
FACULTAD DE DERECHO

# INTIMIDAD, PROTECCIÓN DE DATOS Y GARANTÍAS DIGITALES EN EL AMBITO LABORAL

Autor: Cristina Cavero Bernardo

5º E-3 A

Derecho Laboral

Tutor/a: Ana Matorras Díaz-Caneja

Madrid

Abril 2019

## RESUMEN

La incorporación de las nuevas tecnologías al mundo laboral ha supuesto un aumento en la circulación de datos de carácter personal de los trabajadores. Asimismo, el derecho a la intimidad del trabajador en la relación laboral ha experimentado intromisiones del poder de dirección y de control del empresario como consecuencia de la introducción de las nuevas tecnologías como instrumentos de control.

Por tanto, en este trabajo de fin de grado se pretende estudiar la problemática que genera el respeto al derecho a la intimidad y la protección de los datos personales en el ámbito laboral. Es por ello que es de suma importancia delimitar hasta dónde puede llegar el control empresarial reconocido en el artículo 20.3 ET para no vulnerar el derecho a la intimidad del trabajador.

Este trabajo pretende fijar los límites empresariales, acudiendo en algunos supuestos a la jurisprudencia, para encontrar el equilibrio entre el control empresarial y las garantías que debe de adoptar el empresario para no vulnerar los derechos fundamentales de los trabajadores.

## PALABRAS CLAVE

Protección de datos, garantías digitales, intimidad, control empresarial.

## ABSTRACT

The use of new technologies in the labor world has led to an increase in the circulation of the employee's personal data. Likewise, the right to privacy of the worker in the employment relationship has experienced intrusions of the power of management and control of the employer as a consequence of the introduction of new technologies as corporate control methods.

Therefore, this project will study the problems generated by respect of the right to privacy and the protection of personal data in the workplace. For this reason, it is extremely important to define the extent to which the company control recognised in article20.3 ET can extend in order not to infringe the employee´s right to privacy.

The aim of this project is to establish the limits of the corporate control methods of the employer, using jurisprudence in some cases, in order to reach a balance between corporate control and the guarantees that the employer must adopt in order not to infringe employee's fundamental rights.

**KEY WORDS**

Data protection, digital guarantees, privacy, corporate control.

## ÍNDICE

ABREVIATURAS ..... 6

1 INTRODUCCIÓN ..... 8

1.1 Justificación de la elección del tema ..... 8

2 DERECHOS DEL CIUDADANO RECONOCIDOS EN RELACIÓN A LA PROTECCIÓN DE DATOS ..... 10

2.1 El marco constitucional ..... 10

*2.1.1 El derecho a la protección de datos como derecho constitucional autónomo 11*

