UNIVERSIDAD DE VALLADOLID

Facultad de Derecho

Grado en Derecho

TECNOLOGÍA, VIGILANCIA EMPRESARIAL Y DERECHO A LA INTIMIDAD DEL TRABAJADOR

Presentado por:

Alberto Furquet Izquierdo

Tutelado por:

María Milagros Alonso Bravo

28/06/2022

AGRADECIMIENTOS

<<En primer lugar agradecer a mi tutora Milagros Alonso Bravo, quien con sus conocimientos y apoyo me guió a través de las etapas de este proyecto.>>

<<También quiero agradecer a mis compañeros y amigos por acompañarme en este camino.>>

<<Por último, agradecer a mi madre, padre y hermano por creer en mí y a mi abuela Benedicta Herráez Prieto por estar a mi lado en cada momento de mi vida.>>

ÍNDICE

• RESUMEN

Durante los últimos años se ha visto incrementada la influencia de las nuevas tecnologías tanto en la realización de la actividad laboral de los trabajadores, como en la forma de controlar el empresario el cumplimiento de las obligaciones laborales.

Este trabajo consiste en un análisis de los poderes que tiene el empresario, en concreto el poder de vigilancia y control, en el estudio de dos grandes derechos fundamentales que entran en juego cuando los límites del poder de vigilancia y control son sobrepasados, concretamente el derecho fundamental a la protección de datos y el derecho a la intimidad y, por último, se realiza un estudio sobre tres especialidades introducidas por la LOPD con motivo de la intrusión de las TICs en el ámbito laboral, que son la videovigilancia, la grabación de sonido y el control del uso de los medios informáticos de titularidad empresarial, analizando sobretodo sus límites a través de la jurisprudencia.

• ABSTRACT

In recent years, the influence of new technologies has increased both in the performance of workers' work activities and in the way in which the employer controls the fulfilment of work obligations.

This work consists of an analysis of the powers of the employer, specifically the power of surveillance and control, in the study of two major fundamental rights that come into play when the limits of the power of surveillance and control are exceeded, namely the fundamental right to data protection and the right to privacy, finally, a study is made of three specialities introduced by the LOPD due to the intrusion of ICTs in the workplace, namely video surveillance, sound recording and control of the use of company-owned computer media, analysing above all their limits through case law.

1. INTRODUCCIÓN

La inclusión en los últimos años de las nuevas tecnologías en el desarrollo de la actividad laboral ha supuesto un gran impacto en las relaciones laborales, tanto de forma positiva, como de forma negativa, creando una serie de inconvenientes como por ejemplo en la seguridad y salud en el trabajo o en la selección del personal.

Una de las consecuencias de esta influencia de las tecnologías de la información y las comunicaciones (en adelante "TICs") consiste en el establecimiento de los límites de su utilización tanto por parte del empresario como de los trabajadores de la empresa; antes de que se regulara por la legislación, el Tribunal Supremo (en adelante TS) se adelantó considerando que el problema era precisamente el establecimiento de los límites, descartando el debate sobre la licitud o no del uso de las TICs; liberado así el debate, realizó las siguientes consideraciones[1]:

i. Límites técnicos, siendo inadmisible la ralentización del rendimiento del ordenador de la empresa con motivo de su uso privado por parte del trabajador y, de igual manera, se considera incumplimiento de la buena fe contractual la reducción de la velocidad del ordenador de la empresa con motivo de la instalación o uso de programas privados.
ii. El uso de las TICs no puede suponer un daño o riesgo para los medios tecnológicos empresariales puestos a disposición del trabajador.
iii. Prohibición de eliminar el uso de las TICs que puedan generar responsabilidad externa para la empresa.
iv. Prohibición de actividades que vulneren la buena fe contractual ajenas a la actividad laboral del trabajador.
v. Posible vulneración de la obligación de la prestación de servicios por parte del trabajador por la utilización prolongada de las TICs.

Nos podemos encontrar con situaciones concretas ante el incumplimiento de las limitaciones del uso de las TICs que pueden llegar a vulnerar diferentes derechos fundamentales, destacando: el derecho a la intimidad personal (artículo 18.1 CE); derecho a la protección de datos personales (artículo 18.4 CE) y el derecho al secreto de las

[1] STS 18 de junio de 2006 (RJ 2006/8452).

comunicaciones (artículo 18.3 CE); aunque nosotros, en este trabajo, nos vamos a centrar en el desarrollo de los derechos fundamentales de protección de datos y a la intimidad.

Estos incumplimientos pueden surgir del uso abusivo de los poderes que le confiere el Estatuto de los Trabajadores (en adelante "ET") desarrollado por el Real Decreto Legislativo 2/2015, de 23 de octubre, al empresario, pudiéndolos encontrar en el artículo 20 de dicha ley, concretamente el poder de vigilancia y control, aunque nos podemos encontrar con dos poderes más, el poder de dirección y el poder sancionador, derivados de las notas básicas de la definición de dependencia y subordinación de los trabajadores, extraídas del artículo 1.1 del ET: trabajadores cómo *"aquellos que voluntariamente prestan sus servicios retribuidos por cuenta ajena y dentro del ámbito de organización y dirección de otra persona, física o jurídica, denominada empleador o empresario",* pero los poderes que nos interesan desarrollar para el contenido del trabajo son los poderes de vigilancia y control.

Para poder analizarlos, debemos de partir del artículo 38 de la Constitución Española (en adelante CE), donde se proclama el derecho a la libertad de empresa dentro del marco de la economía del mercado y, según el Tribunal Constitucional (en adelante TC), esta libertad de empresa conlleva "el reconocimiento a los particulares de una libertad de decisión no sólo para crear empresas y, por tanto para actuar en el mercado, sino también para establecer los propios objetivos de la empresa y planificar su actividad en atención a sus recursos y a las condiciones del propio mercado"[2].

El artículo 20 del ET, sobre la dirección y control de la actividad laboral, permite al empresario realizar ciertas medidas para la vigilancia y el control de la actividad laboral, eso sí, con el límite establecido en el apartado 3 del mismo artículo sobre la "consideración debida a su dignidad", lo que conlleva el respeto a los derechos fundamentales, sobre todo a los derechos vinculados con la intimidad[3].

En relación con la limitación del poder de control empresarial, a la hora de entrar en conflicto con los derechos fundamentales, debemos de distinguir tres grandes criterios establecidos por los tribunales[4]:

[2] STC 8 de Julio de 1993 (RTC 418/1987 y 421/1987 nº 1902/1991 y 1904/1991).
[3] GOERLICH PESET, José María "*Poderes del Empresario",* en AAVV, *Derecho del Trabajo, Tirant lo Blanch, Valencia, 2016*.
[4] RASCÓN LÓPEZ, RODRIGO, *Reflexiones sobre los límites del poder de control empresarial ejercido sobre los trabajadores por medios tecnológicos,* La Revista internacional del derecho práctico.

a) El criterio de proporcionalidad, según el cual se debe de estudiar si el método de control empresarial es idóneo, adecuado y el menos lesivo para el fin perseguido. Este criterio será desarrollado más adelante.

b) Criterio de la expectativa de la intimidad: este criterio se orienta a partir de la expectativa de intimidad que surge en el trabajador cuando comienza una relación laboral, de tal manera que los controles imprevistos por parte del empresario o empleador podrían vulnerar este derecho a la intimidad del trabajador; en cambio, si el empresario se lo comunica con anterioridad al trabajador o a un representante legal de los trabajadores, no se podría considerar vulnerado este derecho por la expectativa creada en el trabajador.

c) Criterio de autodeterminación informativa, donde se pone en relieve la capacidad de los trabajadores para controlar su información personal, al mismo tiempo que si se obtienen datos o si se van a menar datos de los trabajadores, estos deben de ser informados previamente.

Como hemos visto, poder de vigilancia y control del empresario no es ilimitado, sino que debe de respetar la dignidad del trabajador y sus derechos y libertades fundamentales; nos encontramos entonces con el carácter ambiguo de la normativa donde, por un lado, tenemos los límites a los poderes empresariales establecidos por las disposiciones legales (entre ellos el artículo 4 del ET donde se establecen los derechos básicos de los trabajadores) y, por otro, los establecidos por el contrato de trabajo, revistiendo al trabajador de unos derechos y garantías que el empresario no puede traspasar.

Ese carácter ambiguo ha conllevado que los tribunales deban de establecer unas pautas ante el surgimiento de las TICs, muchos de ellos contradictorios, creando una cierta inseguridad jurídica, hasta que en 2018 surgió la Ley Orgánica de Protección de Datos (en adelante LOPD) donde ya se desarrollan las especialidades introducidas por las TICs como pueden ser la videovigilancia, el control de los usos de dispositivos informáticos o la limitación del uso de micrófonos (entre otros) durante el desarrollo de la actividad laboral del trabajador, y es precisamente en lo que consiste este trabajo, en desarrollar ciertas

especialidades introducidas por las TICs en el ámbito laboral que están ligadas a los derechos fundamentales nombrados anteriormente.

2. CONFLICTO ENTRE LOS PODERES EMPRESARIALES Y LOS DERECHOS FUNDAMENTALES DEL TRABAJADOR EN EL USO DE LAS TICs.

Como hemos venido diciendo anteriormente, el Ordenamiento Jurídico otorga al empresario una serie de poderes para el cumplimiento de la actividad laboral del trabajador, pero que no son ilimitados, y si el empresario traspasa las fronteras de dichos poderes puede llegar a vulnerar ciertos derechos fundamentales, aunque nosotros nos vamos a centrar en el estudio del Derecho a la intimidad y el Derecho a la protección de datos.

Antes de entrar a desarrollar cada derecho, hemos de aclarar que se tratan de Derechos fundamentales autónomos, cada cual, con un contenido diferente, pues, aunque ambos estén consagrados en el artículo 18 de la CE, pero ya en el año 2000 el TC en su STC 292/2000 de 30 de noviembre manifestó el derecho a la protección de datos como derecho fundamental autónomo e independiente del derecho a la intimidad y familiar.

Es más, esta sustantividad propia que presenta el derecho a la protección de datos frente al derecho a la intimidad proviene del reconocimiento constitucional del primer derecho (artículo 18.4 CE) frente a la intimidad reconocida en el artículo 18.1 CE.

Ahora bien, también es cierto que en el ámbito laboral podemos considerarlo como un derecho mixto, pues para que se garantice la protección de datos no solamente se necesita un título habilitante (ya lo veremos más adelante) sino que, además, cuando hablamos de las especialidades introducidas por las TICs en nuestro derecho, hay que garantizar el contenido de ambos derechos, del derecho a la protección de datos y además garantizar derechos fundamentales vinculados a él como el derecho a la intimidad, pudiendo decir que dentro de su contenido esencial estarían otros derechos fundamentales como el derecho a la intimidad o el derecho al secreto de las comunicaciones.

Así pues, no se ha incorporado de manera expresa la referencia al derecho de protección de datos en la LOPD de 2018, es más, en el artículo 20 bis del ET reconoce el derecho a la intimidad de los trabajadores en el uso y frente al uso de los dispositivos digitales, por lo que podemos extraer que no se ha querido incorporar al texto estatutario el derecho

de protección de datos como derecho fundamental, a pesar de su autonomía respecto al derecho a la intimidad.[5]

Por lo que, como podemos ver, aunque hoy en día están configurados como derechos autónomos e independientes, en ciertos aspectos del ámbito laboral introducidos por las nuevas tecnologías, ambos derechos quedan vinculados, debiendo de respetar el empresario el contenido de ambos derechos para encontrarse en el marco de la legalidad.

2.1. Derecho a la intimidad del trabajador

En este punto, vamos a desarrollar el derecho a la intimidad como derecho fundamental regulado en nuestra Carta Magna, y el mismo derecho desde la perspectiva del ámbito laboral.

