de la aplicación del RGPD es el Comité Europeo de Protección de Datos, en adelante CEPD, es un organismo europeo independiente que contribuye a la aplicación coherente de las normas de protección de datos en toda la Unión Europea y promueve la cooperación entre las autoridades de protección de datos de la UE."

[28] BAZ RODRIGUEZ, J.*: op. cit.*, pág. 23.

[29] *FERNÁNDEZ VILLAZÓN, L.A.: op, cit., pág. 208.*

2.2. EL DERECHO ESPAÑOL

El legislador español formaliza el mandato del RGPD y dicta la Ley Orgánica 3/2018 de 6 de diciembre de 2018, en adelante, LOPD. No cabe duda de que contar con estos dos cuerpos normativos va a permitir "una aplicación efectiva de las normas"[30] y "ayudará a fomentar la sensibilidad social"[31] que es unos de los principales problemas que presenta esta materia. Sin embargo, si analizamos el contenido de los preceptos, realmente estamos ante un "avance tímido, limitado y no exento de problemas interpretativos". [32]

Pues el contenido laboral en LOPD, se encuentra dentro del Título X, «Garantías Digitales» que comprende desde el articulo 87 al 91. EL hecho de que el legislador no haya dedicado un apartado concreto al «Tratamiento de datos en el ámbito laboral» cómo era deseable, hace presumir que la regulación del derecho a la protección de datos en el ámbito del trabajo no atenderá como podríamos esperar los retos y transformaciones que plantea la nueva realidad digital.

La LOPD no contiene un régimen de garantías adicionales a las previstas en el RGPD, si no que se ha encargado de regular algunas de las cuestiones problemáticas más comunes de conflicto entre el poder de dirección del trabajador y los derechos fundamentales de los trabajadores, pero sin "efectuar una ponderación completa acerca de las medidas específicas de protección de datos que el desarrollo del derecho a la libertad informática exige en todas las fases de la relación laboral"[33]. No contamos con

[30] *Idém. pág. 209.*

[31] *Ibidem.*

[32] *Ibidem.*

[33] FERNÁNDEZ VILLAZÓN, L.A.*: op. cit.*, pág. 210.

una regulación sistematizada, sino todo lo contrario, estamos ante una regulación dispersa en la que ocasiones es difícil encontrarle lógica.[34]

Así, se regula, i) Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral (artículo 87); ii) Derecho a la desconexión digital en el ámbito laboral (artículo 89); iii) Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo (artículo 89); iv) Derecho a la intimidad ante la utilización de sistemas de geolocalización (artículo 90); v) Derechos digitales en la negociación colectiva (artículo 91).

Por otra parte, la LOPD modificó el Estatuto de los Trabajadores y añadió al texto normativo el nuevo artículo 20 bis, «El derecho de los trabajadores a la intimidad en relación con el entorno digital y a la desconexión» en el ET. Es curioso que a través de la LOPD se haya introducido el articulo 20.bis en el ET y en el artículo no se haga mención expresa al derecho a la protección de datos y solamente mencione el derecho a la intimidad.

De esta forma el precepto está tratando al derecho a la protección de datos como un derecho instrumental de garantía de otros derechos, en especial del derecho a la intimidad. Es cierto que esta interpretación también se desprende del articulo18.4 CE, pero ha sido la jurisprudencia la que por medio de la STC 292/2000 concluyó que el derecho a la protección de datos es un derecho fundamental autónomo y diferenciado, con su propio contenido y lógica interna.

Aunque podríamos haber esperado una redacción más acertada con este nuevo artículo ponemos fin al silencio que ha mantenido el ET sobre el derecho a la protección de datos. Asimismo, se podría haber aprovechado esta modificación del ET para añadir el derecho a la protección de datos como derecho básico de los trabajadores consagrados en el artículo 4 ET.

[34] PRECIADO DOMÈNECH, C.H.: *op. cit.*, pág. 239-241.

El legislador español en vez de aprovechar la oportunidad que la UE le otorga para establecer garantías más específicas y quien sabe si posicionarse como un país referente en la materia, lo único que ha regulado son algunos problemas que se plantean con la libertad informática en relación con el poder de dirección y control del empresario.

Además, esos problemas ya se encontraban recogidos en resoluciones de los Tribunales y "la jurisprudencia presento dificultades a la hora de asimilar el funcionamiento del derecho a la protección de datos, en consecuencia, al incorporar a la ley las soluciones adoptadas por los tribunales, se han incorporado de nuevo esas dificultades de asimilación."[35]

La Agencia Española de Protección de Datos, en adelante, AEPD, es la autoridad administrativa independiente que tiene la misión de velar por el cumplimiento de la legislación de protección de datos, controlar su aplicación a fin de garantizar el derecho a la protección de datos personales de los ciudadanos y promover y sensibilizar sobre la comprensión de riesgos, normas y garantías en relación con el tratamiento de datos.

Los documentos que emite pertenecen al terreno del *soft law*[36], pero esto no le resta valor alguno, pues son muchas las instrucciones, circulares e informes jurídicos que ha emitido la AEPD en relación a cuestiones laborales, además ha elaborado la Guía de Protección de Datos en las Relaciones Laborales.[37] Además la AEPD es la autoridad de control con potestad sancionadora por tanto es el órgano encargado de iniciar las investigaciones e imponer las sanciones a los infractores en forma de resoluciones.

[35] FERNÁNDEZ VILLAZÓN, L.A.*: op. cit.,* pág.212.

[36] *El* termino *soft law* o derecho blanco hace referencia a los actos jurídicos que sin tener fuerza vinculante obligatoria contienen las pautas inspiradoras de una futura regulación de una materia, abriendo paso a un posterior proceso de formación normativa.

[37] Disponible en https://www.aepd.es/es/documento/la-proteccion-de-datos-en-las-relaciones-laborales.pdf (Fecha de última consulta: 12 de junio de 2022)

2.3. ELEMENTOS DETERMINANTES EN LA APLICACIÓN DEL RÉGIMEN JURÍDICO DE LA PROTECCIÓN DE DATOS: «PERSONAS FÍSICAS», «DATO PERSONAL», «DATOS SENSIBLES»

La protección que otorga el Reglamento solo debe aplicarse a las *«personas físicas»*, independientemente de su nacionalidad o de su residencia, en relación con sus datos personales. Por tanto, excluye del ámbito de aplicación a las personas jurídicas y en especial, a empresas constituidas como personas jurídicas. (Considerando N. º14, RGPD)

Por tanto, el RGPD despliega su eficacia en relación con los datos personales de una persona física identificada o identificable, definida como *"Toda persona cuya identidad pueda determinarse, directa o indirectamente"*. Así lo determina el articulo 1 y 4.1) RGPD y artículo 5.a) LOPD.

El profesor PRECIADO DOMÈNECH[38], determina dos criterios para configurar el *«análisis de la identificabilidad»:* El *criterio de razonabilidad*. Este criterio se refiere a la disponibilidad de los medios, es decir, que se pueda identificar a la persona física haciendo uso de unos medios razonables, teniendo en cuenta la tecnología disponible en el momento del tratamiento, así como los avances tecnológicos (Considerando Nº26, RGPD). El *criterio de proporcionalidad*. Este criterio se refiere al esfuerzo que le pueda suponer al responsable de tratamiento u otra persona distinta identificar a la persona física, si supone un esfuerzo desproporcionado identificar a la persona física no se aplicará el RGPD a esos datos.

[38] PRECIADO DOMÈNECH, C.H.: *El derecho a la protección de datos en el contrato de trabajo*, Ed Aranzadi, Pamplona, 2017, pág. 236-237.