*2.1.2 El derecho a la intimidad personal y familiar ..... 12*

*2.1.3 El derecho a la protección de datos ..... 13*

*2.1.4 Contenido ..... 16*

2.2 El marco legal: derecho a la intimidad y a la protección de datos en el marco normativo ..... 20

2.3 Consentimiento ..... 23

3 PROTECCIÓN DE DATOS Y GARANTÍAS DIGITALES EN EL ÁMBITO LABORAL ..... 24

3.1 Uso de dispositivo de videovigilancia ..... 24

*3.1.1 Concepto de videovigilancia ..... 24*

*3.1.2 Facultad de vigilar empresario ..... 24*

*3.1.3 Límites ..... 26*

*3.1.4 Información ..... 28*

*3.1.5 Comentarios STC 39/2016, de 3 de marzo ..... 29*

*3.1.6 Comentario STC 29/2013, de 11 de febrero ..... 32*

3.2 Sistemas de geolocalización ..... 34

*3.2.1 Concepto de geolocalización ..... 34*

*3.2.2 Información ..... 35*

*3.2.3 Vehículos ..... 36*

*3.2.4 ¿Qué datos pueden ser recabados? ..... 38*

*3.2.5 Limites ..... 38*

3.3 Uso de dispositivos digitales ..... 40

*3.3.1 Concepto de correo electrónico ..... 40*

*3.3.2 Dirección de correo electrónico ..... 41*

*3.3.3 Facultad del empresario ..... 41*

*3.3.4 Limites ..... 42*

*3.3.5 Información* ..... *43*
*3.3.6 Comentario TEDH caso Barbulescu II* ..... *44*
3.4 Control biométrico ..... 47
*3.4.1 Concepto de datos biométrico* ..... *47*
*3.4.2 Facultad del empresario* ..... *48*
*3.4.3 Limites* ..... *49*
*3.4.4 Información* ..... *50*
3.5 Bring your own device ..... 52
*3.5.1 Concepto* ..... *52*
*3.5.2 Riesgos* ..... *52*
*3.5.3 Medidas de protección* ..... *53*
*3.5.4 Control del empresario* ..... *53*
3.6 Teletrabajo ..... 55
*3.6.1 Concepto de teletrabajo* ..... *55*
*3.6.2 Derechos del trabajador* ..... *55*
*3.6.3 Facultad del empresario* ..... *55*
*3.6.4 Control de la jornada laboral* ..... *56*
4 INSTITUCIONES REGULADORAS ..... 58
4.1 Agencia Española de Protección de Datos ..... 58
5 CONCLUSIONES ..... 59
6 REFERENCIAS BIBLIOGRÁFICAS ..... 61
6.1 Legislación ..... 61
*6.1.1 Comunitario* ..... *61*
*6.1.2 Nacional* ..... *62*
6.2 Jurisprudencia ..... 62
*6.2.1 Tribunal Constitucional* ..... *62*
*6.2.2 Tribunal supremo* ..... *63*
*6.2.3 Tribunal Superior de Justicia* ..... *63*
*6.2.4 Tribunal Europeo de Derechos Humanos* ..... *64*
6.3 Obras doctrinales y recursos de internet ..... 64
6.4 Otros recursos ..... 66

**ABREVIATURAS**

| | |
|---|---|
| **AEPD** | Agencia Española de Protección de Datos |
| **CE** | Constitución española (BOE núm. 311, de 29 de diciembre de 1978). |
| **CEDH** | Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, hecho en Roma el 4 de noviembre de 1950 |
| **CNN-CERT** | Centro Criptológico Nacional |
| **EIPD** | Evaluación del impacto en la protección de datos |
| **ET** | Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores (BOE núm. 255, de 24 de octubre de 2015) |
| **LOPD** | Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (BOE, núm., 294, de 6 de diciembre de 2018) |
| **Núm.** | Número |
| **RGPD** | 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 (DO L 191 de 4 de mayo de 2016) |
| **STC** | Sentencia del Tribunal Supremo |
| **STEDH** | Sentencia del Tribunal Europeo de Derechos Humanos |
| **STS** | Sentencia Tribunal Supremo |

| | |
|---|---|
| **STSJ** | Sentencia del Tribunal Superior de Justicia |
| **TC** | Tribunal Constitucional |
| **TEDH** | Tribunal Europeo de Derechos Humanos |
| **TS** | Tribunal Supremo |
| **TSJ** | Tribunal Superior de Justicia |

# 1 INTRODUCCIÓN

## 1.1 Justificación de la elección del tema

Actualmente vivimos en una sociedad altamente tecnológica, donde el uso de la tecnología no solo está presente en nuestra vida diaria personal, sino que también en el ámbito laboral.

Las nuevas tecnologías son una realidad cambiante, que "han revolucionado el mundo laboral de nuestros días" y debido a su elevado ritmo de crecimiento, se ha generado "una realidad plagada de situaciones que hasta hace relativamente pocos años resultaban impensables en todos los órdenes".[1]

Por tanto, debido al veloz avance tecnológico, las empresas y los trabajadores se han tenido que adaptar a su uso como herramientas de control y de trabajo. Los avances de la tecnología revolucionan la forma en la que trabajamos y será necesario conocer la protección de la que gozan los trabajadores en su puesto de trabajo, amparada en los derechos constitucionales de tercera generación, dentro de los cuales destacamos el derecho a la protección de datos.

No obstante, el mundo laboral no es único factor que compromete el derecho a la protección de datos, ya que el uso de aplicaciones móvil o la creación de cuentas en plataformas digitales también genera un riesgo de exposición de nuestros datos personales.