2.1.1. Derecho a la intimidad como derecho fundamental

Para poder centrarnos en la figura del trabajador, debemos apuntar antes que el derecho a la intimidad se encuentra dentro de los derechos fundamentales regulado en el Título I Carta Magna, es decir, dentro de los derechos inherentes a la persona, concretamente en el apartado 1 del artículo 18, donde se nos dice que: "*1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen",* al igual que encontramos este mismo derecho reconocido por el Convenio Europeo de Derechos Humanos (en adelante CEDH) en su artículo 8: *1. "Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia."*

Sí bien es cierto de que no existe un concepto legal, el TC estableció que "el concepto de intimidad personal no puede enmarcarse en una definición que precise detalladamente su alcance, (…) pero ha de tenerse en cuenta que conforma patrimonio personal y hace necesario relacionar la cuestión con lo que constituye el espacio vital de cada uno, y que se proyecta sobre el concepto impreciso de lo que constituye el círculo reservado e íntimo, compuesto por datos y actividades que conforman la particular vida existencial de cada persona y autoriza a preservarla de las injerencias extrañas"[6] . Como concepto, podemos definir la intimidad como "el derecho a aislarse, de ser desconocido, de que los demás no sepan ni indaguen lo que somos o lo que hacemos, o incluso, lo que pensamos y creemos",

[5] LÓPEZ BALAGUER, Mercedes y RAMOS MORAGUES, Francisco: "*Control empresarial del uso de dispositivos digitales en el ámbito laboral desde la perspectiva del derecho a la protección de datos y a la intimidad".* Universidad de Valencia, 2020. Vol. 10. Núm. 2. Págs. 512 y ss.
[6] STC 112/2004 de 12 de julio (RTC 2004/112).

y cuyo contenido se concreta en "la facultad de excluir del conocimiento ajeno cualquier hecho comprendido dentro del propio ámbito que reserve el ciudadano para sí mismo, y para su familia"[7]

Es más, siguiendo a Xavier O`callagham, la intimidad se "funda en la inviolabilidad de la persona y, en el fondo, se basa en la dignidad humana"[8]

Es importante delimitar el concepto de intimidad con el de privacidad, atribuyendo al primero un mayor grado de intensidad y donde la privacidad se localiza como una de sus dos dimensiones, pues esta última puede ser conocida por algún ámbito de la persona, es decir, se puede exteriorizar, mientras que la intimidad en sentido estricto se sitúa fuera del conocimiento de los demás.

2.1.2. Derecho a la intimidad en el ámbito laboral.

El derecho a la intimidad del trabajador dentro de la relación laboral con el empresario, viene establecido en primer lugar en los artículos 4.2.e), donde se reconoce que *"En la relación de trabajo, los trabajadores tienen derecho: (…) Al respeto de su intimidad (…)"* y, en relación con el uso de dispositivos digitales, aparece regulada en el artículo 87.1 de la LOPD, *"Los trabajadores y los empleados públicos tendrán derecho a la protección de su intimidad en el uso de los dispositivos digitales puestos a su disposición por su empleador."*

La controversia que se suscita frente a este derecho es que, debido al avance de las nuevas tecnologías como el uso de sistemas de grabación de imagen o sonido, la geolocalización, el acceso a internet lo que conlleva el uso del correo electrónico o un aumento de la aparición del teletrabajo, entre otros, ha conllevado la aparición de nuevas formas de intromisión por parte del empresario en la intimidad del trabajador y, con ello, la aparición de una legislación garantista como protectora de la intimidad y la imagen de los trabajadores[9].

Si bien es cierto que este derecho tiene diversas vertientes dependiendo del tipo de conducta empresarial que lesiona dicho derecho[10], el TC[11] ha establecido una serie de

[7] Arias Domínguez, A. y Rubio Sánchez, F. El Derecho de los Trabajadores a la Intimidad. Navarra: Aranzadi, S.A., (2006).
[8] O`Callagham, Xavier: "Honor, Intimidad e Imagen", en *Libertad de Expresión y sus Límites.* Madrid, 1991.
[9] De León, Alonso: "*El derecho a la intimidad del trabajador y el poder de control empresarial" 2019*.
[10] Demelsa Liberato, Diandra: *"Derecho a la intimidad del trabajador y poder empresarial"*. Universidad de León. *2018*.
[11] STC 112/2004 de 12 de julio (RTC 2004/112).

requisitos para que no se de una vulneración de este derecho, que se basa en el principio de proporcionalidad, debiendo de superar el triple juicio:

i. Idoneidad en las medidas adoptadas, es decir, que la medida sea adecuada para lograr el objetivo perseguido por la empresa.

ii. Necesidad en la medida utilizada, empleando la medida menos invasiva y más moderada para el trabajador, de lo contrario será considerada como una medida abusiva.

iii. Proporcional en sentido estricto, pues la medida debe de ser equilibrada, evitando los mayores perjuicios para el trabajador, y teniendo en cuenta la existencia de una relación entre la invasión que se produce a los derechos fundamentales del trabajador y el fin que es buscado por el empresario.

Cuando no se respeta este derecho, es decir, cuando se ejercita el poder de vigilancia y control empresarial fuera de los límites establecidos por el legislador o por los tribunales, nos encontramos en una situación de invasión o vulneración del derecho a la intimidad, es lo que se denomina la colisión entre el derecho a la intimidad del trabajador y el poder de control empresarial, pues ni el primero es un derecho absoluto ni el poder de control del empresario es un poder ilimitado.

2.2. El derecho a la protección de datos

2.2.1. Evolución

El primer antecedente lo encontramos en la LORTAD[12], en cuyo artículo primero señalaba que el objeto de la ley era limitar el uso de la informática y otras técnicas y medios de tratamiento automatizado de los datos de carácter personal para garantizar el honor, la intimidad personal y familiar de las personas físicas y el pleno ejercicio de sus derechos.

Esta ley, fue derogada por la LOPD de 1999[13], cuyo objetivo principal fue regular el tratamiento de los datos personales y los ficheros donde se contenían; regular los derechos

[12] Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal.
[13] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

de las personas físicas y las obligaciones respecto a los ficheros y el tratamiento de los datos de carácter personal. Esta ley fue completada por el RLOPD[14].

Aun así, el derecho fundamental necesitaba ser perfilado por el Tribunal Constitucional, destacando las siguientes sentencias:

i. STC 254/1993 de 20 de julio de 1993[15]. La importancia de esta sentencia la encontramos porque es la primera manifestación del TC en cuanto al derecho fundamental de protección de datos, pero con el nombre de autodeterminación informativa, independiente del derecho a la intimidad "*estamos ante un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la CE llama 'la informática"* (Fundamento VI).

ii. STC 94/1998, de 4 de mayo[16], donde el TC confirma que nos encontramos ante un derecho fundamental y donde se nos presenta como una potestad del ciudadano para oponerse a datos personales empleados para distintos fines.

iii. STC 292/2000, de 30 de noviembre del 2000[17], donde el TC configura el contenido del derecho de una persona a la protección de sus datos personales, estableciéndolo como un derecho fundamental y autónomo, pudiendo encontrar ya su contenido en la LOPD de 1999, teniendo el ciudadano derecho a decidir sobre sus propios datos.

iv. STC 292/2000, donde se informa y configura este derecho fundamental a la protección de datos diferenciado del derecho a la intimidad.

Por último, en 2016 entró en vigor el Reglamento UE 2016/679 (RGPD), nacido de la búsqueda de la armonía y homogeneización de la regulación en materia de protección de datos, y cuya consecuencia fue su adaptación en España fue la puesta en vigor de la Ley Orgánica de protección de Datos y Garantías de los Derechos Digitales (en adelante la "LOPD").

[14] Real Decreto 1720/2007 de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
[15] STC 254/1993, de 20 de julio de 1993 (RTC 1993,254), nº recurso 1827/1990.
[16] STC 94/1998, de 4 de octubre (RTC 94/1998), nº de recurso 840/1995.
[17] STC 292/2000 de 30 de noviembre (RTC 2000/292), nº recurso 1463/2000.

2.2.2. Concepto y regulación

El derecho a la protección de datos es aquel derecho fundamental de toda persona física que la faculta para disponer y controlar sus datos de carácter personal, pudiendo decidir cuáles proporcionar a terceros, así como conocer quién posee esos datos y para qué, y oponerse a esa posesión o tratamiento.

El Tribunal Constitucional en la Directiva 95/46/CE, y la LOPD delimita el concepto de dato personal, tratamiento de datos personales y fichero de datos personales:

a) Se entenderá por dato personal: toda información sobre un apersona física identificable ("el interesado"); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social.

b) Se entenderá por tratamiento de datos personales cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y de aplicación a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, comunicación, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción.

c) Se entenderá por fichero de datos personales todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, y asea centralizado o descentralizado o repartido de forma funcional o geográfica.

Este derecho viene reconocido en el artículo 18.4 de la Constitución Española, donde aparece como un mandato al legislador para garantizar los derechos fundamentales frente al uso de la informática, artículo 8.1 de la Carta de los Derechos Fundamentales de la Unión Europea*: "Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan"*, en su apartado 2: *"Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación"* y el 16 del Tratado de

Funcionamiento de la Unión Europea, con el mismo contenido que la anterior, estableciendo normas sobre protección de las personas respecto al tratamiento de sus datos personales.

En el Convenio Europeo de Derechos Humanos y de las Libertades Fundamentales de 4 de noviembre de 1950 encontramos un reconocimiento del derecho al respeto de la vida privada y familiar, incorporando así el derecho a la privacidad, y debido a su gran vinculación con el derecho a la protección de datos, el Consejo de Europa adoptó el 28 de enero de 1981 el Convenio o número 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

Por otro lado, el Reglamento (UE) 2016/679[18] se encarga de un desarrollo exhaustivo del derecho a la protección de datos, comportando una voluntad excluyente de los legisladores nacionales en cuanto a su desarrollo. Además, el Reglamento es de aplicación directa, sin necesidad de que sea transpuesto por las normas nacionales de los Estados Miembro.

Por último, en el ámbito nacional, encontramos la LOPD, cuyo objeto es garantizar y proteger, en cuanto al tratamiento de los datos personales, los derechos fundamentales y las libertades públicas de las personas físicas, y especialmente su derecho al honor e intimidad personal y familiar.

En cuanto a su contenido, el TC se ha manifestado considerando que "El derecho fundamental al que estamos haciendo referencia garantiza a la persona un poder de control y disposición sobre sus datos personales. Pues confiere a su titular un haz de facultades que son elementos esenciales del derecho fundamental a la protección de los datos personales, integrado por los derechos que corresponden al afectado a consentir la recogida y el uso de sus datos personales y a conocer los mismos. Y para hacer efectivo ese contenido, el derecho a ser informado de quién posee sus datos personales y con qué finalidad, así como el derecho a oponerse a esa posesión y uso exigiendo a quien corresponda que ponga fin a la posesión y empleo de tales datos (…) persigue garantizar a la persona el poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado"[19].

[18] Reglamento UE 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)

[19] STC 290/2000 de 30 de noviembre de 2000 (ES:TC: 2000:290, Nº de Recurso 201/1993)

El TC diseña en su STC 292/2000 el contenido del derecho a la protección de datos, donde manifiesta la incorporación de un nuevo derecho en el artículo 18.4 de la CE, independiente del derecho a la intimidad (fundamento V).

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

2.2.3. El principio de calidad de los datos personales

El principio de calidad de los datos personales viene regulado en el artículo 6 de la Directiva 95/46/CE, donde se dispone que los datos personales deben de ser:

a) Tratados de manera leal y lícita.
b) Recogidos con fines determinados, explícitos y legítimos y no sean tratados posteriormente de manera incompatible con dichos fines; no se considerará incompatible, el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando los Estado miembros establezcan las garantías oportunas.
c) Adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente.
d) Exactos y, cuando sea necesario, actualizados. Deberán de tomarse todas las medidas razonables, para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificados;
e) Conservados en una forma que permita la identificación de los interesados durante un periodo no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente.

Este principio responde a una finalidad de garantizar el derecho a la intimidad, estableciendo de tal manera una serie de restricciones en relación con la recogida y tratamiento de los datos personales.

2.2.4. El consentimiento en el tratamiento de los datos

Según el artículo 4.11 del RGPD, el consentimiento se define como "la manifestación de voluntad libre, específica, informada e inequívoca por la cual una persona acepta, mediante una clara acción afirmativa, el tratamiento de sus datos personales".

Podemos distinguir tres tipos de consentimiento:

- Consentimiento expreso, definido como aquel que se otorga de forma concreta, explícita y directa, pudiendo registrarse de una o varias maneras que no dejen lugar a dudas. Suele ser mediante la firma de documento oficial.
- Consentimiento tácito: aquel que se deduce de la inacción o el silencio de la parte del interesado, es decir, cuando no se niega el interesado al tratamiento de sus datos. Este consentimiento no es válido en cuanto a la recogida y tratamiento de los datos personales.