El concepto de *«dato personal»* engloba a cualquier información relativa a una persona física identificada o identificable. El RGPD protege a los datos personales, como puede ser un nombre, número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de una persona física. [39]

El ámbito de aplicación del RGPD se extiende también a los datos anónimos, pero con una particularidad: Los datos anonimizados, cifrados o presentados con un seudónimo[40], que puedan utilizarse para identificar a una persona - mediante cualquier medio o junto con información adicional-, se consideran datos personales y se inscriben en el ámbito de aplicación del RGPD. En cambio, se excluyen del ámbito de protección los datos anónimos *«per se»* y los datos anonimizados que no permitan identificar a una persona de forma irreversible. [41]

Dentro de los datos personales, es necesario mencionar la categoría especial de *«datos sensibles»*, como son: ideología, afiliación sindical, convicción religiosa, orientación sexual, creencias, datos relacionados con la salud. Estos datos se consideran especiales y por ello, gozan de una especial y mayor protección.

El articulo 9.1 RGPD establece como regla general que el tratamiento de datos sensibles está prohibido. Lo que motiva esta prohibición es que el tratamiento de datos sensibles conlleva importantes riesgos para los derechos y libertades fundamentales, riesgos que en el contexto del ámbito laboral alcanzan una mayor intensidad.

[39] FERRER SERRANO, R.L: *op. cit.*, pág. 32-36

[40] El artículo 4.5) RGPD define a la *«seudonimización»* como el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física, identificada o identificable.

[41] En este sentido, PRECIADO DOMÈNECH, C.H.: *op. cit.*, pág. 237-239.

Conviene destacar la STS 4686/2015, de 12 de noviembre, en la que el Tribunal Supremo determina que el consentimiento no podrá legitimar el tratamiento de datos con el propósito de elaborar una "lista negra" de personas trabajadoras conflictivas o sindicalizadas.

La prohibición general admite excepciones, pero únicamente las contempladas en el artículo 9.2 RGPD. Entre ellas la prevista en el artículo 9.2.b), legitima las operaciones de datos sensibles cuando *"El tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable de tratamiento o del interesado en el ámbito del Derecho laboral y la seguridad y protección social (...)"*. En concreto, el empresario tiene que ser conocedor de la condición de discapacidad del empleado para poder beneficiarse de la bonificación de la cuota de la Seguridad Social por contratar a una persona con discapacidad física o sensorial.

3. EL TRATAMIENTO DE LOS DATOS EN EL ÁMBITO LABORAL

El nuevo modelo normativo de protección de datos establece como principio rector que cualquier tratamiento de datos tiene que tener una base jurídica que lo legitime. El artículo 6 RGPD expone seis bases jurídicas sin preferencia ni jerarquía entre ellas.[42]

El consentimiento. El primer presupuesto de licitud del tratamiento de datos que la norma menciona es el consentimiento, definido por el articulo 4.11 RGPD como "*toda manifestación de voluntad libre, especifica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen*" entendido por tanto como una manifestación especial del poder de disposición de los datos. [43]

[42] PRECIADO DOMÈNECH, C.H.: *op. cit.*, pág. 253-256. BAZ RODRIGUEZ, J.: *op. cit.*, pág. 107-113.

[43] GONZÁLEZ BIEDMA, E.: "Derecho a la información y consentimiento del trabajador en materia de protección de datos" *Revista Temas Laborales* núm.138, 2017. pág. 228-233.

El responsable de tratamiento debe considerar cual es la base jurídica adecuada como fundamento jurídico del tratamiento previsto, generalmente el consentimiento es una base jurídica que se usa con frecuencia, pero con la condición de que otorgue a los interesados una capacidad real de elección sin padecer perjuicio alguno. Esta condición entraña un obstáculo para que esta base jurídica opere con normalidad en el campo laboral debido a la naturaleza de la relación entre empleado y empleador marcada por una fuerte dependencia y desequilibrio de poder. [44]

En este sentido el CEPD, en las *Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679* entiende que en la mayoría de casos donde vayan a realizarse operaciones de tratamiento de datos personales de futuros o actuales empleados es conveniente utilizar otra base jurídica. Esto no significa que no se pueda utilizar el consentimiento como base jurídica en las relaciones de trabajo, pero si finalmente se optase por ella es necesario probar que "el hecho de que otorguen o no dicho consentimiento no tenga consecuencias adversas".

La STS 4086/2015, Sala de lo Social vino a declarar como abusivas y contrarias al derecho a la protección de datos las cláusulas-tipo que se incluían en el contrato por las que el trabajador se comprometía a facilitar su número de teléfono y/o su correo, electrónico y a comunicar la modificación de aquellos si sufrían cambio alguno. La doctrina determinó que esos datos no eran necesarios para el mantenimiento o cumplimiento de una relación laboral, pudiendo el trabajador ponerlos a disposición de la empresa mediante el consentimiento, pero no podían incluirse como una cláusula del contrato. El TS dio respaldo al marco normativo del momento sobre la protección de datos y pretendió que se excluyera "toda posibilidad de que la debilidad contractual del trabajador pueda viciar su consentimiento".[45]

---

[44] CAPEÁNS AMENEDO, C.: *op. cit.,* pág. 18-21.

[45] BAZ RODRIGUEZ, J.: *op. cit.,* pág. 109.

La suscripción o ejecución de un contrato de trabajo. Cuando el tratamiento sea "*necesario para la ejecución del contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales*" (artículo 6.1.b RGPD). En la relación de trabajo no es necesario otorgar el consentimiento para el tratamiento de los datos personales, siempre que los datos que se vayan a tratar sean los estrictamente necesario para la ejecución de la relación laboral, el consentimiento se entiende de algún modo implícito en la relación negocial. (STC 39/2016, FJ3)

Cumplimiento de una obligación legal. Cuando el tratamiento sea *"necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento"* (artículo 6.1.c RGPD). Es relevante esta base jurídica en las relaciones laborales porque el plano normativo laboral prevé múltiples supuestos en los que el empresario tendrá que obtener determinados datos personales para el cumplimiento de una obligación estipulada en la ley.

En esta ocasión la ley actúa como base legitimadora del tratamiento "en atención a intereses de las partes, como por la propia configuración del empresario como una suerte de gestor delegado de los poderes públicos".[46] En concreto el pago delegado de la Seguridad Social o el pago delegado de prestaciones de la Seguridad Social por el responsable de tratamiento.

Para la satisfacción de intereses legítimos. El tratamiento es *"necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero siempre que no prevalezcan sobre esos intereses los derechos o libertades fundamentales del interesado que son tutelados por el derecho a la protección de datos"*. Se encuentra regulado en el artículo 6.1.f) RGPD y considerando N.º 47 RGPD.

Esta base jurídica tiene un carácter muy abierto por esa razón no es suficiente invocar un interés legítimo para legitimar un tratamiento de datos personales sin contar con el consentimiento del interesado. Es indispensable realizar un juicio de ponderación entre

[46] BAZ RODRIGUEZ, J.: *op. cit.,* pág. 110.

el interés legítimo de quien va a tratar los datos y los derechos fundamentales del trabajador, con el propósito de precisar cuál debe predominar atendiendo al caso concreto. “Estamos, ante dos conceptos jurídicos indeterminados que generan un escenario incierto en una pluralidad inagotable de supuestos y circunstancias presentes y futuros”.[47]

Para el GT29, el *interés legítimo* como base de legitimación, puede servir para ofrecer “espacios adicionales de tratamiento de los datos personales “, “al estimarse más laxa o menos perfilada o acotada técnicamente que las restantes”, pero no significa que favorezca usos apropiados y abusivos debido a su condición polivalente. Para que esto no suceda nuestra regulación ha fijado una serie de supuestos en los que el interés legítimo se puede invocar como base de legitimación, como la monitorización de la actividad laboral.