Sin embargo, la introducción de las nuevas tecnologías de la información y comunicación en el mundo laboral genera numerosos conflictos entre el derecho a la intimidad del trabajador y el poder de dirección y control del empresario.

Esto se debe a que el abusivo ejercicio del poder de control empresarial sobre los medios informáticos puestos a disposición del trabajador puede resultar lesivo para los derechos fundamentales de la persona del trabajador, tales como el derecho a la intimidad personal.

---

[1] Sempere Navarro, A. V. y San Martín Mazzucconi, C., *Nuevas Tecnologías y Relaciones Laborales*, Aranzadi, Navarra, 2002 p. 31

De tal forma que se derivan ciertas controversias a la hora de fijar los límites del ejercicio de la facultad de control del empresario y del trabajador. Esto se debe a que la introducción de las nuevas tecnologías en el ámbito laboral reduce la intimidad personal del trabajador.

Es por ello, que el objeto de estudio del presente trabajo consistirá en analizar como las nuevas tecnologías han generado numerosos conflictos en las relaciones laborales, poniendo en peligro el equilibrio entre los intereses del empresario y los derechos del trabajador.

Por tanto, el trabajado se centra en analizar y delimitar los límites del empresario mediante el ejercicio del poder empresarial de dirección, control y vigilancia y la no vulneración del derecho a la intimidad y el derecho a la protección de datos.

## 2 DERECHOS DEL CIUDADANO RECONOCIDOS EN RELACIÓN A LA PROTECCIÓN DE DATOS

### 2.1 El marco constitucional

La Constitución Española (en adelante, CE) recoge en la Sección 1ª del Capítulo Segundo del Título I, en los artículos del 14 al 29 los derechos fundamentales y libertades públicas que todo ciudadano tiene reconocido por ser "inherentes e irreducible" a todos los seres humanos. [2]

Por tanto, son derechos que pertenecen a la persona como tal y no por el mero hecho de ser ciudadanos, ya que tienen como fin principal garantizar la dignidad humana.

Puesto que nos encontramos dentro de un Estado de derecho democrático, la especial defensa de los derechos fundamentales y libertades públicas ha de garantizarse mediante un conjunto de garantías y medios de defensa más rígidos.

El artículo 53.1 CE vincula a todos los poderes públicos a los derechos y libertades públicas reconocidos en el Capítulo segundo del Título I.

Además, otorga a los ciudadanos una serie de garantías legislativa, al quedar condicionado el desarrollo de los derechos fundamentales al principio de reserva de Ley, tal y como prevé el artículo 53.1 y 81 CE.

Por tanto, el ciudadano goza de una protección consolidada ante el Estado al tratarse derechos básicos para la construcción del orden político y social.

Tras haber mencionado el importante papel de los derechos constitucionales y la máxima protección de los derechos fundamentales y libertades públicas dentro de nuestro ordenamiento jurídico, vamos a analizar dentro de estos derechos fundamentales, los dos que afectan a las relaciones laborales.

[2] Álvarez Vélez, Mª. I. (coord.), *Lecciones de Derecho Constitucional*, Tirant lo Blanch, Valencia, 2014, p. 361

### *2.1.1 El derecho a la protección de datos como derecho constitucional autónomo*

El artículo 18.1 CE garantiza el derecho al honor, a la intimidad personal y familiar y la propia imagen, y en su apartado 4 regula la limitación de la informática para garantizar la protección de los derechos recogidos en el apartado 1.

El artículo 18 CE señala

> 1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.
> 2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.
> 3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.
> 4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.[3]

Por tanto, los apartados 1, 2 y 3 del artículo 18 son derechos fundamentales independientes que a su vez guardan una conexión con la intimidad.

A continuación, se va a analizar en primer lugar la intimidad personal recogida en el artículo 18.1 CE y, en segundo lugar, la protección de datos de carácter personal recogido en el artículo 18.4 CE.