- Consentimiento presunto, dándose este cuando el interesado, a través de sus actos o comportamiento, acepta el posible tratamiento de sus datos. Este consentimiento tampoco se considera válido en cuanto al tratamiento de los datos personales.

En cuanto a su régimen jurídico, podemos hablar de dos tipos de datos personales en el ámbito laboral: los que están sometidos dentro del régimen ordinario, que tiene cuatro títulos habilitantes para su tratamiento, donde el primero de ellos el consentimiento del interesado como regla general; pero el legislador considera que puede no haber consentimiento del interesado cuando haya un fin justificado conectado con la ejecución del contrato, la aplicación de medidas precontractuales, cumplimiento de las obligaciones laborales o con la protección de intereses vitales o satisfacción de intereses legítimos del responsable o de un tercero, por lo que encontramos otras tres causas: la necesidad de ejecución del contrato de trabajo, la necesidad de dar cumplimiento a las obligaciones legales y la de proteger intereses vitales o legítimos, sirviendo estos como títulos habilitantes del empresario para el tratamiento de los datos personales del trabajador.

Por otro lado, nos encontramos con los datos especialmente sensibles (porque, por ejemplo, revelan ideologías o la salud de los trabajadores); en estos casos, como regla general, será necesario un consentimiento explícito del trabajador relacionado con fines específicos. Ahora bien, también puede haber otros títulos habilitantes para el tratamiento de estos datos, justificados por una necesidad legítima del tratamiento, vinculado al cumplimiento de las obligaciones laborales o de seguridad social, a la satisfacción de fines preventivos o laborales o relacionados con la prestación social, protección de intereses vitales o realización de actividades legítimas por parte de una asociación o fundación.

Ante lo expuesto, podemos ver cómo los datos especialmente sensibles tienen un mayor control con respecto a la finalidad, poniendo condiciones más estrictas sobre su uso, justificación o destino.[20]

2.2.5. El deber empresarial de informar a los trabajadores.

Siguiendo los artículos 13 y 14 del REPD[21], el responsable del tratamiento, cuando los datos personales no se hayan obtenido del interesado, deberá de facilitar la siguiente información al interesado:

- Identidad, datos del contacto del responsable y, en su caso, de su representante
- Datos de contacto del delegado de protección de datos
- El fin que se busca con el tratamiento de los datos
- Los intereses legítimos del responsable o de un tercero cuando el tratamiento de los datos obtenidos sea necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre y cuando no prevalezcan los intereses o derechos y libertades fundamentales del interesado.
- Los destinatarios de los datos personales obtenidos.
- La intención del responsable de transferir los datos personales a un tercer país u organización internacional

[20] Rodríguez Escanciano, S., *Derechos laborales digitales: garantías e interrogantes.* Aranzadi, 2019, pp 127 ss.

[21]REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

- Las garantías de las que dispone el interesado y los medios para obtener una copia de estas.

Además, también se le facilitarán:

- El plazo de conservación de los datos personales cuando sea posible, de lo contrario, los criterios para determinarlo.
- El derecho a solicitar al responsable del tratamiento el acceso, rectificación, supresión, limitación o a su oposición al tratamiento, así como el derecho a la portabilidad de los datos recogidos personales recogidos.
- Derecho a retirar el consentimiento en los casos del artículo 6.1.a) y 9.2.a) del RGPD
- Derecho a presentar una reclamación ante una autoridad de control
- La información de las consecuencias de no facilitar los datos personales cuando se trate de un requisito legal, contractual o necesario para suscribir un contrato y se está obligado a aportarlo.
- Existencia de decisiones automatizadas.

El responsable del tratamiento de los datos obtenidos aportará la información relacionada con los mismos:

a) Plazo máximo de un mes desde la obtención de los datos.
b) En el momento de la primera comunicación al interesado.
c) En el momento en que los datos personales sean comunicados por primera vez.

2.2.6. Casos de exclusión del deber de información

El responsable no tendrá la obligación de aportar la información anteriormente explicada cuando:

a) El interesado ya esté informado.
b) Resulte imposible o suponga un esfuerzo desproporcionado comunicar dicha información.
c) La información esté prevista por el derecho comunitario o nacional.
d) Si los datos personales tienen carácter confidencial sobre la base de una obligación de secreto profesional.

2.2.7. Aportación de la Agencia Española de Protección de Datos (AEPD).

La Agencia Española de Protección de Datos es un organismo público con personalidad jurídica propia y plena capacidad pública y privada, encargada de velar por el cumplimiento de la Ley Orgánica de Protección de Datos, con sede en Madrid.

La AEPD, en este caso, recomienda utilizar un modelo de información "por capas o niveles" en su "Guía para el Cumplimiento del Deber de Informar", de esta manera, se facilita la tarea del Responsable del Tratamiento y se consigue una obtención de información más relevante de forma más rápida y simplificada respetando los principios de licitud, lealtad y transparencia:

- El primer nivel consiste en una información básica, resumida, en el mismo momento y en el mismo medio en que se recojan los datos.

- El segundo nivel consistiría en remitir una información adicional, más detallada de la información, en un medio más adecuado para su presentación, comprensión y archivo.

A parte de ello, recomienda presentar los cinco primeros epígrafes (Responsable, Finalidad, Legitimación, Destinatarios y Derechos) incluyendo el de Procedencia cuando los datos no procedan del propio interesado.

La siguiente imagen es un ejemplo dado por la AEPD sobre una agrupación recomendada para presentarla por capas o niveles:

Epígrafe	Información básica (1ª capa, resumida)	Información adicional (2ª capa, detallada)
"Responsable" (del tratamiento)	Identidad del Responsable del Tratamiento	Datos de contacto del Responsable
		Identidad y datos de contacto del representante
		Datos de contacto del Delegado de Protección de Datos
"Finalidad" (del tratamiento)	Descripción sencilla de los fines del tratamiento, incluso elaboración de perfiles	Descripción ampliada de los fines del tratamiento
		Plazos o criterios de conservación de los datos
		Decisiones automatizadas, perfiles y lógica aplicada
"Legitimación" (del tratamiento)	Base jurídica del tratamiento	Detalle de la base jurídica del tratamiento, en los casos de obligación legal, interés público o interés legítimo.
		Obligación o no de facilitar datos y consecuencias de no hacerlo
"Destinatarios" (de cesiones o transferencias)	Previsión o no de Cesiones	Destinatarios o categorías de destinatarios
	Previsión de Transferencias, o no, a terceros países	Decisiones de adecuación, garantías, normas corporativas vinculantes o situaciones específicas aplicables
"Derechos" (de las personas interesadas)	Referencia al ejercicio de derechos.	Cómo ejercer los derechos de acceso, rectificación, supresión y portabilidad de sus datos, y la limitación u oposición a su tratamiento
		Derecho a retirar el consentimiento prestado
		Derecho a reclamar ante la Autoridad de Control
"Procedencia" (de los datos)	Fuente de los datos (cuando no proceden del interesado)	Información detallada del origen de los datos, incluso si proceden de fuentes de acceso público
		Categorías de datos que se traten

22

2.2.8. El deber de información en la LOPD[23]

Vemos reconocido este deber de información empresarial en los artículos 87 y 89 de la LOPD:

- Art 87.3 LOPD: *"Los trabajadores deberán ser informados de los criterios de utilización a los que se refiere este apartado*"

[22] Ejemplo de agrupación recomendada por a AEPD en su *"Guía Para el Cumplimiento del Deber de Informar"*.
[23] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

- Art 89.1 LOPD*: "Los empleadores habrán de informar con carácter previo, y de forma expresa, clara y concisa, a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de esta medida"*

En relación con el contenido de este deber, también encontramos el artículo 11 de la misma ley, según el cual:

"1. Cuando los datos personales sean obtenidos del afectado el responsable del tratamiento podrá dar cumplimiento al deber de información establecido en el artículo 13 del Reglamento (UE) 2016/679 facilitando al afectado la información básica a la que se refiere el apartado siguiente e indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información.

2. La información básica a la que se refiere el apartado anterior deberá contener, al menos:
a) La identidad del responsable del tratamiento y de su representante, en su caso.
b) La finalidad del tratamiento.
c) La posibilidad de ejercer los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679.

Si los datos obtenidos del afectado fueran a ser tratados para la elaboración de perfiles, la información básica comprenderá asimismo esta circunstancia. En este caso, el afectado deberá ser informado de su derecho a oponerse a la adopción de decisiones individuales automatizadas que produzcan efectos jurídicos sobre él o le afecten significativamente de modo similar, cuando concurra este derecho de acuerdo con lo previsto en el artículo 22 del Reglamento (UE) 2016/679.

3. Cuando los datos personales no hubieran sido obtenidos del afectado, el responsable podrá dar cumplimiento al deber de información establecido en el artículo 14 del Reglamento (UE) 2016/679 facilitando a aquel la información básica señalada en el apartado anterior, indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información.
En estos supuestos, la información básica incluirá también:
a) Las categorías de datos objeto de tratamiento.

b) Las fuentes de las que procedieran los datos"

Por otro lado, la LOPD divide en dos grupos los datos que se deberán de aportar necesariamente al afectado, basándose en el modo en que han sido obtenidos:

a) Cuando los datos se obtengan del afectado
    a. Identidad del responsable del tratamiento y del representante.
    b. Finalidad del tratamiento.
    c. Los derechos establecidos en los artículos 15 a 22 del RGPD (Derecho de acceso al interesado, de rectificación, de supresión, a la limitación del tratamiento, derecho a la portabilidad de los datos, derecho de oposición y decisiones individuales automatizadas, incluida la elaboración de perfiles).

b) Cuando los datos personales no se hayan obtenido del afectado
    a. La Información del punto anterior
    b. Las categorías de datos
    c. Las fuentes de los datos

2.2.9. Deber de información previa a los representantes de los trabajadores

Si bien es cierto que "cuando se establezca en su caso"[24] el deber de informar a los representantes de los trabajadores no deja claro los supuestos en que deben de ser informados, podemos ver como el derecho fundamental de protección de datos también contiene un deber de información colectivo cuando se reconoce no solo por ley, sino también por la negociación colectiva.

La AEPD señala que los representantes de los trabajadores deberán de ser informados sobre la introducción de nuevos sistemas de registros de datos que afecten al conjunto de los trabajadores.

Además, según el artículo 64 del ET, donde en su apartado 1 nos dice *que "El comité de empresa tendrá derecho a ser informado y consultado por el empresario sobre aquellas cuestiones que puedan afectar a los trabajadores, así como sobre la situación de la empresa y la evolución del empleo en la misma, en los términos previstos en este artículo"* y en el 5: "*El comité de empresa tendrá derecho a emitir informe, con carácter previo a la ejecución por parte del empresario de las decisiones adoptadas por este, sobre las*

[24] Artículo 89.1 LOPD

siguientes cuestiones (…) f) La implantación y revisión de sistemas de organización y control del trabajo, estudios de tiempos, establecimiento de sistemas de primas e incentivos y valoración de puestos de trabajo", podemos concluir que es suficiente soporte legal como para que se derive la obligación del empresario de informar a los representantes de los trabajadores sobre la instalación de los aparatos de grabación.

2.2.10. Los Derechos ARCO.

Los llamados "Derechos ARCO" son aquellos derechos personalísimos a través de los cuales una persona física puede ejercer el control sobre sus datos personales, evitando así que su información personal pueda ser tratada sin límites.

Estos derechos los encontramos desarrollados en la LOPD y en el REPD:

1) Acceso: (artículos 15 del REPD y 13 de la LOPD), y podemos definirlo como el derecho del afectado a saber qué datos están siendo objeto de tratamiento, su finalidad y el origen, así como las comunicaciones realizadas o previstas por los mismos.

En relación con este derecho, el TS[25] estima que no es un derecho absoluto y por lo tanto justifica que la empresa comunique datos personales de los trabajadores a los representantes legales o sindicales para que ejerzan las competencias otorgadas por la ley.

2) Rectificación (artículos 16 REPD Y 14 LOPD): es el derecho del interesado a que se modifiquen, sin dilación indebida, los datos personales inexactos o inadecuados, debiendo de introducir en la solicitud de rectificación a qué datos se refiere y la corrección que haya de realizarse.

3) Cancelación/Derecho al olvido (artículos 17 REPD y 15 LOPD): derecho a que se supriman los datos que:

    a. No sean necesarios con los fines para los que se obtuvieron,

    b. El interesado retire el consentimiento,

    c. Se oponga con arreglo a su situación particular (derecho de oposición regulado en el artículo 21 del REPD).