El tratamiento de los datos personales de los trabajadores, cuando se justifique en un interés legítimo solamente se podrá hacer uso de los mecanismos y técnicas que sean estrictamente necesario para satisfacer el fin en proporción a las necesidades y objetivos de la empresa. El empresario deberá adoptar medidas dirigidas a paliar las consecuencias que el tratamiento pueda ocasionar sobre los derechos fundamentales y libertades de los trabajadores, garantizando un equilibrio optimo entre ambos.

Si dicho equilibrio no se cumple el trabajador podrá ejercer el derecho de oposición ex articulo 21 RGPD. En concreto el empresario bajo el cumplimiento de un interés legítimo puede acceder a las conclusiones de los reconocimientos médicos en materia de Prevención de Riesgos Laborales (articulo 22 LPRL).

[47] BAZ RODRIGUEZ, J.: *op. cit.,* pág. 111.

4. LOS DERECHOS DE LA PERSONA TRABAJADORA Y LA RESPONSABILIDAD EN EL USO DE LOS DATOS

El RGPD tiene como principal misión fortalecer el control efectivo sobre sus datos personales y como resultado de ello se ha superado el esquema clásico de facultades formado por los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición) pues a partir de la entrada en vigor del RGPD se puede hablar hasta de ocho derechos sobre los que se construye el nuevo esquema protector: 1) Transparencia; 2) Información; 3) Acceso; 4) Rectificación; 5) Supresión; 6) Limitación del Tratamiento; 7) Portabilidad de los datos y 8) Oposición. Se encuentran regulados en la sucesión de artículos 12-22 RGPD y 12-18 LOPD. [48]

El ***derecho de acceso***. Este derecho es regulado por el artículo 15 RGPD y artículo 13 LOPD. "Es un derecho central en materia de protección de datos"[49], "centralidad que deriva de su condición de pre-requisito para el ejercicio del resto de los derechos y facultades y el propio control de la regularidad de las actuaciones". [50]

En efecto este derecho reconoce a los interesados la facultad de solicitar al responsable de tratamiento la confirmación sobre si se están tratando o no sus datos personales y en caso de que la respuesta sea afirmativa, este derecho también incluye la facultad de solicitar información sobre la finalidad del tratamiento, categorías de datos, destinatarios, derechos del interesado, su origen -si no se se han obtenido del propio interesado- y la existencia de decisiones automatizadas.

[48] MERCADER UGUINA, J.: *op. cit.*, pág. 59-67. CAPEÁNS AMENEDO, C.: *Derecho del Trabajo y nuevas tecnologías.* Ed. Colex, 2020, pág. 34. BLAZQUEZ AGUDO, E.M.: *Aplicación práctica de la protección de datos en las relaciones laborales: efectos derivados del Reglamento Europeo de Protección de Datos,* E.d Wolter Kluwer, 2018, pág. 110-115. BAZ RODRIGUEZ, J.: *op. cit.*, pág. 119-129.

[49] BLAZQUEZ AGUDO, E.M.*: op. cit.*, pág. 110.

[50] BAZ RODRIGUEZ, J.: *op. cit.*, pág. 120.

Es un derecho estrechamente vinculado con el deber de información regulado en el artículo 15 RGPD, que solamente se accede a él cuando no se le ha comunicado previamente la información sobre el tratamiento de sus datos.

El ***derecho de rectificación*** es regulado en el artículo 16 RGPD y artículo 14 LOPD. Este derecho reconoce al interesado el derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos cuando los datos sean inexactos y completarlos cuando los datos sean incompletos. No obstante, este derecho también supone para el trabajador un deber, en el caso de la información sea necesaria para el desarrollo de la actividad laboral el trabajador deberá colaborar en la modificación de la información.

El ***derecho de oposición*** se encuentra regulado en el articulo 21 y 22 RGPD y articulo 18 LOPD. Este derecho otorga una facultad al interesado de oponerse en cualquier momento al tratamiento de los datos personales por motivos relacionados con su situación particular sobre dos bases de legitimación concretas: la necesidad de satisfacer un interés público o un interés legítimo del responsable de tratamiento o de un tercero. El trabajador carecerá de esta facultad cuando el tratamiento de sus datos esté basado en el propio contrato de trabajo.

Desde el momento que el trabajador ejercite el derecho de oposición el responsable del tratamiento debe paralizar automáticamente el tratamiento de los datos hasta que se acrediten “los motivos legítimos imperiosos” para que el tratamiento prevalezca sobre los derechos, libertades e intereses del interesado o para la formulación, ejercicio o defensa de reclamaciones.

El ***derecho a la limitación del tratamiento*** se encuentra regulado en el articulo 18 RGPD y articulo 16 LOPD. La persona trabajadora tendrá derecho a obtener del responsable de tratamiento la limitación del tratamiento de los datos cuando el interesado impugne la exactitud de los datos mientras se verifica la inexactitud; cuando se entienda que el tratamiento es ilícito y el interesado opte por la limitación mientras se verifica la ilicitud del tratamiento a efectos de sanciones; cuando sea el responsable

quien no necesita tratar los datos personales y sí que lo necesite el interesado para la formulación, ejercicio o defensa de reclamaciones; cuando el interesado se oponga al tratamiento y sea necesario la verificación de que prevalecen los motivos legítimos del responsable.

El ***derecho de supresión*** se encuentra regulado en el articulo 17 RGPD y articulo 15 LOPD. Este derecho se denominaba derecho de cancelación, con el nuevo título se pretende establecer de forma clara la diferencia que estriba entre el derecho a la rectificación (la modificación en el supuesto de inexactitud) y la supresión (anulación).

La persona trabajadora tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan cuando los datos personales ya no sean necesarios para los fines que fueron recogidos, los datos hayan sido tratados de forma inadecuada o cuando el trabajador retire su consentimiento en el que se basa el tratamiento.

Al margen de estas eventualidades, difícilmente los trabajadores podrán ejercer este derecho en el tratamiento que la empresa hace de sus datos para el regular desarrollo de la actividad laboral excepto cuando se dé por finalizada la relación laboral, el trabajador, en este caso, podrá ejercer este derecho porque se entiende que la finalidad que ampara el tratamiento se ha extinguido. Aunque una empresa diligente en materia de protección de datos debería suprimir los datos del trabajador en el instante en el que se diera por finalizada la relación laboral.

El RGPD determina una serie de excepciones que el empresario podrá oponer al trabajador en el ejercicio del derecho a la supresión. En primer lugar, cuando el tratamiento sea preciso para el cumplimiento de una obligación legal, pensemos en los trabajos que requieren de una manipulación constante de productos tóxicos, en este caso el empresario deberá llevar a cabo una vigilancia de la salud de sus trabajadores en virtud del artículo 22 de la Ley de Prevención de Riesgos Laborales. En segundo lugar, cuando existan razones de interés público en el ámbito de la salud pública, en este caso no hay nada más actual como la pandemia del Covid-19. Por último, cuando el

tratamiento de los datos sea necesario para el ejercicio o la defensa de reclamaciones, en este sentido, cuando un trabajador ha sido captado por las cámaras robando y esa grabación sirve como prueba en un proceso judicial.

El ***derecho a la portabilidad*** se encuentra regulado en el artículo 20 RGPD y artículo 17 LOPD. Este derecho "viene a configurar un nuevo derecho para el interesado por el que se quiere tanto reforzar el control sobre sus propios datos, como también al tiempo crear una herramienta de defensa de la competencia en el mercado digital"[51].

Es un derecho relacionado con el derecho de acceso, pues en situaciones de cambio del responsable de tratamiento como complemento al derecho de acceso, el interesado tiene derecho a recibir sus datos personales que hayan sido tratados, en un formado estructurado, de uso común y de lectura mecánica e interoperable.

El trabajador podrá ejercer este derecho respecto de los datos que se hayan facilitado al empleador de manera consciente en el momento que tuvo lugar la celebración del contrato, pero no se limita solamente a estos datos, sino que este derecho también abarca los datos que son resultado de la supervisión laboral y la observación de la persona trabajadora y de su trayecto en la empresa.