Hoy en día, estos dos derechos se han vuelto de suma importancia puesto que nos encontramos ante un acelerado avance en la rama tecnológica. Es por ello que se ha convertido estrictamente necesario desarrollar el derecho a la protección de datos dentro de los textos constitucionales de los Estados Miembros de la Unión Europea. [4]

Para enfrentarnos a los avances tecnológicos y a la nueva tecnología en el ámbito laboral, tenemos que entender que el derecho a la intimidad regulado en el artículo 18.1 CE no es suficiente para proteger al ciudadano y a sus datos de carácter personal. Es por ello que como indica Fernández Rodríguez, podremos enfrentarnos a la evolución de la sociedad mediante la

---

[3] Artículo 18. 4 de la Constitución española (BOE núm.311, de 29 de diciembre de 1978) [en adelante, CE]

[4] Seone, J.A., "La ampliación del catálogo de derechos fundamentales", *Persona y derecho,* vol. 54, 2006, p.447 (disponible en http://dadun.unav.edu/handle/10171/14628; última consulta el 23/03/2019).

configuración de derechos fundamentales que protejan al individuo de las injerencias y amenazas de la sociedad de la información. [5]

### *2.1.2 El derecho a la intimidad personal y familiar*

Según el artículo 18 CE de la sección 1ª de los derechos fundamentales y libertades públicas: "Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen". [6]

Nos encontramos ante un derecho de la personalidad, protegiendo la esfera privada de la vida personal de cualquier intento de inferencias ajenas. Por lo tanto, se trata de evitar que terceros tengan conocimiento de datos relativos a la vida personal y familiar.[7]

A través de este derecho se pretende proteger información ligada a la situación familiar, asuntos médicos, consumo de bebidas alcohólicas o creencias religiosas entre otros.[8]

Este derecho está estrechamente ligado a la dignidad del individuo y al libre desarrollo de la personalidad.

La intimidad personal va ligada a la dignidad, garantizando así el pleno desarrollo de la persona a nivel individual sin intromisiones de terceros. En la STC 53/1985, de 11 de abril resalta la importancia de la dignidad cuando se refiere a ella como "un valor espiritual y moral inherente a la persona, que se manifiesta singularmente en la autodeterminación consciente y responsable de la propia vida y que lleva consigo la pretensión al respeto por parte de los demás".[9]

Según Mercader Uguina, las principales diferencias que podemos destacar entre el derecho a la intimidad personal y familiar respecto del derecho de protección de datos son que:

> El derecho a la protección de datos personales entra de lleno en el ámbito de la privacidad. Este concepto es más amplio que el de intimidad, pues la intimidad protege la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona, mientras que la privacidad constituye

---

[5] Fernández Rodríguez, J J. *Secreto e Intervención de las comunicaciones e internet.* Thomson Civitas, Madrid, 2004. p.41

[6] Artículo 18 CE

[7] Álvarez Vélez, Mª . I., *op. cit., p. 361*

[8] Medina Guerrero, M., *La protección Constitucional de la intimidad frente a los medios de comunicación*, Tirant to Blanch, Valencia, 2005, p. 16

[9] STC 53/1985, de 11 de abril (BOE núm. 119, de 18 de mayo de 1985). (disponible en http://hj.tribunalconstitucional.es/es/Resolucion/Show/433 ; última consulta el 27/03/2019).

un conjunto más amplio, más global, de facetas de la personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca, pero que, enlazadas entre sí, arrojan un retrato de la personalidad del individuo que este tiene derecho a mantenerse reservado.[10]

Por un lado, la intimidad personal y familiar preserva el entorno más personal de intromisiones de terceras personas, dotando al individuo con el poder jurídico de poder imponer a terceros la abstención de cualquier intromisión en su ámbito privado personal y familiar. Por ello, a modo de un breve resumen, se puede decir que el derecho a la intimidad protege la esfera personal de intromisiones ilegitimas.

Por otro lado, el derecho a la protección de datos tiene como objetivo proteger el uso y destino cualquier tipo de dato personal, dotando al individuo un poder de disposición y control sobre sus datos personales.

La principal diferencia será que dentro de la protección de datos se incluye no solo los datos pertenecientes a la esfera íntima, si no que engloba la protección del conjunto de todos los datos de un individuo, sean íntimos o no.