[25] STS 7 febrero 2018, rec. 78/2017 (RJ 2018, 740)

d. Hayan sido tratados ilícitamente

e. Hayan de suprimirse para el cumplimiento de una obligación legal establecida por el derecho comunitario o de los estados miembros.

f. Se hayan obtenido en relación con los servicios de la sociedad de la información con las condiciones aplicables al consentimiento del niño.

Ahora bien, estos datos no serán suprimidos en los siguientes términos:

i. Para ejercer el derecho a la libertad de expresión e información.

j. Por razones de interés público en el ámbito de la salud pública

k. Con fines de archivo en interés público, de investigación científica o histórica, fines estadísticos que obstaculizasen el objetivo del tratamiento.

l. Para la formulación, ejercicio o defensa de reclamaciones.

4) Derecho de oposición (artículos 21 REPD y 18 LOPD): es aquel derecho que tiene el interesado a que no se lleve a cabo el tratamiento de datos de carácter personal o se cese en el mismo, sobretodo en los casos de mercadotecnia directa.

Encontramos conveniente hacer referencia a otros derechos que tiene el interesado:

1. Derecho a la limitación del tratamiento (artículos 18 REPD y 16 LOPD) de los datos cuando:

   a. El interesado impugne la exactitud de los datos personales

   b. El tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de uso

   c. Ya no sean necesarios para el fin del tratamiento.

   d. El interesado se haya opuesto mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.

2. Derecho a la portabilidad (artículos 20 REPD y 17 LOPD): derecho a que el interesado reciba los datos personales que le incumban y a transmitirlos a otro responsable del tratamiento.

3. Derechos relacionados con decisiones individuales automatizadas, incluida la elaboración de perfiles (artículos 22 REPD) según el cual el interesado tendrá derecho a no ser objeto de na decisión basada únicamente en el tratamiento automatizado salvo por celebración o ejecución de un contrato entre el interesado y un responsable del tratamiento autorizada por el derecho comunitario o el de los Estados miembros.

3. MECANISMOS DE CONTROL EMPRESARIAL.

3.1. Control del uso de medios informáticos de titularidad empresarial.

3.1.1. Concepto y regulación.

Ante el avance tecnológico y la introducción en el ámbito laboral de las nuevas tecnologías, nos debemos plantear la evolución del equilibrio entre el interés legítimo del empresario de proteger su empresa y la expectativa razonable de confidencialidad de los trabajadores[26].

Podemos encontrar una regulación de esta materia en el artículo 87 de la LOPD, "el derecho a la intimidad en el uso de los dispositivos digitales", y es que, en este sentido, vamos a hacer referencia a los límites del uso de dispositivos digitales puestos a disposición del trabajador por parte del empresario tales como ordenadores, teléfonos, tabletas, etc.; y, para ello, debemos de resolver dos cuestiones fundamentales:

a) Cuáles son los límites fundamentales del uso de fines privados de los dispositivos digitales de titularidad empresarial por parte del trabajador.

b) Cuáles son los límites de intervención de esos dispositivos informáticos por parte del empresario derivado de su poder empresarial.

El primer apartado del artículo 87 LOPD consiste en el reconocimiento del derecho a la intimidad; en su segundo apartado, donde se declara el derecho del empleador a acceder

[26] Dictamen 2/2017 sobre el tratamiento de datos en el trabajo (8 de junio 2017). Grupo de Trabajo sobre Protección de Datos del artículo 29, pág.4.

a los medios digitales facilitados a los trabajadores, y el tercer apartado hace referencia al procedimiento que debe de seguir el empresario para un control legítimo.

En cuanto a los derechos que entran en juego en esta materia, nos encontramos con tres derechos fundamentales: el derecho a la intimidad personal (artículo 18.1 CE); derecho a la protección de datos personales (artículo 18.4 CE) y el derecho al secreto de las comunicaciones (artículo 18.3 CE); Así mismo entra en juego también el artículo 20.bis del ET tras la entrada en vigor de la LOPD, donde se han reforzado estos límites constitucionales.

3.1.2. Límites al control empresarial sobre el uso de los dispositivos digitales

En este caso, los dispositivos digitales son de titularidad empresarial, donde el trabajador no tiene ninguna facultad de uso o disfrute para uso privado, sino que la finalidad es la satisfacción de los intereses privados.

Las finalidades que puede tener el empresario para controlar los usos de los dispositivos digitales son tres (artículo 87 LOPD):

1) Comprobar el complimiento de la actividad laboral del trabajador
2) Garantizar la integridad de los dispositivos digitales
3) Comprobar que no se utilicen los dispositivos digitales para usos privados por parte del trabajador.

Puede suceder que el empresario se dirija a los dispositivos digitales con cualquiera de las dos primeras finalidades antes expuestas y que encuentre que el trabajador ha realizado un uso privado del medio informático facilitado; ante esto, la doctrina ha venido entendiendo que el empresario deberá de respetar el derecho del trabajador a la privacidad virtual[27].

3.1.3. Jurisprudencia del TEDH

3.1.3.1. *Caso Barbulescu II contra Rumanía*[28]

Este caso que vamos a analizar procede de la jurisprudencia del Tribunal Europeo de Derechos Humanos (en adelante "TEDH"), donde el demandante trabaja para una empresa privada como ingeniero de ventas y creó una cuenta en Yahoo! Messenger para

[27] ORELLANA CANO, A.M: "*El derecho a la protección de datos personales como garantía de la privacidad de los trabajadores",* Aranzadi. Madrid 2019 *cit.,* pág. 160.
[28] STEDH "*Caso Barbulescu II vs Rumanía"* núm. 2017/61 de 5 de septiembre de 2017.

tratar con clientes, pero que usó también para fines personales, habiendo en el reglamento de la empresa una prohibición de uso para fines personales de los recursos de la empresa; ahora bien, el reglamento no hacía mención alguna sobre la posibilidad de la empresa de vigilar las comunicaciones de los empleados.

El demandante fue despedido tras la supervisión de las conversaciones que mantenía en Yahoo! con fines personales y demandó a la empresa ante los tribunales nacionales que, tras ver sus pretensiones fallidas entendiendo el demandante que se trata vulneración de su derecho al secreto de las comunicaciones y el derecho a la intimidad por parte de los tribunales nacionales y por el mismo TEDH, llegó hasta la Gran Sala del TEDH, donde vio satisfecha su pretensión.

Tras esta gran sentencia, donde vemos que entra en conflicto el poder de vigilancia del empresario y los derechos fundamentales del trabajador, alegando este la vulneración del artículo 8 del CEDH, nació el Test Barbulescu de Garantía de la Privacidad (TBGP), siendo de obligatoria aplicación en la vigilancia del empresario a los empleados y este consiste en lo siguiente:

i. Comprobar si la vigilancia se ha hecho con conocimiento del trabajador, habiendo sido informado este previamente de las medidas de vigilancia a adoptar, incluyendo su alcance y el grado de intromisión en la vida privada del trabajador.

ii. Obligación de someter el control al test de proporcionalidad, identificando un motivo legítimo que justifique dicha vigilancia y que, cuanto mayor sea el grado de control, mayor fuerza deberá de tener la justificación; debiendo de valorar si se podría haber utilizado otra medida menos lesiva para llegar a tal fin y si tal medida ha resultado útil para alcanzar el objetivo perseguido.

Esta sentencia tiene gran impacto en los derechos afectados por el control de las comunicaciones, pues el TEDH confirma que hay que tener en cuenta no solamente el derecho a la intimidad y al secreto de las comunicaciones, sino también al derecho fundamental de protección de datos personales, pues la vigilancia del trabajador implica una recogida y tratamiento de sus datos.

Otra de las cuestiones que se destaca, en este caso, es la limitación al uso del criterio de la expectativa de derecho que se usa para enjuiciar las medidas empresariales que afectan a los derechos fundamentales.

En relación con el criterio de la expectativa del derecho, el TS[29] declaró en 2007 que: *"existe un hábito social de tolerancia con ciertos usos personales moderados de los medios informáticos y de comunicación facilitados por la empresa (….) esta tolerancia crea también una expectativa general de confidencialidad en esos usos; expectativa que no puede ser desconocida, aunque tampoco convertirse en un impedimento permanente de control empresarial",* por lo que el trabajador no puede exigir expectativa alguna de intimidad si ha sido informado previamente de los controles para supervisar su actividad laboral. Ahora bien, en 2011, el TS[30] fue reduciendo esa expectativa hasta el punto de que los trabajadores podían prever la revisión de sus correos electrónicos cuando el empresario establezca reglas absolutas que prohíban el uso del correo electrónico para usos personales, pudiendo así la empresa comprobar que se cumple dicha prohibición, desapareciendo así la expectativa de la intimidad o confidencialidad.

Ante este criterio, el TC[31] también se ha pronunciado, declarando que, en primer lugar, ante la instalación de un programa de uso común por parte de las empleadas, anula cualquier expectativa de intimidad en ese programa y, en otra sentencia posterior[32], expone que no es necesario informar directamente al trabajador, sino que basta con que se prevea en el Convenio Colectivo para romper la expectativa de confidencialidad con respecto a sus comunicaciones en relación al correo. A esta doctrina del TC se le denomina "revocación suave de las garantías de los derechos fundamentales del trabajador"[33], de tal manera que el derecho fundamental a la intimidad y al secreto de las comunicaciones no se modulan frente al poder de dirección sino ante las pautas impartidas por el empresario.

Por lo tanto, queda en contradicción la doctrina del TC con la del TEDH que, según esta última, sí que es necesario que haya una comunicación previa de que las comunicaciones van a ser controladas y su prohibición para usos personales para que quede desvirtualizada la expectativa de la intimidad o confidencialidad del trabajador; incluyendo además que los tribunales nacionales deberán de verificar si el empresario ha transmitido una información

[29] STS 26 de septiembre de 2007, núm. 1097/2005 (ES:TS:2007:8599).
[30] STS 6 de octubre de 2011, núm. 4053/2010 (ES:TS:2011:8876)
[31] STC 241/2012 de 17 de diciembre (nº recurso 7304/2007)
[32] STC 170/2013 de 7 de octubre. (nº recurso 2907/2011)
[33] BAYLOS GRAU, A., "La protección de los derechos fundamentales por el Tribunal Constitucional español: auge y declive de la función de tutela", *RDS*, núm. 69, pág. 28.

transparente, concreta y precisa de la naturaleza y alcance de la vigilancia, incluyendo además una valoración del test de proporcionalidad.

Consecuentemente al impacto de esta doctrina del TEDH, podemos decir que, como conclusión, nos encontramos con los siguientes requisitos en los casos de vigilancia empresarial:

1) La intimidad debemos de interpretarla en sentido amplio, no solamente en sentido estricto en relación con la vida privada sino más allá, teniendo en cuenta las relaciones sociales.
2) Necesidad de información previa al trabajador sobre las medidas vigilancia, su naturaleza, características y finalidad.
3) La notificación de la prohibición del uso del correo electrónico ha de ser clara concreta y precisa, al igual que en el uso del mecanismo de control y vigilancia.

4) Los mecanismos de control empresariales dirigidos al contenido de las comunicaciones deberán de ser sometidos a un control de proporcionalidad más intenso.
5) Justificar expresamente los motivos del uso de las medidas de vigilancia, debiendo de ser motivos concretos, reales y precisos, más allá de la alusión al control empresarial del artículo 20.3 ET.
6) La normativa interna de las empresas no puede reducir totalmente la vida privada social del trabajador, quedando siempre una expectativa de privacidad, aunque exista una prohibición expresa y reiterada del uso de los medios informáticos con fines personales.

3.1.3.2. Caso Libert contra Francia[34]

En este caso nos encontramos con la existencia de una negociación de los protocolos para el uso de los dispositivos digitales donde se permite el uso con fines privados de los medios informáticos, debiendo de diferenciar dos tipos de archivos, los profesionales y los privados, y el empresario solo puede controlar los archivos profesionales, salvo "riesgo o acontecimiento especial" donde se habilitaba poder introducirse en los archivos privados.

[34] STEDH "*Caso Libert vs Francia"* 22 de febrero de 2018 (TEDH/2018/35)

En concreto, uno de los trabajadores tenía una carpeta llamada "risas" en la unidad "D:/datos personales" y la empresa se introdujo en dicha carpeta, constatando la transgresión de la buena fe contractual.