En relación a la finalización del contrato, el extrabajador podrá solicitar a la empresa los datos relativos a su rendimiento laboral previo o las diversas condiciones personales o profesionales que el empleador tuvo en cuenta para decantarse por él. También cabe la posibilidad de que este derecho de portabilidad pueda ser ejercitado por los demandantes de empleo en relación con los portales de empleo, agencias de colocación, empresas de trabajo temporal o cualquier agente análogo. [52]

Las obligaciones del responsable del tratamiento se han intensificado desde la entrada en vigor del RGPD. Ahora se le exige al responsable una responsabilidad proactiva,

[51] BLAZQUEZ AGUDO, E.M.: *op. cit.*, pág. 127.

[52] Para saber más en este sentido, *Directrices sobre el derecho a la portabilidad de los datos* elaborados en 2016 y revisados en 2017 por el GT 29.

"tiene que estar continuamente valorando y proponiendo actuaciones a los efectos del cumplimiento de las reglas de protección de los datos personales"[53],

El principio de responsabilidad activa es contemplado doblemente en el RGPD. Por un lado, el artículo 5.2 "*El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo*" y por el artículo 24.1 que dispone "*El responsable de tratamiento aplicará las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme al presente Reglamento*".

Además, este principio se recoge en el artículo 4.2 de la Recomendación del Comité de Ministros a los Estados Miembros sobre el tratamiento de datos de carácter personal en el marco del empleo. También en la versión actualizada de 2013 de las Directrices sobre la privacidad adoptadas por la Organización de Cooperación y Desarrollo Económicos.

De esta forma el responsable de tratamiento desecha su faceta pasiva para convertirse en un sujeto activo que debe hacer un seguimiento permanente de los distintos aspectos del tratamiento teniendo en cuenta los nuevos avances tecnológicos que pueden entrañar un alto riesgo para los derechos y libertades de los trabajadores. [54]

El responsable del tratamiento debe adoptar las medidas técnicas y organizativas necesarias para garantizar y demostrar que las operaciones de tratamiento son adecuadas y licitas. Tiene que examinar la naturaleza, el ámbito y contexto del tratamiento de los datos personales y determinar la finalidad del tratamiento, teniendo en cuenta que en cualquier momento la autoridad de control le puede solicitar la verificación del cumplimiento de la normativa aplicable.

Además, tiene que prever los potenciales riesgos para los derechos y libertades fundamentales con el propósito de poder evitarlos. El profesor MERCADER entiende

[53] BLAZQUEZ AGUDO, E.M.: *op. cit.*, pág. 80.

[54] *Ibidem.*

que "la accountabiliy debe materializarse en el reconocimiento, asunción de responsabilidad y actitud transparente sobre los impactos de las políticas, decisiones, acciones, productos y desempleo asociados a una organización."[55]

En definitiva "el responsable debe mantener una actitud consciente, diligente y proactiva por parte de las organizaciones frente a todos los tratamientos de datos personales que lleve a cabo".[56] Por ello "es importante una concienciación de la importancia del principio de responsabilidad proactiva y el respecto de la privacidad y el tratamiento ético y seguro de los datos de sus trabajadores.[57]

De forma que las obligaciones que asume el responsable del tratamiento de datos para cumplir con su responsabilidad proactiva son:

Obligación de protección desde el diseño. Es conveniente que el responsable de tratamiento diseñe una política de tratamiento de los datos que se adapte a las finalidades perseguidas en cada caso desde el inicio del tratamiento, esto permite que se traten los datos estrictamente necesarios de acuerdo a la finalidad para la que han sido recogidos.

Obligación de disponer de un sistema de gestión preventiva de los riesgos del tratamiento de los datos (Articulo 25 y 35 RGPD y articulo 28 LOPD). Desde que entró en vigor el RGPD es obligatorio la realización de análisis de riesgos con el objetivo de establecer medidas de seguridad que permitan valorar los riesgos de forma continua y prever los efectos que tienen los avances tecnológicos en las operaciones de

[55] MERCADER UGUINA, J.: *op. cit.*, pág. 37.

[56] Disponible en https://www.aepd.es/es/preguntas-frecuentes/2-rgpd/3-principios-relativos-al-tratamiento/FAQ-0208-que-es-el-prinipio-de-responsabilidad-proactiva (Fecha de última consulta: 12 de Junio de 2022)

[57] SIMÓN CASTELLANO, P.: *Las funciones del delegado de protección de datos en los distintos sectores de la actividad.* Ed. Bosch, Madrid, 2020, pág. 172.

tratamiento[58] antes de que estos se produzcan con el objetivo de adoptar medidas que garanticen la protección de los datos personales.[59]

Una vez realizado el análisis de riesgos nos encontramos ante dos escenarios: Si tras realizar el análisis de riesgos se concluye que las actividades de tratamiento no conllevan riesgos relevantes no será necesario realizar la Evaluación de Impacto, en adelante EIPD. En este caso sería adecuado registrar la realización del análisis previo y argumentar porque el tratamiento de estos datos presenta una baja exposición al riesgo.

Si tras realizar el análisis de riesgos se concluye que el tratamiento pueda suponer un alto riesgo para los derechos y libertades de las personas titular de los datos habrá que realizar obligatoriamente una EIPD (articulo 35 RGPD y 28.f) LOPD).[60] En este caso se procederá a analizar la necesidad y proporcionalidad del tratamiento; se realizará un análisis sobre las amenazas que puedan derivar en riesgos para los titulares de los datos en caso de materializarse estas y finalmente habrá que trazar un plan de acción con las medidas de salvaguarda necesarias para eliminar o minimizar los riesgos.[61]

El artículo 73.t) LOPD tipifica como infracción grave la no realización de la oportuna EIDP en los casos en los que era exigible. No hay excusa para no conocer que casos exigen la realización de la EIPD porque la AEPD publicó una lista en la que enumeraba los tratamientos en los que sí es obligatorio llevar a cabo una EIPD.[62]

El tratamiento de los distintos datos personales de los trabajadores tiene cabida en algunos supuestos que enumera la lista elaborada por la AEPD, como el tratamiento que

[58] BLAZQUEZ AGUDO, E.M.*: op. cit.*, pág. 80.

[59] CAPEÁNS AMENEDO, C.: *op. cit.*, pág. 24.

[60] CAPEÁNS AMENEDO, C.: *op. cit.*, pág. 25.

[61] SIMÓN CASTELLANO, P.: *op. cit.*, pág. 163.

[62] Disponible en https://www.aepd.es/sites/default/files/2019-09/listas-dpia-es-35-4.pdf (fecha de última consulta 7 de junio de 2022)

implique toma de decisiones automatizadas, tratamientos que supongan geolocalización, tratamiento que impliquen la utilización de nuevas tecnologías, etc.

El sujeto responsable *está obligado al registro de actividades de tratamiento de datos personales*, en adelante, RAT. La Directiva 95/46/CE apostó por establecer una obligación general de notificar el tratamiento de datos personales, pero supuso una carga administrativa y además no consiguió una mejora en la protección de los datos personales.

Por esa razón el nuevo Reglamento optó por implementar procedimientos y mecanismos eficaces que se centran en las operaciones de tratamientos que implican un riesgo para los derechos y libertades de los individuos. (Considerando N.º 89 RGPD). El RGPD sustituyó la obligación de inscribir ficheros por la de llevar un registro de actividades de tratamiento que deberá contener la información que detalla el articulo 30 RGPD y 31 LOPD.

El RAT "constituye la piedra angular o núcleo central del cumplimiento normativa en materia de datos personales"[63] porque "constituye la expresión más tangible de responsabilidad proactiva"[64]. Es un instrumento imprescindible para organizar y controlar aquellas actividades que desarrolla la empresa en las cuales debe tratar datos y los trabajadores están involucrados.