De tal forma que se observa que el ámbito de protección es más amplio y global en la protección de datos que en el derecho a la intimidad, puesto que no solo abarca la protección de datos personales, sino que la de cualquier dato identificable que permita crear en conjunto un perfil completo del individuo. -

### *2.1.3 El derecho a la protección de datos*

Mercader Uguina sostiene que "el valor o bien jurídico protegido es la libertad del individuo frente a los abusos y presiones a que puede verse sometido como consecuencia del tratamiento de sus datos personales".[11]

Para definir el derecho de protección de datos personales tenemos que acudir a la STC 292/2000, de 30 de noviembre.

La presente sentencia nace como una reacción al auge del desarrollo tecnológico y su colisión

[10] Mercader Uguina, J R, *Protección de datos en las Relaciones Laborales,* Francis Lefebvre, Madrid, 2018, p. 20.

[11] Mercader Uguina, J.R., *op. cit.,* p. 20

con la sociedad, frenando así la potencial amenaza del control de los datos de carácter personal por parte de terceros.

El Tribunal Constitucional (en adelante, TC), dicta la Sentencia 292/2000, de 30 de noviembre en la que aborda la temática de la protección de datos. Donde se delimita, dentro de nuestro ordenamiento jurídico, la naturaleza de derecho fundamental y su carácter autónomo.

Esta sentencia desarrolla el planteamiento inicial que anteriormente se inició con la STC 24/ 1993, de 20 de junio, donde se busca proteger el conjunto de los valores constitucionales, así como dotar de una fuerte protección a la esfera privada e íntima de los individuos ante la latente irrupción tecnológica y evitar una lesión de los derechos.[12]

Es necesario mencionar la gran relevancia de esta sentencia, ya que como señala Casas Baamonde "la STC 290/2000 reconoció un nuevo derecho fundamental, declarando su contenido esencial, tomándolo de la construcción avanzada por la STC 254/1993".[13]

Por tanto, no fue hasta este nuevo giro jurisprudencial cuando el derecho a la protección de datos pasa a tener la consideración de derecho fundamental autónomo y específico.

Concretamente, el derecho a la protección de datos es configurado de manera desvinculada respecto del derecho fundamental a la intimidad personal y familiar.

Por lo tanto, se separa el derecho a la intimidad del derecho a la protección de datos personales al considerarse derechos distintos. Tal y como indica Mercader Uguina: "intimidad y protección de datos no tienen que ir necesariamente unidas".[14]

El objetivo del artículo 18.4 CE es proporcionar al ciudadano poder de disposición y control del uso de sus datos personales.

En primer lugar, para poder entender qué poder de disposición y control posee el individuo

---

[12] STC 24/1993, de 20 de junio (BOE núm. 47, de 24 de febrero de 1993). (disponible en http://hj.tribunalconstitucional.es/es/Resolucion/Show/2153 ; última consulta el 27/03/2019).

[13] Casas Baamonde, M E., "El derecho a la protección de datos de carácter personal en la jurisprudencia del tribunal constitucional*", Anuario de relaciones laborales de España, núm.6,* 2015, p. 120

[14] Mercader Uguina, J.R.*, op. cit., p. 20*

sobre sus datos personales, debemos de comprender la razón de ser de dichos poderes, es por ello que en el Fundamento Jurídico 6 se recoge

> Su función es otorgar a la persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado. De tal modo que, si el derecho a la intimidad permite excluir ciertos datos de una persona del conocimiento ajeno, el derecho a la protección de datos garantiza a los individuos un poder de disposición sobre esos datos.[15]

Así, el ciudadano se podrá proteger de un uso inadecuado de la informática que atente contra su dignidad humana, reconocida en el artículo 10.1 CE, controlando que datos se encuentran en posesión de terceros y los usos posibles que les puedan dar.