El TEDH declaró que el protocolo no es contrario al artículo 8 CEDH, y que la sanción impuesta tampoco es contraria al mismo artículo.

3.1.4. Jurisprudencia del TS

3.1.4.1. Asunto Inditex[35]

Este caso versa sobre el despido de un trabajador de Inditex, el cual recibe cierta cantidad de dinero de una proveedora y la empresa tuvo conocimiento de ello tras encontrarse "casualmente" una serie de facturas provenientes de la compra de un Mercedes X6 y la posterior revisión de los correos electrónicos del trabajador.

En la empresa existía una prohibición de la utilización de los ordenadores con fines personales, restringiendo su uso a fines laborales. Y el trabajador considera que las pruebas obtenidas vulneran su derecho a la intimidad.

Ante esto, el TS declaró que el trabajador había tenido conocimiento del control que podía ejercer el empresario y que la empresa tenía un interés legítimo para actuar, incluyendo en su dictamen que el grado de intromisión fue el menor posible; y, para ello, se basó en los siguientes argumentos:

a) La empresa limitó expresamente el uso de los ordenadores con fines laborales, prohibiendo su uso para fines privados.
b) Cada vez que el trabajador accedía a su ordenador, era informado de la política de seguridad de información y se le advertía de las medidas de control y vigilancia.
c) El "hallazgo casual" de las facturas del coche fue el motivo por el que la empresa realizó medidas de control.
d) El examen de los correos electrónicos fue mediante la búsqueda de palabras clave, no realizándose así de manera genérica ni indiscriminada.

Por lo que, como podemos ver, esta sentencia del TS aporta unos criterios que coinciden con la doctrina del TEDH.

[35] STS 8 de febrero de 2018 (JUR 2018/58399)

3.1.5. Jurisprudencia del TC

3.1.5.1. STC 170/2013 de 7 de octubre[36].

El presente caso consiste en un recurso de amparo ante una sentencia del TSJ de Madrid, por considerar errónea la interpretación que da este tribunal respecto a la licitud de la admisibilidad de las pruebas de una empresa, alegando el trabajador una vulneración del derecho a la intimidad personal y al secreto de las comunicaciones.

El demandante, siendo este trabajador de la empresa Alcaliber SA, entiende que la entidad para la que trabajaba se había extralimitado en sus facultades de fiscalización, pues interceptó de forma ilícita el contenido de sus correos electrónicos registrados en el ordenador (siendo este de titularidad empresarial), y sin haber sido informado previamente.

La empresa, alega que no interceptó los mensajes en el proceso de comunicación, sino con posterioridad, negando así la vulneración del derecho al secreto de las comunicaciones y, además, que tampoco hay vulneración del derecho a la intimidad, puesto que los correos interceptados se refieren al incumplimiento del deber de reservar secretos de la empresa. Por último, también fundamenta su defensa en que el trabajador era consciente de la prohibición convencional del uso no profesional del correo electrónico y que su utilización podía quedar sujeta al control empresarial.

El TC, fundamenta, en relación con la vulneración del derecho de secreto de las comunicaciones:

- STC 241/2012[37], según la cual:
  - *"no cabe duda de que es admisible la ordenación y regulación del uso de los medios informáticos de titularidad empresarial por parte del trabajador, así como la facultad empresarial de vigilancia y control del cumplimiento de las obligaciones relativas a la utilización del medio en cuestión, siempre con pleno respeto a los derechos fundamentales".* (FJ 4).
  - *"los grados de intensidad o rigidez con que deben ser valoradas las medidas empresariales de vigilancia y control son variables en función de la propia configuración de las condiciones de disposición y uso de las herramientas informáticas y de las instrucciones que hayan podido ser impartidas por el empresario a tal fin".* (FJ4).
  - *"no podía existir una expectativa razonable de confidencialidad derivada de la utilización del programa instalado"* (FJ 5).

[36] STC 170/2013 de 7 de octubre (Recurso de amparo 2907/2011)
[37] STC 241/2012 de 17 de diciembre (Recurso de amparo 7304/2007)

- Basado en los argumentos anteriores y en el Convenio Colectivo de la industria química, el TC declaró que no hay vulneración del derecho al secreto de las comunicaciones, pues se *"llevó pues a cabo a través de un canal de comunicación que, conforme a las previsiones legales y convencionales indicadas, se hallaba abierto al ejercicio del poder de inspección reconocido al empresario; sometido en consecuencia a su posible fiscalización, con lo que, de acuerdo con nuestra doctrina, quedaba fuera de la protección constitucional del art. 18.3 CE."(* FJ 4), descartando así la lesión de dicho derecho.

  Por otro lado, el TC argumenta lo siguiente en relación con la vulneración del derecho a la intimidad:

- STC 173/2011[38], donde se dice que el cúmulo de información que se almacena por su titular en un ordenador, forma parte del ámbito de la intimidad constitucionalmente protegido.
- STEDH (Asunto Copland vs Reino Unido)[39], donde *"los correos electrónicos enviados desde el lugar del trabajo» están incluidos en el ámbito de protección del art. 8 del Convenio europeo para la protección de los derechos humanos y de las libertades fundamentales, por cuanto pueden contener datos sensibles que afecten a la intimidad y al respeto a la vida privada"* (§§ 41 y 44).

Finalmente, el TC considera que, tras analizar el triple juicio de proporcionalidad del caso, rechaza que se haya lesionado también el derecho a la intimidad; por lo que el TC desestimó el recurso interpuesto.

3.1.6. Diferencia entre el uso dispositivo de titularidad privada y de titularidad empresarial durante la actividad laboral.

Lo que nos interesa en este apartado es diferenciar los límites que tiene el empresario dependiendo de si el medio informático utilizado para la actividad laboral es de titularidad privada o, de lo contrario, de titularidad empresarial.

En primer lugar, hemos de entender que el artículo 87.2 de la LOPD otorga al empresario el derecho de acceso a los medios digitales facilitados por él a los trabajadores para controlar la actividad laboral, pero no hace referencia alguna a aquellos que son de titularidad del trabajador. Por lo que, en este caso, parece que el empresario no tendría

[38] STC 173/2011, de 7 de noviembre (ECLI: ES:TC:2011:173)
[39] STEDH "*Asunto Copland VS Reino Unido"* 3 de abril de 2007 (núm. 62617/2000)

derecho a acceder a dichos dispositivos. Ahora bien, el artículo 20.3 del ET, otorga al empresario la facultad de adoptar las medidas que estime de vigilancia y control en relación con los derechos y deberes del trabajador.

El TS[40], desde la perspectiva penal, ha señalado que es irrelevante que la titularidad del dispositivo sea del trabajador o del empresario, es decir, la titularidad real, sino que hay que atender a quién sea el usuario, por lo que el GT29[41] recomienda que, en estos casos, el trabajador debe de adoptar ciertas medidas para diferenciar bien entre el uso privado y el uso dedicado a la actividad laboral del medio digital.

En contra posición con lo anterior, desde la perspectiva laboral, la AN[42] entiende que el acceso por el empresario a un dispositivo de titularidad del trabajador conllevaría un abuso de poder.

Ante este debate, seguimos la opinión de Fco. Javier Fernández Orrico, y entendemos que en ciertos casos sí que cabe un control por parte del empresario en los dispositivos de titularidad privada pero solamente en aquellos casos que sean para controlar el cumplimiento de la actividad laboral, descartando cualquier justificación por motivo de controlar la integridad de los dispositivos ni controlar carpetas u otros elementos pertenecientes al dispositivo.

3.2. Videovigilancia

3.2.1. Concepto y regulación.

Antes de la entrada en vigor de la actual LOPD, existía un contexto de inseguridad jurídica debido al gran peso que tenían los tribunales (TS, TC y TEDH) de regular esta materia por la falta de regulación legal. Más tarde, con la entrada en vigor de la LOPD en el 2018, ya encontramos una regulación más extensa como un desarrollo del artículo 20.3 del ET sobre las medidas de control y vigilancia del empresario para verificar el cumplimiento de las obligaciones del trabajador.

La videovigilancia la encontramos regulada en el artículo 89 de la LOPD, donde se reconoce el derecho de los empresarios a tratar las imágenes obtenidas a través de sistemas

[40] STS 489/2018, 23 de octubre (RJ 2018, 4937)
[41] GT29 2/2017, pág., 8.
[42] SAN 6 de febrero de 2019 (AS 2019, 905)

de cámaras o videocámaras para el ejercicio de las funciones de control de los trabajadores o los empleados públicos.

Según la Disposición Final Primera de la LOPD, el artículo 89 de la misma ley tiene naturaleza de ley orgánica y, como tal, desarrolla derechos fundamentales, en concreto el derecho a la intimidad del trabajador; ahora bien, aunque no hace mención expresa al derecho a la protección de datos, encontramos el artículo 2.1 de la LOPD, donde nos vincula tal medida de vigilancia y control con el derecho a la protección de datos y, según el artículo 22.1 LOPD, dicho tratamiento de imágenes se realizará "con la finalidad de preservar la seguridad de las personas y bienes, así como de sus instalaciones".

3.2.2. Límites.

El artículo 89 de la LOPD establece que las funciones de control se deben ejercer "dentro de su marco legal y con los límites inherentes al mismo", siendo estos límites:

a) El respeto al principio de proporcionalidad, necesidad e idoneidad del sistema.

En este sentido, la AEPD[43] se ha pronunciado defendiendo dicho criterio como elemento fundamental en el uso de tales medidas de vigilancia y control. Hemos de decir que, esta medida no será admisible en general para las empresas como sistema permanente y continuado de control[44].

b) Los empresarios deberán de informar con carácter previo y de forma expresa, clara y concisa, a los trabadores y, en su caso, a sus representantes legales. (artículo 89.1).

Se requiere que el trabajador sea consciente de que le están observando, no requiere su autorización, sino que sea informado de ello, con la finalidad de controlar su actividad laboral; a parte de ello, debe de ser expresa, es decir, no puede ser obtenida por medios indirectos o implícitos como a través de sus compañeros de trabajo, debe de ser transmitida sin intermediarios[45]; debe de ser clara y concisa, sin que le quepa duda alguna al trabajador de que le están vigilando. Por último, debe de ser también transmitida a los representantes

[43] AEPD Informe 0495/2009.
[44] MERCADER UGINA, Jesús Rafael, *Protección de datos y garantía de los derechos digitales en las relaciones laborales.* Madrid, 2019.
[45] Fernández Orrico, Fco. Javier., "*Criterios sobre usos de dispositivos tecnológicos en el ámbito laboral: hacia el equilibrio entre el control empresarial y la privacidad del trabajador".* Universidad Miguel Hernández. 2021.

de los trabajadores, de manera que no se transmita a direcciones particulares de los trabajadores ni a sus móviles privados[46], debiendo informar también del tipo de tecnología empleada.

c) Prohibición de la instalación de sistemas de videovigilancia en lugares destinados al descanso o esparcimiento de los trabajadores tales como vestuarios, aseos, comedores, y análogos. (artículo 89.2), siendo este un límite absoluto

3.2.3. Caso de Fragante delito.

Es una excepción a la norma general, regulada en el artículo 89.1 de la LOPD, donde el único requisito que se exige para que la prueba obtenida a través de una cámara de videovigilancia sea válida es el regulado en el artículo 22.4 de la LOPD, es decir, "la colocación de un dispositivo informativo en lugar suficiente visible identificado, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos en los artículos 15 a 22 del Reglamento (UE) 2016/679" en caso de que nos encontremos en un la comisión flagrante de un acto ilícito.

Ahora bien, debemos de saber a qué se refiere con "acto ilícito" el legislador, y es que dependiendo de a qué sentido se refiere, dicha prueba puede tener relevancia o no a efectos penales[47], y es que, si nos guiamos por una interpretación literal y/o histórica, nos lleva a entender que se trata de un acto ilícito penal, pues según Eduardo Taléns[48], tendría valor probatorio en el proceso penal, pues no tendrían valor para una sanción laboral; pero desde el punto de vista de la tramitación parlamentaria de la LOPD, nos lleva a una interpretación contraria[49]; por lo que debemos de diferenciar de si se queda limitado a proteger a las personas y cosas, es decir, por motivos de seguridad o, de lo contrario, debemos de considerarlo obtenido lícitamente según el artículo 90.2 LRJS[50]. Para ello, nos debemos de

---

46 AEPD. *Fichas prácticas de videovigilancia. VI. "Cámaras para el control empresarial", cit.*

47 LÓPEZ BALANGUER, MERCEDES y RAMOS MORAGUES, FRANCISCO: "*Control empresarial del uso de dispositivos digitales en el ámbito laboral desde la perspectiva del derecho a la protección de datos y a la intimidad"*. Universidad de Valencia, 2020. Vol. 10. Núm. 2. Págs 529.