Además "es un documento de gestión vivo",[65] esto quiere decir que la información debe ser actualizada constantemente por el responsable o encargado del tratamiento. Además, es imprescindible que contengan todos los extremos contenidos en el artículo 30 RGPD, de lo contrario la empresa incurrirá en una infracción leve.

[63] SIMÓN CASTELLANO, P.: *op. cit.*, pág. 156.

[64] *Ibidem.*

[65] *Ibidem.*

Asimismo, el necesario que el RAT este bien estructurado y actualizado, pero en este sentido es cierto que el precepto no establece una forma concreta en la que debe estructurarse el registro. La AEPD propone un modelo en el que se agrupen a todas las actividades de tratamiento que compartan la misma finalidad, legitimación o colectivo de afectados. El hecho de no disponer del registro de actividades o no ponerlo a disposición de la autoridad de control que lo solicite constituirá una infracción grave (articulo 73 LOPD). [66]

El deber de seguridad informática: El responsable de tratamiento debe elaborar un catálogo de medidas de seguridad que deberá aplicar según la naturaleza de datos personales que trate[67] con el fin de evitar violaciones o brechas de seguridad. (articulo 32 RGPD). Los instrumentos que articulan este deber se denominan "protocolos de seguridad".

El trabajador también debe cumplir con este deber pues es considerado "un sujeto coadyuvante necesario, con obligaciones de diligencia al respecto ex articulo 5 ET, para el cumplimiento de aquel deber de seguridad a cargo del responsable de tratamiento". [68]

El deber de bloquear los datos personales sometidos a demanda de rectificación o de supresión (Articulo 32 LOPD). Cuando cualquier trabajador ejercita su derecho de rectificación o supresión el responsable de tratamiento debe identificar y bloquear dichos datos mediante medidas técnico-organizativas que imposibiliten su tratamiento.[69] En el caso de que el bloqueo suponga un esfuerzo desproporcionado o un coste desmedido al responsable, el articulo 32.4 y 5 LOPD habilitan un modo alternativo, pues se procederá a "un copiado seguro de la información de modo que conste

[66] CAPEÁNS AMENEDO, C.: *op. cit.*, pág. 22-24.

[67] BLAZQUEZ AGUDO, E.M.: *op. cit.*, pág. 80.

[68] MOLINA NAVARRETE, C.: *Datos y derechos digitales de las personas trabajadoras en tiempos de (pos) covid19*, Ed. Bomarzo, Albacete, 2021, pág. 45.

[69]MOLINA NAVARRETE, C.: *op. cit.*, pág. 41-46.

evidencia digital, o de otra naturaleza, que permita acreditar la autenticidad de la misma, la fecha del bloqueo y la no manipulación de los datos durante el mismo". [70]

Es importante la figura del Delegado de Protección de Datos, en adelante, DLP, por la estrecha vinculación y la destacable labor de auxilio que presta al responsable del tratamiento en el cumplimiento de sus obligaciones y además porque el DLP "constituye un genuino defensor de la ciudadanía de los datos".[71] Se encuentra regulado en los artículos 37-39 RGPD y artículos 33 y ss. LOPD.

El DLP puede formar parte de la plantilla o ser un profesional ajeno con el que contraigamos un contrato mercantil de servicios (articulo 37.5 RGPD). Una de las características más importantes de esta nueva figura es la *independencia*, porque no puede recibir ninguna instrucción ni ser destituido ni sancionado en el desempeño de sus funciones (articulo 36.2 LOPD). Por otro lado, es la *confidencialidad*, pues debido al cargo que desempeña y por tanto su activa participación en las operaciones de tratamiento debe guardar la debida confidencialidad con respecto a la información que tenga acceso.

5. EL PAPEL DE LA NEGOCIACIÓN COLECTIVA

El legislador comunitario como nuestra LOPD son conscientes de las particularidades que supone el ejercicio del derecho a la protección de datos en el marco de las relaciones laborales por ello ambos cuerpos normativos, de distinta forma y con diferente intensidad, habilitan a los interlocutores sociales para que puedan desarrollar normas más específicas para garantizar la protección de los derechos y libertades fundamentales de los trabajadores respecto de sus datos personales. [72] Esta oportunidad

[70] MOLINA NAVARRETE, C.: *op. cit.*, pág. 46.

[71] MOLINA NAVARRETE, C.: *op. cit.*, pág. 48.

[72] SERRANO GARCÍA, J.M.: *La protección de datos y la regulación de las tecnológicas en la negociación colectiva y en la jurisprudencia*, Ed. Bomarzo, Albacete, 2019, pág. 17-22.

que se brinda a los interlocutores sociales se denomina *«principio de autonomía colectiva»*, aunque la calificación como principio no es la más adecuada, ya que no es un principio en sí mismo porque no opera en todos los espacios en los que el derecho a la protección de datos está presente.

El RGPD en su Considerando N.º 155, reconoce el derecho de los convenios colectivos para establecer "normas específicas relativas al tratamiento de datos personales de los trabajadores en el ámbito laboral". El articulo 88 RGPD habilita a los agentes sociales para que participen en la adopción de medidas adecuadas y especificas con el propósito de preservar la dignidad humana de las personas trabajadoras así como sus intereses legitimas y derechos fundamentales.[73] El artículo 9.2.b) habilita a los convenios para que fijen excepciones a la prohibición del tratamiento de categorías sensibles de datos los trabajadores para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del derecho del trabajo y de la seguridad social adoptando las garantías que sean necesarias para garantizar el respeto de los derechos fundamentales e intereses del trabajador.

La LOPD hace un llamamiento más intenso que el previsto en la normativa comunitaria para que los representantes de los trabajadores participen en algunos aspectos relacionados con la tecnología y la protección de datos.

El articulo 87 LOPD permite al empresario acceder a los dispositivos digitales puestos a disposición de los trabajadores para controlar las obligaciones de sus trabajadores y garantizar la integridad de los dispositivos, pero se han de elaborar unos criterios de utilización de los dispositivos digitales. El apartado tercero del artículo 87, establece que los representantes de los trabajadores tienen que obligatoriamente participar en la elaboración de los criterios de utilización.

Los artículos 89 y 90 LOPD legitiman el uso de sistemas de videovigilancia y geolocalización para controlar el cumplimiento de la relación laboral con la condición

[73] SERRANO GARCÍA, J.M.: *op. cit.*, pág. 18.

de informar a los representantes de los trabajadores con carácter previo y de forma expresa, clara y concisa, acerca de la finalidad, alcance y características del medio de control que se va a instalar. Este deber de información previa a los representantes de los trabajadores supone una garantía adicional en las medidas de control empresarial. [74]

El articulo 91 LOPD representa sin duda al principio de autonomía colectiva porque hace una invitación universal a todos los representantes de los trabajadores para que a través de normas sectoriales establezcan garantías adicionales para los trabajadores en materia de protección de datos y no solo se limite la participación de la negociación colectiva a los derechos digitales.

Pues son múltiples los ámbitos de la relación laboral en los que se va a realizar operaciones de tratamiento de los datos personales por esta razón, "el ámbito de actuación de la negociación colectiva para establecer garantías adicionales será todo lo amplio que sea necesario para asegurar el correcto ejercicio de las obligaciones empresariales si existe la posibilidad de que exista afectación o posibles riesgos para cualquier derecho fundamental por el tratamiento de los datos personales de los trabajadores".[75]

La profesora SIERRA fija varias áreas de actuación en la que son prioritarias la participación de la negociación colectiva.[76] En primer lugar, es primordial otorgar garantías adicionales en el tratamiento de datos especialmente sensibles para los trabajadores y que no están incluidos en el artículo 9.1 RGPD, como son la edad, el sexo, "con la finalidad de evitar situaciones potenciales de discriminación"[77], pues el objetivo es "tratar de proteger el dato personal en sí mismo ya que su tratamiento puede

[74] SERRANO GARCÍA, J.M.: *op. cit.*, pág. 19.