Es por ello, que el poder de disposición y control es determinante a la hora de "decidir cuáles de esos datos proporcionar a un tercero"[16]

Para hacer efectivo el reconocimiento de las facultades de disposición y control que posee cada ciudadano, será necesario que ejerciten los derechos de acceso, rectificación, cancelación y oposición. Junto a ello, el Tribunal reconoce que, además, el individuo dispone de "la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular"[17]

Específicamente, cuando nos referimos a datos personales, tenemos que entender que se refiere a cualquier tipo de dato, si no que se entenderá que:

> No se reduce sólo a los datos íntimos de la persona, sino 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[18]

---

[15] STC 292/2000, de 30 de noviembre (FJ 6) (BOE núm. 4, de 04 de enero de 2001) (disponible en http://hj.tribunalconstitucional.es/es/Resolucion/Show/4276 ; última consulta el 29/03/2019).

[16] STC 292/2000, de 30 de noviembre (FJ 7) *op. cit.*

[17] STC 292/2000, de 30 de noviembre (FJ 7) *op. cit.*

[18] STC 292/2000, de 30 de noviembre (FJ 6) *op. cit.*

De tal forma, que se pretende evitar que cualquier injerencia por parte de un tercero afecte a los derechos del ciudadano ya que el individuo podrá "imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima de la persona y la prohibición de hacer uso de lo así conocido".[19]

Finalmente, se observa que en el artículo 7 de la Carta de Derechos Fundamentales de la Unión Europea, se recoge el derecho a la intimidad privada y familiar, mientras que en el artículo 8 se reconoce a nivel comunitario el derecho de protección de datos de carácter personal.

En este sentido, señala Mercader Uguina, que:

> La Carta de Derechos Fundamentales de la Unión Europea consagra la protección de datos de carácter personal como un derecho autónomo, separado y diferente del derecho al respeto de la vida privada (CDFUE art.7 y 8). Ello determina que el derecho a la intimidad y el derecho a la protección de datos personales sean categorías diferentes, aunque relacionadas. Y esa diferencia implica que, en ocasiones, los mismos hechos puedan ser constitutivos de vulneración de uno de esos derechos y no del otro.[20]

Por tanto, se aprecia que incluso a nivel comunitario, el derecho a la protección de datos de carácter personal es configurado como un derecho autónomo y diferenciado, pero siempre manteniendo una relación con el derecho de la intimidad personal.

El derecho a la intimidad personal y el derecho a la protección de datos guardan una relación entre ellos puesto que el respeto a la intimidad del trabajador es la base de la protección de datos. Se observa la relación existente entre ambos derechos ya que pretenden garantizar una protección de ciertos aspectos del individuo del conocimiento por terceras personas.

### *2.1.4 Contenido*

En una primera aproximación, el TC se refiere al contenido del derecho a la protección de datos como la capacidad de disposición y control sobre los datos.

El Tribunal matiza en la STS 292/2000, de 30 de noviembre FJ 6 que "tal derecho persigue garantizar a las personas un poder de control sobre sus datos personales, sobre su uso y su

---

[19] STC 292/2000, de 30 de noviembre (FJ 5) *op. cit.*

[20] Mercader Uguina, J.R., *op., cit*. p.21

destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado". [21]

Además, como afirma la Agencia Española de Protección de Datos (en adelante, AEPD): "reconoce al ciudadano la facultad de controlar sus datos personales y la capacidad para disponer y decidir sobre los mismos".[22]

Por tanto, observamos que la AEPD lo define desde una aproximación de carácter general y será necesario el apoyo en otros principios que concreten de manera más especifica cómo hacer efectivo el derecho. Para ello, el Tribunal afirma que:

> Estos poderes de disposición y control sobre los datos personales que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. [23]

Por tanto, el consentimiento se reviste de gran importancia a la hora de recoger los datos y se convierte en condición clave para su posterior tratamiento. Pero, debemos de prestar especial atención al FJ 7 que señala:

> […]derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos.[24]

De tal forma, que, según Suero Salamanca, se determinar que el derecho de protección de datos está compuesto por:

> Facultad de consentir la recogida de los datos, facultad de consentir la obtención y acceso a los datos personales, facultad de consentir sobre su posterior almacenamiento y tratamiento, facultad de consentir el uso de los datos personales, o usos posibles, por un tercero, sea la Administración

---

[21] STC 292/2000, 30 de noviembre (FJ 6) *op. cit.*

[22] Guía del derecho fundamental a la protección de datos de carácter personal de AEPD (disponible en www.pimemenorca.org/gest-docs/pub/536 ; última consulta el 1/04 2019).