48TALÉNS VISCONTI, Eduardo., *"Vídeo-vigilancia y protección de datos en el ámbito laboral."*.vol. 6. Núm. 3. Pág. 57-85.

49 Serrano Olivares, Raquel. «Los derechos digitales en el ámbito laboral: comentario de urgencia a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales». *IUSLabor. Revista d'anàlisi de Dret del Treball*, [en línea], 2018, n.º 3,

50Artículo 90.2 de la Ley 36/2011, de 10 de octubre, reguladora de la jurisdicción social: *"No se admitirán pruebas que tuvieran su origen o que se hubieran obtenido, directa o indirectamente, mediante procedimientos que supongan violación de derechos fundamentales o libertades públicas (…)"*

basar en el artículo 22.1 de la LOPD, donde se establece la finalidad del tratamiento de las imágenes obtenidas a través de cámaras o videocámaras, y es la de "preservar la seguridad de las personas y bienes, así como de sus instalaciones".

Además, el TS también se pronunció sobre esto, y dictamina que la obtención de pruebas de las cámaras de seguridad no impuestas para el control laboral es ""una medida justificada por razones de seguridad (control de hechos ilícitos imputables a empleados, clientes y terceros, así como rápida detección de siniestros), idónea para el logro de ese fin (control de cobros y de la caja en el caso concreto) y necesaria y proporcionada al fin perseguido, razón por la que estaba justificada la limitación de los derechos fundamentales en juego, máxime cuando los trabajadores estaban informados, expresamente, de la instalación del sistema de vigilancia, de la ubicación de las cámaras por razones de seguridad, expresión amplia que incluye la vigilancia de actos ilícitos de los empleados y de terceros y en definitiva de la seguridad del centro de trabajo pero que excluye otro tipo de control laboral que sea ajeno a la seguridad, esto es el de la efectividad en el trabajo, las ausencias del puesto de trabajo, las conversaciones con compañeros, etc."[51]

Por lo que debemos de diferenciar dos tipos de obligaciones del trabajador:

a) En primer lugar, aquellas relacionadas con las condiciones de trabajo ordinarias, cuyo incumplimiento detectado por una cámara no identificada e informada vulneraría el derecho fundamental a la intimidad, de tal manera que no podría ser sancionada de manera lícita.

b) En segundo lugar, aquellas relacionadas con el cumplimiento del deber de buena fe contractual respecto de la protección de las personas o de las cosas, cuyo incumplimiento detectado de la misma forma anterior, sí que podrá ser sancionada de manera lícita.

En cuanto al carácter flagrante de la comisión del delito, podemos interpretarlo de dos maneras diferentes:

[51]STS 77/2017 de 31 de enero de 2017, REC 3331/2015. (ES:TS: 2017:654)

i) Interpretación restrictiva, según la cual no existe ninguna sospecha de que se esté cometiendo un acto ilícito, pero aun así es captada la comisión del acto ilícito por las cámaras identificadas y no informadas.

ii) Interpretación más amplia por la que las cámaras identificadas y no informadas captan la comisión de un acto ilícito, pero del que ya se tenían sospechas fundadas por determinados indicios o irregularidades.

En ambos casos, la prueba se considerará legítima pues, en el primero, el TS[52] declaró que las cámaras sugieren "una finalidad protectora del patrimonio empresarial y la grabación de conductas que atenten contra esa finalidad"; y en el segundo caso, la sospecha fundada de que se está cometiendo un acto ilícito es suficiente para la justificación de la colocación de cámaras identificadas y no informadas.

3.2.4. Cámaras no identificadas y no informadas (Cámaras ocultas).

Hasta ahora, hemos desarrollados los supuestos en que las cámaras se encontraban identificadas o identificables, pero no habían sido informados los trabajadores de su existencia. En este apartado, nos vamos a centrar en sí es lícito colocar cámaras ocultas, es decir, cámaras que no estén identificadas y que no se hayan informados ni a los trabajadores ni a los representantes legales de los trabajadores de su existencia en el puesto de trabajo y, si las pruebas que se obtienen al captar un acto ilícito serían pruebas válidas.

En un principio, podemos entender tras una lectura del artículo 22.4 LOPD que estas cámaras no son admisibles, pues como mínimo se exige al empresario que se identifiquen las cámaras con un cartel informativo; ahora bien, hemos de fijarnos en la doctrina del TEDH donde se reconoce la admisibilidad de este tipo de vigilancia con ciertas condiciones.

A continuación, vamos a exponer diferentes sentencias de los Altos Tribunales, debiendo de tener en cuenta que las Sentencias de los tribunales españoles son anteriores a la LOPD, mientras que las del TEDH son más tardías, por lo que estamos a la espera de nuevas sentencias del TS y TC, pudiendo ver recogen la jurisprudencia del TEDH.

[52] STS 7 de julio de 2016, REC 3233/2014. (ES:TS: 2016:4070).

3.2.5. Jurisprudencia del TEDH

3.2.5.1. Caso López Ribalda y otros contra España.[53]

En primer lugar, encontramos el *Caso López Ribalda y otros contra España*, según el cual en una reunión de un supermercado se informó al personal de que se iba a realizar una instalación de cámaras visibles por indicios de robos, pero además se instalaron cámaras ocultas, cosa que no fue transmitido al personal. Tras la instalación de ambas cámaras, se captó por las cámaras ocultas el robo, por parte de varios empleados, de bienes en las cajas del supermercado, y fueron despedidos con motivos disciplinarios catorce empleados, sin permitir a ninguno de ellos visualizar las grabaciones que captaron el acto ilícito cometido y, cinco de ellos demandaron a la empresa por no cumplir con el deber de información requerido por la legislación vigente, declarando una vulneración del respeto a la vida privada garantizado por el artículo 8 del CPDHLF. El TEDH acabó admitiendo la videovigilancia con cámara oculta, pero condicionada:

- Aplicación de la doctrina Barbulescu II mutantis mutandis, es decir, se aplica el test Barbulescu incorporando preguntas sobre la proporcionalidad, necesidad e idoneidad en la videovigilancia: (apartado 116).

1) Si se ha notificado al empleado la posibilidad de que el empleador adopte medidas de videovigilancia y aplicación de esas medidas.

2) Alcance de la vigilancia por el empleador y el grado de intrusión en la vida privada, debiendo de tenerse en cuenta el nivel de privacidad de la zona vigilada.

3) Justificación razonada, directamente proporcional al grado de intrusión en la vida privada.

4) Si se podría haber evitado utilizando medios menos intrusivos.

[53] STEDH "*Caso Ribalda y otros vs España"* 17 de octubre de 2019 (Nº 1874/13 y 8574/13)

5) Hay que tener en cuenta la utilización por el empleador de los resultados obtenidos y si esos resultados se han utilizado para lograr el objetivo declarado de la medida.

6) Si se ha proporcionado al empleado las medidas apropiadas, sobre todo cuando esas medidas son de carácter intrusivo (como información, alcance de la vigilancia, etc.).

- Hay que tener en cuenta diferentes ámbitos:
  - Espacial, pues el tribunal considera que hay que distinguir los distintos lugares en que se lleva a cabo la vigilancia, pues en los lugares de carácter privado debe de haber una mayor protección o incluso una prohibición de esta medida, como por ejemplo en los vestuarios. De tal manera que la protección será menor en lugares visibles o accesibles a los compañeros o al público en general (apartado 125).

  - Temporal: en este caso, la duración de la videovigilancia oculta tuvo una duración de 10 días, declarando el tribunal que no era excesiva, incluso en el caso Köpke, se consideró también que no era excesiva una duración de 14 días. (apartado 126).

  - Subjetivo: en este caso se entiende que los empleados fueron despedidos debido a las imágenes obtenidas por las grabaciones y, además, no fueron utilizadas para ningún otro fin nada más que para encontrar a los responsables de las pérdidas de los bienes y adoptar las medidas disciplinarias contra ellos. (apartado 127).

- El Tribunal considera que son de carácter fundamental el requisito de transparencia y el derecho de información en las relaciones laborales, evitando así todo posible abuso por parte del empresario, pero que son criterios que deben de considerarse al valorar la proporcionalidad de la medida yendo caso por caso,

pues si falta esa información, las garantías de los demás criterios serán más importantes (apartado 131).

- El Tribunal estima que "la injerencia en la privacidad de las demandantes era proporcionada (…) si bien no puede aceptar la proposición de que la más mínima sospecha de apropiación indebida o de cualquier otro acto ilícito por parte de los empleados podría justificar la instalación de una videovigilancia encubierta por parte del empleador", por lo que deben de ser "graves irregularidades" y debe de valorarse el alcance de los robos para que sea una justificación suficiente como para adoptar tal medida. (apartado 134).

3.2.6. Jurisprudencia del TS

3.2.6.1. STS 7 de julio de 2016 (RJ 2016/4434)[54]

En este caso nos encontramos con la instalación de cámaras de vigilancia en una tienda de ropa bajo sospecha de que la trabajadora hurtaba prendas. Las cámaras fueron instaladas sin informar a la trabajadora, solamente se puso un cartel informativo visible de que la zona estaba videovigilada, pudiendo así conocer los trabajadores su existencia.

El TS entendió que no se vulneraba el derecho a la intimidad y que se cumplía el principio de proporcionalidad, siendo un medio idóneo y una intervención equilibrada.

3.2.6.2. STS 2 de febrero de 2017 (RJ 2017/168)[55]

Esta sentencia versa sobre el despido disciplinario de un trabajador de un gimnasio con motivo de la mala gestión de los pagos domiciliados por los clientes, el no cumplimiento de las reuniones con los técnicos y de no realizar los informes para la dirección del club y la Dirección de fitness, dejando pasar a otros compañeros de otros clubes que no tienen permiso de acceso y a clientes que, de igual manera, deja pasar gratuitamente y, por último, el incumplimiento grave y reiterado de la jornada laboral. Todo ello fue captado por las cámaras de seguridad instaladas en la entrada y en los espacios públicos de la empresa.

[54] STS 7 de julio de 2016, RJ 2016/4434 (ES:TS:2016:3146).
[55] STS 2 de febrero de 2017, RJ 2017/168. (ECLI:ES:TS: 2020:812).

El TS rechaza que haya habido vulneración del derecho a la intimidad, considerando apropiado el uso, en este caso, de las cámaras de videovigilancia, pues el trabajador conocía de su existencia, siendo esta medida razonable y proporcionada.

3.2.7. Jurisprudencia del TC

3.2.7.1. STC 39/2016, de 3 de marzo[56]

Esta sentencia del TC trata sobre el despido a una trabajadora de un supermercado por apropiación indebida de dinero de la caja registradora, captado mediante cámaras de videovigilancia que fueron instaladas bajo la sospecha de ciertos hurtos. La controversia surge porque no se informó a la trabajadora de la colocación de las videocámaras, solamente se puso un cartel informativo diciendo "zona videovigilada" a la vista.

En este caso, el TC dictaminó que el deber de información empresarial se cumplía con el cartel informativo puesto previamente a la instalación de las cámaras, considerando que dicho cartel cumplía con el distintivo informático que exige la Instrucción 1/2006.

Ahora bien, es cierto que, algún autor entiende que este dictamen del TC hace que se devalúe el contenido esencial del derecho a la protección de datos, entendido así por el TC en su STC 292/2000 de 3 de marzo.[57]

3.2.7.2. Caso de la Universidad de Sevilla[58]

En este caso nos encontramos con un trabajador de la Universidad de Sevilla que realizaba una jornada laboral diferente a la que firmaba en las hojas de registro de la jornada laboral, según las cuales el trabajador entraba a las 8:00 y salía a las 15:00; ante las sospechas de estas irregularidades, se decidió utilizar las cámaras de seguridad instaladas en los accesos de las dependencias con la finalidad de evitar robos, para acreditar el incumplimiento del horario por parte del trabajador, controlando así las entradas y salidas del puesto de trabajo. De esta manera se le incoa un expediente disciplinario.