[75] SIERRA HERNAIZ, E.: "El papel de la negociación colectiva en el tratamiento de los datos personales de los trabajadores" *Revista Temas Laborales*, núm. 152, 2020, pág. 129.

[76] SIERRA HERNAIZ, E.: *op. cit.*, pág. 129-136.

[77] SIERRA HERNAIZ, E.: *op. cit.*, pág. 132.

dar lugar a discriminaciones ocultas"[78]. En el mismo sentido, es necesario reforzar las garantías para las operaciones de tratamiento de datos que si están incluidos en el artículo 9.1 RGPD, como son los datos de salud, igualmente para evitar cualquier sesgo discriminatorio.

En segundo lugar, es necesario adoptar garantías adicionales con la finalidad de afianzar la protección de los derechos digitales frente a facultades de control del empresario y el ejercicio de los derechos reconocidos. Una opción es crear Comisiones *ad hoc* con el único propósito de proteger y salvaguardar los derechos digitales, que deberán determinar los criterios de utilización de los dispositivos digitales, la formación y medidas que se deben adoptar para sensibilizar a los trabajadores en relación a sus derechos digitales. [79]

6. UNA PERSPECTIVA JURISPRUDENCIAL: EL CONTROL DEL TRABAJADOR A TRAVÉS DE CÁMARAS DE VIDEOVIGILANCIA

El articulo 89 LOPD bajo la rúbrica "Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo", legitima el control de la actividad laboral con fundamento en él artículo 20.3 ET por medio de dispositivos de videovigilancia en el lugar de trabajo siempre que se respete la legalidad vigente y sus límites (STC 38/2016 FJ. 4).[80]

Es importante que los limites estén bien definidos porque "los avances tecnológicos han dado lugar a mecanismos de control realmente invasivos, porque a través de ellos se puede obtener información que excede de la mera comprobación del cumplimiento de las obligaciones laborales, de la ejecución de la prestación del trabajo, alcanzando a la

[78] *Ibidem.*

[79] *Ibidem.*

[80] La AEPD entiende que la grabación de imágenes de los trabajadores conlleva el tratamiento de datos personales. Resol. R/00035/2016, de 27 de febrero.

esfera personal del individuo, esto es, a circunstancias que deberían encontrarse al margen del poder de dirección"[81]. En definitiva "la tecnología permite un control, cada más exhaustivo, invasivo y barato en beneficio de la empresa"[82] y en detrimento del trabajador.

El uso frecuente de sistemas de videovigilancia en los centros de trabajo es mucho anterior a la entrada en vigor de la LOPD. El legislador español ha hecho una reproducción literal de la doctrina contenida en las sentencias del Tribunal Constitucional sobre el uso de sistemas de videovigilancia para controlar a los trabajadores. [83]

En articulo 89.1 LOPD establece por primera vez la obligación de informar previamente a los trabajadores y a sus representantes de la puesta en marcha de los sistemas de control de la imagen. En realidad, esto ya lo sabíamos, porque forma parte del contenido esencial del derecho a la protección de datos, pero significa un avance en nuestro ordenamiento.

Sin embargo, el segundo inciso del primer apartado exime el deber de información a los trabajadores de los sistemas de videovigilancia cuando se haya captado la comisión flagrante de un acto ilícito por parte de un trabajador. La redacción es confusa porque el legislador está legitimando el control oculto por parte del empleador en dos ámbitos: en primer lugar, en el lugar de trabajo hay un sistema de videovigilancia pero su función es la seguridad del lugar, ante las sospechas sobre las posibles irregularidades de uno o varios trabajadores el empleador decide utilizar el sistema de videovigilancia instalado para una finalidad distinta. En segundo lugar, el empleador tiene indicios de que se

[81] RODRIGUEZ ESCANCIANO, S.: *Poder de Control Empresarial, Sistemas Tecnológicos y Derechos Fundamentales de los Trabajadores.* Ed. Tirant Lo Blanch, 2015, pág. 33.

[82] TODOLI SIGNES, A.*: Digitalización, Recuperación y Reformas Laborales*, Ed. Ministerio de Trabajo y Economía Social, Madrid, 2022, pág. 226.

[83] BLAZQUEZ AGUDO, E.M.: *op. cit.*, pág. 44-48.

están cometiendo irregularidades por parte de uno o varios trabajadores y en el establecimiento no exista un sistema de videovigilancia y decide instalar un sistema de videovigilancia para controlar a los trabajadores.

Por último, el artículo 89.2 establece la prohibición de instalar cualquier tipo de sistema de grabación en cualquier lugar destinado al descanso o esparcimiento de los trabajadores, como pueden ser aseos, vestuarios o cualquier entorno análogo. Esta restricción es muy importante porque, aunque se tuvieran sospechas de que algún trabajador estuviera cometiendo un acto ilícito, no se podría implantar ningún sistema en las zonas de descanso del personal. Este precepto no supone ninguna novedad porque la prohibición de las grabaciones en los lugares destinados al descanso se afirmó en la STC 198/2000.

Jurisprudencia del Tribunal Constitucional. En 2000 el TC dictó sus primeras sentencias sobre el uso de sistemas de videovigilancia en los puestos de trabajo: la STC 98/2000 y STC 186/2000. Estas sentencias legitimaban el uso de videovigilancia cuando existieran "fundadas sospechas sobre la existencia de un comportamiento antijurídico por parte de algún trabajador, legitima al empleador para instalar mecanismos de grabación en determinados espacios en los que se lleve a cabo la prestación laboral y siempre que ello se ajuste estrictamente a las exigencias de proporcionalidad, de manera que venga a ser una medida idónea, necesaria, proporcionada y de carácter estrictamente temporal." (STC 39/2016 Antecedentes de hecho nueve), pero lo hacía desde la perspectiva del genérico derecho a la intimidad personal del artículo 18.1 CE, resolvía el problema haciendo una ponderación entre el derecho fundamental a la intimidad del trabajador en su puesto de trabajo y el interés legítimo de la empresa en el control de la actividad.

Esta tendencia se mantuvo hasta 2013, cuando por fin el TC en la STC 29/2013, de 11 de febrero, declaró de forma contundente que el derecho a la protección de datos también se encontraba afectado en esta forma de control empresarial. En esta sentencia el Tribunal aplicó la normativa de protección de datos, fundamentalmente el deber de información previa y el principio de finalidad, es decir que no se pueden usar los datos

con fines distintos para los que se justificó su tratamiento. En este caso el tribunal declaró inconstitucional la utilización, sin aviso, de unas cámaras para asegurar la seguridad de los edificios cuando el fin era comprobar que los trabajadores cumplían con la jornada laboral. De esta forma el TC "perfiló el contenido del derecho fundamental a la protección de datos de una manera profunda y decidida en favor del trabajador".[84]

Después el TC matizó su doctrina cuando dictó la STC 39/2016, de 8 de abril. Los hechos se pueden resumir de la siguiente manera: se advirtieron múltiples irregularidades tras la instalación de un nuevo sistema informático en la caja del establecimiento. La empresa decide instalar un sistema de videovigilancia compuesto por una sola cámara dirigida a la caja donde presuntamente se estaban llevando a cabo actividades ilícitas de apropiación indebida, con el objetivo de acreditarlas y por tanto mantener esta forma de control con ese único fin.

Se procedió a la instalación y a la colocación del distintivo "zona videovigilada" cumplimiento con la normativa vigente en materia de protección de datos. Mediante el sistema de videovigilancia se comprobó quien era el trabajador que estaba comiendo las irregularidades y la cuantía de la cantidad que se estaba apropiando indebidamente. Se procedió a su despido. La trabajadora elevó la causa hasta el TC alegando que su derecho a la protección de datos había sido vulnerado por no haberla informado de la instalación del sistema de videovigilancia.