---

[56] STC 39/2016, de 3 de marzo (RTC 2016/39)
[57] GONZÁLEZ GONZÁLEZ, C.: "*Guía práctica sobre Protección de Datos: ámbito laboral,* cit., pág. 329.
[58] STC 29/2013 de 11 de febrero (RTC 2013/29). Nº rec. 10522/2009.

Ante esto, el trabajador decidió interponer demanda por vulneración del derecho a ser informado de la medida de vigilancia, y vulneración del derecho a la intimidad, llegando así hasta el TC, el cual entendió vulnerado este derecho por no informar al trabajador sobre esa utilidad de supervisión laboral asociadas a la captura de su imagen.

Por lo que la Sala, argumenta que:

- Hay que dar una información previa y expresa, precisa, clara e inequívoca a los trabajadores de la finalidad de control de la actividad laboral.
- Esa información debe de concretar las características y alcance del tratamiento de los datos, es decir, en qué casos las grabaciones podían ser examinadas, durante cuánto tiempo y con qué propósito.
- Se debe de informar, además, de que las imágenes captadas pueden utilizarse para la imposición de sanciones.

Estos criterios, según José Luis Goñi Sein[59], se pueden utilizar en todas las formas de vigilancia y control empresarial, incluyendo el uso de Internet y del correo electrónico.

3.2.8. Conclusiones.

Tras el estudio de la videovigilancia como mecanismo de control del empresario, podemos extraer tres conclusiones dependiendo del tipo de videovigilancia que se trate:

a) Videovigilancia como sistema de control ordinario: será necesario cumplir con los requisitos del deber de información por parte del empresario a los empleados y a los representantes legales de los trabajadores, de la existencia de las cámaras y sobre la finalidad del control de manera clara y exhaustiva, respetando los límites de la proporcionalidad, idoneidad y necesidad.

b) Videovigilancia identificada pero no informada, siendo válida cuando exista sospecha "siquiera mínima" de robos o irregularidades, quedando afectada la protección de las personas o el patrimonio de la empresa

[59] GOÑI SEIN J.L., "Los derechos fundamentales inespecíficos en la relación laboral individual: ¿necesidad de una reformulación? Primera Ponencia del XXIV Congreso Nacional de Derecho del Trabajo y de la seguridad Social, organizadas por la Asociación Española de Derecho del Trabajo y de la Seguridad Social. Pamplona, 2014. cit, pág. 74.

c) Videovigilancia no identificada y no informada (oculta): será admisible en los casos en que la sospecha sea de gran gravedad porque "atente al buen funcionamiento de la empresa" y "al clima general de desconfianza para la empresa", según el TEDH.

3.3. Grabación de sonidos

3.3.1. Concepto y regulación

La captación del sonido o de la voz de un trabajador al igual que la captación de imágenes por videocámaras, permiten identificar a personas, más aún si se adjunta a un expediente, lo que conlleva que estemos hablando de datos personales y, como vemos, queda incluida en ámbito de regulación de la LOPD[60].

Siguiendo a Susana Rodríguez Escanciano, las grabaciones de conversaciones están amparadas tanto por el derecho fundamental a la intimidad (artículo 18.1 CE), como por el derecho fundamental al secreto de las comunicaciones (artículo 18.3 CE), y únicamente mediante autorización judicial es posible una injerencia en las conversaciones; además, la captación de una conversación es más sensible que la de una imagen, puesto que las palabras pueden revelar pensamientos y sentimientos internos, pudiendo así comprobar más fácilmente el incumplimiento laboral.[61]

La grabación de sonido viene mencionada en el artículo 89.3 de la LOPD como dato especialmente protegido y, además, con una estricta limitación. A parte de ello, este artículo menciona los únicos casos en los que se podrá admitir la grabación de sonido en el lugar de trabajo o, mejor dicho, las condiciones que se deben dar:

a) Que nos encontremos ante riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad desarrollada en el centro de trabajo.

b) Respeto al principio de proporcionalidad e intervención mínima; por lo que, según el TC, las grabaciones indiscriminadas suponen una mayor intromisión en la intimidad, lo que hace que puedan llegar a ser desproporcionadas[62];

[60] AEPD Informe jurídico 497/2007.
[61] RODRÍGUEZ ESCANCIANO, Susana., "*Videovigilancia empresarial: límites a la luz de la Ley Orgánica 3/2018, de 5 diciembre, de protección de datos personales y garantía de los derechos digitales.",* 2019. Núm. 9328 op. cit., p. 6,
[62] STC 98/2000, de 10 de abril. (RTC 2000/98). Nº rec. 4015/96.

c) Respeto a las garantías de los apartados anteriores.

d) La conservación de las grabaciones de sonido será guardada como máximo durante el plazo de un mes, más tarde deberán de ser suprimidas, salvo para la acreditación de actos ilícitos. (artículo 22.3 LOPD). Si bien es cierto que este apartado hace referencia a la videovigilancia, cabe entender que también se aplica por analogía a los datos obtenidos mediante grabación de sonido.

La captación de sonidos viene regulada también en el artículo 7 de la Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen, donde considera intromisiones ilegítimas que:

1. El emplazamiento en cualquier lugar de aparatos de escucha, filmación, dispositivos ópticos u otro medio apto para grabar o reproducir la vida íntima de las personas. (apartado 1)

2. Utilización de aparatos de escucha, dispositivos ópticos, o de cualquier otro medio para el conocimiento de la vida íntima de las personas o de manifestaciones o cartas privadas no destinadas a quien haga uso de tales medios, así como su grabación, registro o reproducción. (apartado 2).

3. La revelación de datos privados de una persona o familia conocidos a través de la actividad profesional u oficial de quien los revela (apartado 4).

Ahora bien, en el artículo 89.2 de la LOPD, encontramos una prohibición absoluta sobre la instalación de sistemas de grabación de sonidos, al igual que en el caso de videovigilancia, y es en los lugares destinados al descanso o esparcimiento de los trabajadores o de los empleados públicos como pueden ser los vestuarios, comedores y análogos.

3.3.2. Jurisprudencia del TEDH

Como hemos dicho anteriormente, la grabación del sonido resulta más sensible a la de una imagen, de ahí que el TEDH –Asunto *Halford*- aclare la necesidad de que se avise al trabajador sobre la posible interceptación de los diálogos.

3.3.2.1. Caso Copland contra Reino Unido[63]

Doña Lynette Copland, interpone demanda contra Reino Unido de Gran Bretaña e Irlanda del Norte debido al seguimiento de sus llamadas telefónicas, correo electrónico y uso de internet durante su actividad laboral, alegando vulneración de los artículos 8 (Derecho al respeto a la vida privada y familiar) y 13 (Derecho a un recurso efectivo) del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales.

En este caso, el TEDH considera que las llamadas telefónicas realizadas durante la actividad laboral, se encuentran dentro del concepto de vida privada y correspondencia regulados en el artículo 8.1 del CEDH, extendiéndose a los correos electrónicos y la navegación en internet desde el lugar de trabajo.

Aun así, no se prohíbe determinados controles sobre el uso del teléfono, correo electrónico o internet en la empresa, pero parece que solamente si se realiza bajo el consentimiento del titular o si se contemplan de forma clara y expresa en una ley, de tal manera que se cumpla la exigencia de previsibilidad.

3.3.2.2. Caso Halford contra Reino Unido.

Se trata de una inspectora de policía que, tras la respuesta de una campaña del Comité de Control de la Policía contra ella por la denuncia que interpuso por discriminación, fueron grabadas y captadas las llamadas telefónicas que realizó desde su despacho de trabajo. Ante esto, llega ante el TEDH alegando una vulneración de los artículos 8 (derecho al respeto de la vida privada y familiar) y artículo 13 (derecho a un recurso efectivo) del Convenio para la Protección de los Derechos Humanos y de las libertades Fundamentales. En este caso, no hay prueba alguna de que se hubiera avisado a la demandante de que las llamadas podían ser interceptadas.

El TEDH determinó que hubo vulneración de ambos artículos y aclara la necesidad de que se avise al trabajador sobre la posible interceptación de los diálogos.

[63] STEDH "*Asunto Copland VS Reino Unido"* núm. 62617/2000, de 3 de abril de 2007.

3.3.3. Jurisprudencia del TS

3.3.3.1. Caso Unión Telefónica Sindical contra Telefónica de España SAU sobre Conflicto Colectivo[64]

En este caso se nos presenta una demanda ante el TS de Unión Telefónica Sindical de conflicto colectivo, la cual considera ilegal las escuchas practicadas por Telefónica de España SAU, pidiendo a su vez que cesen dichas escuchas y sus grabaciones sobre las conversaciones de determinados trabajadores con sus clientes.

El TS acabó desestimando el recurso planteado por UTS, fundamentando que el único objetivo de realizar dicha práctica es el control de la actividad laboral del trabajador, respetando así su derecho a la intimidad.

3.3.4. Jurisprudencia del TC

3.3.4.1. Caso la TOJA[65]

Nos podemos encontrar en una situación donde se puede producir por separado vulneraciones de los derechos fundamentales tanto por parte de la videovigilancia como por parte de la grabación de sonido, en el caso de que se solapen y se incorporen ambas, puede suponer que nos encontremos ante una doble acción sobre la protección de datos, produciendo una grave intromisión en la intimidad de los trabajadores[66]. Es el claro ejemplo de la TOJA.

Los antecedentes del caso se localizan en un casino donde se instalan sistemas audiovisuales para aumentar el control y la vigilancia. En este caso, el TC, basado en el criterio de proporcionalidad, que se trata de una medida que no es necesaria, pues su instalación "no ha sido efectuada como consecuencia de una quiebra en los sistemas de seguridad y control anteriormente establecidos, sino que se tomó dicha decisión para complementar los sistemas de seguridad ya existentes", y además que este tipo de medidas que no solamente captan las conversaciones de los trabajadores, sino también la de los clientes de manera continuada e indiscriminada, sobrepasa notoriamente las facultades que le son conferidas para la vigilancia y control provenientes del artículo 20.3 del ET, y considera

---

[64] STS 52/2003 de 5 de diciembre de 2003 (ES 2003/7798).
[65] STC 98/2000, de 19 de abril (RTC 2000/98)
[66] Fernández Orrico, Fco. Javier., "*Criterios sobre usos de dispositivos tecnológicos en el ámbito laboral: hacia el equilibrio entre el control empresarial y la privacidad del trabajador*". Universidad Miguel Hernández. 2021.

que sí que hay una vulneración del derecho fundamental a la intimidad (artículo 18.1 CE). Por lo que la mera utilidad o conveniencia de la instalación de este tipo de medidas de vigilancia y control no es legitimada.

Por lo tanto, no es argumento necesario escuchar y grabar las conversaciones privadas de los trabajadores y los clientes como medida de incremento de la seguridad, provocando una intromisión ilegítima del artículo 18.1 CE relacionado con el derecho fundamental a la intimidad, no estando conforme con los principios de proporcionalidad e intervención mínima.

3.4. Consecuencias.

Como podemos ver, parece que está mucho más limitada la captación y/o grabación de sonidos que las de imágenes, pues para que sea lícita una prueba de grabación de sonidos es necesario demostrar que:

a) Hay una justificación legítima reforzada y limitada a la seguridad.
b) El sistema que se utiliza es la medida menos invasiva posible.

3.5. Supuestos especiales.

En este caso nos centramos en supuestos de emergencias, como puede ocurrir en un accidente de aeronave o ferroviario, de tal manera que se estudian las grabaciones de sonido para esclarecer los hechos y así que los investigadores puedan resolver las causas del accidente para que no se vuelvan a repetir en un futuro. En ambos casos nos referimos al estudio de las cajas negras.

Analizando un caso concreto, el accidente del Alvia producido el 24 de julio de 2013 cerca de la estación de Santiago de Compostela, se abrieron las dos cajas negras del tren, pudiendo así comprobar que dos minutos antes del accidente el maquinista recibió una llamada de trabajo y activó los frenos pasando de 192 Km/h a 153 KM/h.

La AEPD[67] entendió que, en estos casos, las grabaciones de las conversaciones en este tipo de situaciones, son una medida necesaria para garantizar la seguridad y para investigar los hechos que dan lugar al accidente.

[67] AEPD Informe jurídico 0280/2003

4. CONCLUSIONES

Tras analizar los principales derechos fundamentales que entran en juego tras la utilización de los poderes de vigilancia y control por parte del empresario y más concretamente, en el caso de la videovigilancia, grabación de sonidos y control de los usos de los dispositivos informáticos de titularidad empresarial (y nos de titularidad privada), podemos extraer las siguientes conclusiones:

i. El derecho fundamental a la protección de datos se configura como un derecho autónomo e independiente del derecho fundamental a la intimidad, ambos recogidos en la CE (el derecho a la protección de datos en el artículo 18.4 y el derecho a la intimidad en el artículo 18.1), pero que, en el ámbito laboral, sobre todo por la influencia de las TICs, ha supuesto que ambos derechos (incluyendo otros como el derecho al secreto de las comunicaciones) queden vinculados, configurándose como un derecho mixto, pues para garantizar el contenido del derecho de protección de datos, hay que garantizar el contenido esencial de otros derechos fundamentales. Esto se ve claro con el principio de calidad de los datos personales, el cual responde a una finalidad de garantizar el derecho a la intimidad estableciendo restricciones en relación con la recogida y tratamiento de los datos personales.

El derecho a la protección de datos debe de garantizar un poder de control y disposición al trabajador sobre sus datos personales, necesitando el empresario un título habilitante para ello, pudiendo ser el consentimiento expreso del trabajador, pero siendo este innecesario cuando haya un fin justificado como puede ser la necesidad de ejecución de un contrato de trabajo, de dar cumplimiento a las obligaciones legales o la de proteger intereses vitales o legítimos. Además, existe el deber empresarial de informar a los trabajadores sobre los datos personales que se hayan obtenido, no siendo así en los casos en que el interesado ya esté informado, resulte imposible o suponga un esfuerzo desproporcionado comunicar dicha información, la información esté prevista por el derecho comunitario o nacional y, por último, si los datos personales tienen carácter confidencial sobre la base de una obligación de secreto profesional.

Por otro lado, en cuanto al cumplimiento del derecho fundamental a la intimidad, el TC estableció el principio de proporcionalidad, debiendo de superar el triple juicio de idoneidad en las medidas adoptadas, necesidad en la medida utilizada, debiendo utilizar la menos invasiva y más moderada para el trabajador, y la proporcionalidad en sentido estricto, teniendo que ser la medida equilibrada evitando los mayores perjuicios para el trabajador.

ii. En segundo lugar, debemos de resaltar la importancia de la Sentencia Barbulescu II, procedente de la jurisprudencia del TEDH que es la que están siguiendo de guía para nuestros tribunales, pues introduce matizaciones a la doctrina constitucional actual sobre las garantías exigibles para el control licito del empresario de los sistemas informáticos utilizados por los trabajadores:

1) La intimidad debemos de interpretarla en sentido amplio, no solamente en sentido estricto en relación con la vida privada sino más allá, teniendo en cuenta las relaciones sociales.
2) Necesidad de información previa al trabajador sobre las medidas vigilancia, su naturaleza, características y finalidad.
3) La notificación de la prohibición del uso del correo electrónico ha de ser clara concreta y precisa, al igual que en el uso del mecanismo de control y vigilancia.
4) Los mecanismos de control empresariales dirigidos al contenido de las comunicaciones deberán de ser sometidos a un control de proporcionalidad más intenso.
5) Justificar expresamente los motivos del uso de las medidas de vigilancia, debiendo de ser motivos concretos, reales y precisos, más allá de la alusión al control empresarial del artículo 20.3 ET.
6) La normativa interna de las empresas no puede reducir totalmente la vida privada social del trabajador, quedando siempre una expectativa de privacidad, aunque exista una prohibición expresa y reiterada del uso de los medios informáticos con fines personales.

iii. Con motivo de la influencia de las TICs en el ámbito laboral, surgieron unas especialidades introducidas por la Ley Orgánica de Protección de Datos del año 2018, entre las que podemos destacar:

- El control del uso de medios informáticos de titularidad empresarial, donde adquiere gran importancia la sentencia Barbulescu anteriormente desarrollada y, además, el trabajador no está facultado para el uso o disfrute privado del dispositivo. El empresario,

fundamentado en el artículo 87 de la LOPD, estará facultadlo para comprobar el cumplimiento de la actividad laboral del trabajador, garantizar la integridad de los dispositivos digitales y, además, comprobar que no se utilicen para usos privados, respetando siempre el derecho del trabajador a la privacidad virtual.

- La videovigilancia, la cual la podemos dividir en: videovigilancia identificada e informada, videovigilancia identificada pero no informada y, por último, la videovigilancia no identificada y no informada (esta última, las cámaras ocultas, no están reguladas en la LOPD), cada cual, con un grado mayor de dificultad para su licitud, desde la necesidad única de información hasta la puesta de un cartel informativo, dependiendo del caso concreto. En el último caso, nos encontramos con el caso concreto de que el TEDH estimó la grabación mediante cámaras ocultas en una ocasión, eso sí, mientras se habilitaba la grabación simultánea de cámaras no identificadas, pero sí informadas mediante el cartel informativo exigido por el artículo 22.4 de la LOPD, por lo que no podemos entender que se legitime su grabación en el caso de que no se cumplan los requisitos del artículo antes mencionado.
- La grabación de sonido por parte del empresario a los trabajadores es considerada mucho más invasiva que la videovigilancia y, como tal, con mayores restricciones a la hora de su uso.
- En ambas dos (videovigilancia y grabación de sonido) deberá de respetar los estándares mínimos de protección de intimidad y de otros derechos constitucionalmente protegidos (como el derecho a la protección de datos) y se prohíbe su uso en lugares destinados al descanso o esparcimiento de los trabajadores tales como vestuarios, aseos, comedores y análogos.

iv. Por último, en la LOPD no se resuelven todos los aspectos que pueden dar lugar a una vulneración de los derechos fundamentales del trabajador, así como el fragante delito en el caso de la videvogiliancia o las cámaras ocultas, o el uso de medios informáticos propios del trabajador. Estos son aspectos la jurisprudencia deberá de seguir perfilando y en los que seguirá avanzando según surja nuevas situaciones aún no tratadas.

5. BIBLIOGRAFÍA

Arias Domínguez, A. y Rubio Sánchez, F*E Derecho de los Trabajadores a la Intimidad.* Navarra: Aranzadi, S.A., (2006).

BAYLOS GRAU, A., "La protección de los derechos fundamentales por el Tribunal Constitucional español: auge y declive de la función de tutela", *RDS*, núm. 69.

De León, Alonso: "*El derecho a la intimidad del trabajador y el poder de control empresarial" 2019.*

Demelsa Liberato, Diandra: *"Derecho a la intimidad del trabajador y poder empresarial".* Universidad de León. *2018.*

Dictamen 2/2017 sobre el tratamiento de datos en el trabajo (8 de junio 2017). Grupo de Trabajo sobre Protección de Datos del artículo 29.

FERNÁNDEZ ORRICO, Fco. Javier., "*Criterios sobre usos de dispositivos tecnológicos en el ámbito laboral: hacia el equilibrio entre el control empresarial y la privacidad del trabajador".* Universidad Miguel Hernández. 2021.

GOERLICH PESET, José María "Poderes del Empresario", en AAVV, *Derecho del Trabajo, Tirant lo Blanch, Valencia, 2016.*

GONZÁLEZ, C.: "*Guía práctica sobre Protección de Datos: ámbito laboral,*"

GOÑI SEIN J.L.*: "Los derechos fundamentales inespecíficos en la relación laboral individual: ¿necesidad de una reformulación? Primera Ponencia del XXIV Congreso Nacional de Derecho del Trabajo y de la seguridad Social, organizadas por la Asociación Española de Derecho del Trabajo y de la Seguridad Social. Pamplona, 2014.*

LÓPEZ BALANGUER, MERCEDES y RAMOS MORAGUES, FRANCISCO: "*Control empresarial del uso de dispositivos digitales en el ámbito laboral desde la perspectiva del derecho a la protección de datos y a la intimidad".* Universidad de Valencia, 2020. Vol. 10. Núm. 2.

MERCADER UGINA, Jesús Rafael, *Protección de datos y garantía de los derechos digitales en las relaciones laborales,* Madrid, 2019.

O`Callagham, Xavier: "Honor, Intimidad e Imagen", en *Libertad de Expresión y sus Límites.* Madrid, 1991.

ORELLANA CANO, A.M: "*El derecho a la protección de datos personales como garantía de la privacidad de los trabajadores",* Aranzadi, Madrid. 2019.

RASCÓN LÓPEZ, RODRIGO, *Reflexiones sobre los límites del poder de control empresarial ejercido sobre los trabajadores por medios tecnológicos,* La Revista internacional del derecho práctico.

Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores.

RODRÍGUEZ ESCANCIANO, S., *Derechos laborales digitales: garantías e interrogantes.* Aranzadi, 2019.

RODRÍGUEZ ESCANCIANO, Susana., *"Videovigilancia empresarial: límites a la luz de la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales"*,2019. Núm. 9328.

SERRANO OLIVARES, Raquel. «Los derechos digitales en el ámbito laboral: comentario de urgencia a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales». *IUSLabor. Revista d'anàlisi de Dret del Treball.* 2018, n.º 3.

TALÉNS VISCONTI, Eduardo., *"Vídeo-vigilancia y protección de datos en el ámbito..."* Vol.6. Núm.3.

NORMATIVA

Reglamento UE 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

Convenio Europeo de Derechos Humanos Modificado por los Protocolos nos. 11,14 y 15, completado por el Protocolo adicional y los Protocolos nos. 4, 6, 7, 12, 13, 16.

Constitución Española, aprobada por las Cortes Generales en sesiones plenarias del Congreso de los Diputados y del Senado celebradas el 31 de octubre de 1978, ratificada por el pueblo español en referéndum de 6 de diciembre de 1978 y sancionada por S.M. el Rey ante las Cortes el 27 de diciembre del mismo año.

Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal.

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Real Decreto 1720/2007 de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores.

6. ANEXO JURISPRUDENCIAL

STEDH "*Asunto Copland VS Reino Unido"* núm. 62617/2000, de 3 de abril de 2007.

STEDH "*Caso Barbulescu II vs Rumanía"* núm. 2017/61 de fecha 5 de septiembre de 2007.

STEDH "*Caso Libert VS Francia"* núm. 2018/35. de 22 de febrero de 2018

STEDH "*Caso Ribalda y otros VS España"* (Nº 1874/13 y 8574/13). 17 de octubre de 2019

STC 8 de Julio de 1993 (RTC 418/1987 y 421/1987 nº 1902/1991 y 1904/1991).

STC 254/1993, de 20 de julio de 1993 (RTC 1993,254), nº recurso 1827/1990.

STC 94/1998, de 4 de octubre (RTC 94/1998), nº de recurso 840/1995.

STC 98/2000, de 10 de abril. (RTC 2000/98). Nº rec. 4015/96.

STC 290/2000 de 30 de noviembre de 2000 (ES:TC: 2000:290, Nº de Recurso 201/1993).

STC 112/2004 de 12 de julio (RTC 2004/112).

STC 173/2011, de 7 de noviembre (ECLI: ES:TC:2011:173)

STC 241/2012 de 17 de diciembre RTC 2012/241. (nº recurso 7304/2007),

STC 29/2013 de 11 de febrero (RTC 2013/29). Nº rec. 10522/2009.

STC 170/2013 de 7 de octubre. RTC 2013/170. (nº recurso 2907/2011)

STC 39/2016, de 3 de marzo (RTC 2016/39).

STS 52/2003 de 5 de diciembre de 2003 (ES 2003/7798).

STS 18 de junio de 2006 (RJ 2006/8452).

STS 26 de septiembre de 2007, núm. 1097/2005 (ES:TS:2007:8599).

STS 6 de octubre de 2011, núm. 4053/2010 (ES:TS:2011:8876)

STS de7 de julio de 2016, REC 3233/2014. (ES:TS: 2016:4070).

STS 7 de julio de 2016, RJ 2016/4434 (ES:TS:2016:3146).

STS de 31 de enero de 2017, REC 3331/2015. (ES:TS: 2017:654)

STS 2 de febrero de 2017, RJ 2017/168. (ECLI:ES:TS: 2020:812).

STS 8 de febrero de 2018, JUR 2018/58399. (ECLI:ES:TS: 2018:589)

STS 489/2018, 23 de octubre (RJ 2018, 4937)

STS de 7 febrero 2018, rec. 78/2017 (ES:TS: 2018:572)

SAN 6 de febrero de 2019 (AS 2019, 905)