La tarea del TC en esta sentencia es aclarar "el alcance de la información a facilitar a los trabajadores sobre la finalidad del uso de la videovigilancia en la empresa: si es suficiente la información general o, por el contrario, debe existir una información

[84] GARCÍA GRANJO, R.: "El TC avala la videovigilancia encubierta en la empresa: la reinterpretación de un derecho fundamental por la vía de la proporcionalidad, incluso en la ilegalidad (Comentario a la STC de 3 de marzo de 2016, recurso de amparo 7222-2013), *Documentación Área Sociolaboral-CEF*, 2016. Disponible en https://www.laboral-social.com/stc-3-marzo-2016-camaras-ocultas-vigilancia-trabajo-proteccion-datos-proporcionalidad.html (Fecha de última consulta: 13 de junio de 2022)

específica" (STC 39/2016 F.J. 1). El TC considera que la forma de control ejercida sobre la trabajadora por las probadas irregularidades es conforme a derecho y no hay una vulneración del derecho a la protección de datos por los siguientes razonamientos: i) En este supuesto el consentimiento del trabajador no sería necesario porque se entiende implícito en la relación laboral siempre que el tratamiento de los datos de carácter personal sea necesario para el mantenimiento y cumplimiento del contrato, articulo 10.3.b) de la derogada Ley Orgánica de Protección de Datos de 1999). ii) El TC repara en que el deber de información previa se ha cumplido colocando el distintivo, en un lugar visible, que alertada de que la zona estaba videovigilada, dice así el TC "teniendo la trabajadora información previa de la instalación de las cámaras de videovigilancia a través del correspondiente distintivo informativo[85] y habiendo sido tratadas las imágenes captadas para el control de la relación laboral, no puede entenderse vulnerado el art. 18.4 CE.*"*. (F.J.4) iii) La constitucional de cualquier medida de derechos fundamentales viene determinada por la observancia del principio de proporcionalidad, es necesario comprobar que la medida cumple los tres requisitos siguientes: si es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si la medida es necesaria, en el sentido de que no exista otro menos invasiva que logre cumplir el objetivo propuesto (juicio de necesidad); y finalmente si la medida en si misma es proporcionada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto).

Dice así la Sala del TC "la medida de instalación de cámaras de seguridad que controlaban la zona de caja donde la demandante de amparo desempeñaba su actividad laboral era una medida justificada porque existían razonables sospechas de que alguno

[85] La AEPD dictó la Instrucción 1/2006, de 8 de noviembre, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras. Lo que pretende es adecuar los tratamientos de imágenes con fines de vigilancia a los principios sentados por la LOPD y garantizar los derechos de las personas cuyas imágenes son tratados por medio de tales procedimientos.

de los trabajadores se estaba apropiando de dinero; idónea para la finalidad pretendida por la empresa porque de esta forma era posible verificar si algunos de los trabajadores cometía efectivamente las irregularidades sospechadas; necesaria porque la grabación serviría de prueba; y equilibrada porque la grabación de imágenes se limitó a la zona de la caja". (STC 39/2016 F.J. 5).

No existió consenso entre todos los miembros del TC y el Magistrado Fernando Valdés Dal-Ré emitió un voto particular porque entiende que la nueva doctrina nos hace retroceder en la protección de datos de los trabajadores. Los demás magistrados consideran que hay una colisión conflictiva de derechos, entre el derecho a la protección de datos y la facultad de control por parte del empresario, cuando esta última no es un derecho fundamental sino *una regla rectora de la relación contractual*. De modo que, "El contenido esencial de los derechos fundamentales constituye el obligado e imprescindible referente del juicio de constitucionalidad y que no cualquier factor comprometido, como aquí acontece con el interés o el derecho empresarial de vigilar el cumplimiento de la relación laboral, puede oponerse a su garantía sustantiva". (Voto particular del Magistrado Fernando Valdés Dal-Ré en la STC 39/2016)

Esta Sentencia no estuvo exenta de críticas, el profesor VILLAZON entiende que "en los supuestos en que el consentimiento no sea necesario, el deber de información, lejos de atenuarse, incrementa su relevancia, pues entonces será el único que garantice la subsistencia de una mínima capacidad del individuo de controlar el uso por terceros de los datos a él relativos."[86].

Esta sentencia no es acertada en primer lugar porque la facultad de control del articulo 20.3 ET no puede considerarse una expresión directa e indefectible de los artículos 33 y 38 CE. Por lo tanto, en este caso no existe un juicio de constitucional entre el derecho a la protección de datos y la facultad de control del articulo 20.3 ET, pues esta última constituye una regla jurídica rectora de la relación contractual, que además no puede

[86] FERNÁNDEZ VILLAZÓN, L.A.*: op. cit.*, pág. 222.

ejercerse de modo irregular y excesivo como ha ocurrido en estos hechos. Pues de esta forma, esta doctrina constituye "un despropósito jurídico-constitucional, pudiendo arrastrar un caudal de consecuencias prácticas de imposible aceptación en nuestro Estado social". (Voto particular del Magistrado Fernando Valdés Dal-Ré en la STC 39/2016) Por último resulta desconcertante que los tribunales equiparen el deber de información previa con un distinto que advierte de que la zona está vigilada, porque el deber de información previa es el principal pilar para hacer efectivo el derecho a la autodeterminaciónn informática, pues si no sabes que tus datos se están tratando, con que finalidad, quien los trata y que derechos le asisten en virtud de ese tratamiento, es muy complicado que se puede garantizar a los trabajadores el derecho fundamental a la protección de datos.

Jurisprudencia del Tribunal Europeo de Derechos Humanos. Tras la Sentencia del TEDH en el caso Barbulescu c. Rumania de 5 de septiembre de 2017, el TEDH dictó la Sentencia de 9 de enero de 2018, conocida como Caso López Ribalda I, en esta sentencia se aborda el uso de los sistemas de videovigilancia en el lugar de trabajo y el necesario equilibrio que tiene que darse entre el poder de dirección del empresario (articulo 20.3 ET) y el derecho fundamental a la protección de datos (artículo 18.4 CE) y a la intimidad (artículo 18.1 CE).[87]

Los hechos se pueden resumir del siguiente modo, los trabajadores trabajaban para un importante Supermercado, a partir de marzo de 2009 los gestores del supermercado se dieron cuenta de que estaban sufriendo importantes pérdidas económicas en relación con el nivel de existencias y las cifras de ventas. Se instaló un sistema cerrado de televisión compuesto por cámaras visibles y ocultas, estas últimas dirigidas hacia los mostradores de caja para comprobar que estaba sucediendo. El día 25 de junio de 2009, la dirección del supermercado comunico al representante del sindicado que las cámaras

[87] BLAZQUEZ AGUDO, E.M.: *op. cit.*, pág. 51-53.

ocultas revelaron robos por parte de varios empleados.[88] Se procedió al despido de los trabajadores que habían cometido las irregularidades que constituían un incumplimiento grave de las obligaciones de buena fe y lealtad necesarias en la relación laboral.

Antes de poner el caso en manos de la justicia europea, tanto el Juzgado de lo Social, como el Tribunal Superior de Justicia declaró procedente el despido de los trabajadores alegando que el uso de la videovigilancia oculta en el lugar de trabajo sin haber informado previamente a los trabajadores era conforme con el articulo 20.3 ET, que faculta al empleador para que pueda usar las medidas de control y vigilancia que estime oportunas siempre que superen el test de proporcionalidad, determinado en este caso por los siguientes parámetros: por un lado existían fundadas sospechas de que se estaban cometiendo robos en el lugar de trabajo y por otra parte el objetivo perseguido era legítimo, necesario y proporcionado, pues no existen otros medios igual de eficaces que protejan los intereses del empresario y vulneren en menor medida los derechos de los trabajadores. Los trabajadores elevaron la causa ante el TC y el TS, pero ambos inadmitieron los recursos interpuestos ante ellos.

Finalmente, los cinco trabajadores, de los catorce que fueron despedidos, interpusieron una demanda ante el TEDH con el propósito de que declare la vulneración del articulo 6.1 -derecho a un proceso equitativo- y del articulo 8 -derecho al respecto de la vida privada- del Convenio Europeo de Derechos Humanos porque consideran que la toma de imágenes que se llevó a cabo sin comunicación alguna de las cámaras ocultas vulnera sus derechos a la vida privada y por tanto invalida la prueba. [89]

[88] BLASCO BELLICER, A.: *"Jurisprudencia sobre el control empresarial de la actividad del trabajador mediante instrumentos tecnológicos",* en AA.VV (MONREAL BRINGSVAERD,E., Cord): Derecho del Trabajo y Nuevas Tecnologías, ed. Tirant lo Blanch, 2020, pág. 230-233.

[89] DELGADO JÍMENEZ, A.F, 2020, *La privacidad del trabajador y el control tecnológico de la actividad laboral* (en línea). Tesis doctoral. Madrid: Universidad Complutense, pág. 298-306. Disponible en: https://eprints.ucm.es/id/eprint/64098/1/T42088.pdf (fecha de última consulta: 13 de Junio de 2022)

Antes de analizar las sentencias tengo que advertir que la jurisprudencia del TEDH acerca del uso de la videovigilancia oculta en lugares de trabajo debe interpretarse a la luz del RGPD y de la regulación nacional vigente. La razón de ello es que Consejo de Europa es el organismo que aprobó el primer Convenio Internacional sobre protección de datos, por ende, el TEDH solo se dedica a controlar la aplicación del CEDH y en este texto no se reconoce expresamente el derecho a la libertad informática. La jurisprudencia del TEDH no puede tomarse de referencia si limita o restringe los derechos y libertades que son recocidas por la legislación nacional (artículo 53 CEDH).

En relación a los hechos el TEDH reconoce que el uso de sistemas de videovigilancia ocultos se llevó a cabo porque existían fundadas sospechas de que se estaban cometiendo robos por los empleados, pero al mismo tiempo advierte que los datos visuales obtenidos son considerados datos personales y por tanto entran dentro del ámbito de aplicación de la normativa de protección de datos. En la anterior Ley Orgánica 15/1999 de 13 de octubre, de protección de datos de carácter personal, vigente en el momento de los hechos, el artículo 5 establecía la obligación de informar a los titulares de los datos acerca de la existencia de un fichero como de la finalidad y los destinatarios de la información. El articulo habilita para los trabajadores una expectativa razonable de respeto de su privacidad y por tanto la empresa en ese sentido erró.

El TEDH determinó que no ha existido un justo equilibrio entre el derecho de los trabajadores al respeto de su vida privada ex articulo 8 CEDH y el interés del empresario por tanto la actuación llevada a cabo por el empresario vulnera el artículo 8 CEDH.

Sin embargo, España solicitó al TEDH que revisara la sentencia adoptada, para ello el Tribunal analizó la antigua LORTAD y la doctrina de la STC 186/2000, de 10 de junio. Finalmente dictó la Sentencia de 17 de octubre de 2019, conocida como caso López Ribalda II. Lo más relevante de esta sentencia, es que incorpora el Test Barbulescu de Garantía de Privacidad en relación al control ejercido por el empresario mediante el uso de video vigilancia en los puestos de trabajo de sus empleados.

Se deberán tener en cuenta los siguientes factores para hallar un justo equilibrio en el conflicto de derechos e intereses propio de las relaciones laborales:[90] i) Si el trabajador ha podido ser informado acerca de la posibilidad de que el empresario adopte medidas de video vigilancia y del modo en el que va a proceder a su instalación. ii) El alcance de la grabación por el empleador y el grado de intrusión en la privacidad del trabajador. iii) Si el empleador posee y ha expuesto razones legitimas que justifiquen la grabación y su propio alcance. iv) Si es posible haber establecido otro sistema de grabación que sea menos intrusivo para el trabajador. v) Se deberán valorar las consecuencias de la video vigilancia para el trabajador. vi) Si al trabajador se le han proporcionado las garantías adecuadas, especialmente cuando las operaciones de control del empresario son de carácter intrusivo.

Esta sentencia ha supuesto un importante avance pues esclarece la cuestión de los controles ocultos y además valida la doctrina del TC, sentada en su STC 186/2000, de 10 de julio. En este nuevo fallo el TEDH no aprecia vulneración del articulo 8 CEDH porque considera que los controles ocultos son proporcionados, aunque reconoce que el empresario no cumplió con el deber de información previo advierte que podrían haber denunciado el incumplimiento del deber de información previa ante la Agencia Española de Protección de Datos y ante los tribunales tanto por vía civil como administrativa.

La doctrina sentada en esta sentencia determina que la privacidad y la intimidad de los trabajadores exige, como norma general, que el empleador les informe con anterioridad a la puesta en marcha de sistemas de videovigilancia, y de su finalidad. Pero es cierto, que sí que admite el uso de cámaras ocultas, en caso muy específicos donde existan sospechas fundadas de incumplimientos graves o muy graves por parte de los trabajadores que afecte gravemente a los intereses de la empresa siempre que la medida

[90] PRECIADO DOMENECH, C. H. “Comentarios de urgencia a la STEDH de 17 de octubre de 2019 caso López Ribalda c. España (Gran Sala*), Revista de la Comisión de lo Social de Jueces y Juezas para la Democracia*, núm. 2, 2019, pág 7-23.

de videovigilancia sea limitada y proporcionada. En estos casos la información que el empresario debe suministrar a los trabajadores es considerada un factor más a tener en cuenta a la hora de determinar la proporcionalidad de la medida en un supuesto concreto, pero se tiene que llevar acabo un examen más riguroso de los otros factores.

El fallo de esta sentencia no cuenta con el beneplácito de todos los magistrados que componen la sala, tres de los magistrados elaboraron un voto particular en el que manifestaban su desacuerdo con la interpretación efectuada por los demás magistrados. Pues entienden que "Al no constatar ninguna violación del artículo 8 del Convenio, el Tribunal ha decidido permitir el uso ilimitado de la videovigilancia encubierta en el lugar de trabajo sin ofrecer suficientes garantías jurídicas a las personas cuyos datos personales serán recogidos y utilizados para fines desconocidos para ellas. (Voto particular de la STEDH de 17 de octubre de 2019).

7. CONCLUSIÓN

Primera. Durante el transcurso de este estudio he observado que la regulación del derecho a la protección de datos en el ámbito laboral es insuficiente y además su esquema es confuso porque no está ordenada de forma sistemática. Esto supone un grave problema porque las normas están dirigidas a los ciudadanos y deben ser accesibles para ellos.

Segunda. El RGPD ofrece la posibilidad a los estados miembros como a sus interlocutores sociales de que establezcan normas más específicas con el fin de otorgar mayor protección a los derechos y libertades en relación con el tratamiento de los datos personales de los trabajadores. Ninguno de estos dos actores ha logrado su cometido con éxito por tanto debe ser un organismo supranacional el que tutele este derecho.

Tercero. El aumento de las formas de control debido a los avances tecnológicos está intensificando aun más el desequilibrio de poder que hay entre las partes en un contrato de trabajo.

Cuarto. La jurisprudencia del TC y TEDH sobre él uso de sistemas de videovigilancia por parte del empleador ex articulo 20.3 ET es muy permisiva porque la normativa de protección de datos es muy restrictiva con las formas de control que el empresario puede implementar sobre los trabajadores, en cambio los tribunales por medio de sus sentencias están legitimando la infracción de la normativa de protección de datos a la hora de determinar la licitud o ilicitud de una prueba que determiné la procedencia de un despido disciplinario.