[23] STC 292/2000, de 30 de noviembre (FJ 7) *op. cit.*

[24] STC 292/2000, de 30 de noviembre (FJ 7) *op. cit.*

Pública o un particular.[25]

No obstante, se aprecia otro bloque de derechos y facultades que permiten proteger a la persona frente al uso de sus datos personales. Este bloque de derechos está formado por el derecho de información, de acceso, de rectificación, de cancelación y de oposición, tal y como se recoge en la sentencia "derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos". [26]

Junto al consentimiento, señala el Tribunal:

> [...] son elementos característicos de la definición constitucional del derecho fundamental a la protección de datos personales los derechos del afectado a consentir sobre la recogida y uso de los datos personales y a saber de los mismos. Y resultan indispensables para hacer efectivo ese contenido el reconocimiento del derecho a ser informado de quién posee sus datos personales y con qué fin, y el derecho a oponerse a esa posesión o uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos. Es decir, exigiendo del titular del fichero que le informe de que datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios; y, en su caso, requerirle para que los rectifique o cancele.[27]

Por tanto, se logra un gran avance en la delimitación del contenido de del derecho de protección de datos, dotando al individuo de un gran poder frente al ejercicio del derecho a la protección de datos, garantizando a sus datos de carácter personal seguridad jurídica, incorporando:

> un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso.[28]

En conclusión, los elementos principales del contenido del derecho a la protección de datos, son en primer lugar el consentimiento del afectado para la captación y tratamiento de sus datos y, en segundo lugar, la habilitación legal como fundamento que justifique el tratamiento de los

---

[25] Suero Salamanca, J. A., "Comentarios a la sentencia del tribunal constitucional 292/2000, de 30 de noviembre", 2001 (disponible en http://www.madrid.org/usupadron/legislacion/protdatos/protecciondatos.pdf; última consulta 2/04/2019).

[26] STC 292/2000, de 30 de noviembre FJ 6 *op. cit.*

[27] STC 292/2000, de 30 de noviembre FJ 7 *op. cit.*

[28] STC 292/2000, de 30 de noviembre FJ 7 *op. cit.*

datos personales.

Finalmente, cabe señalar lo más relevante sobre poder de control es el conocimiento sobre la información personal, su uso y destino. El derecho a la protección de datos va más allá del derecho a la intimidad convirtiéndose en un "instrumento jurídico de tutela de la dignidad y el libre desarrollo de la personalidad alcanza en el ordenamiento jurídico sustantividad propia, y se configura como derecho a la personalidad".[29]

[29] Herrán Ortiz, A. I., "El derecho a la protección de datos personales en la sociedad de la información", *Cuaderno Deusto de Derechos Humano*, núm. 26, 2003, p. 21

## 2.2 El marco legal: derecho a la intimidad y a la protección de datos en el marco normativo

En primer lugar, dentro de la normativa laboral, el artículo 4.2 e) del Estatuto de los Trabajadores (en adelante ET) establece que:

> los trabajadores tienen derecho al respeto de su intimidad y a la consideración debida a su dignidad, comprendida la protección frente a ofensas verbales y físicas de naturaleza sexual y frente al acoso por razón de origen racial o étnico, religión o convicciones, discapacidad, edad u orientación sexual.[30]

Dentro del ámbito laboral, es frecuente que la esfera relativa a la intimidad personal del trabajador se vea condicionada por el control ejercido por parte del empresario, para comprobar el cumplimiento del horario, tareas, responsabilidades que le son requeridas.

Pero, la existencia de un contrato laboral que regule la relación existente entre el trabajador y el empresario nunca será "un título legitimador de recortes en el ejercicio de los derechos fundamentales que incumben al trabajador como ciudadano, que no pierde su condición de tal por insertarse en el ámbito de una organización privada".[31]

Es por ello, que se debe tener en cuenta que, dentro de la relación laboral, hay que respetar del principio de proporcionalidad, que será necesario poner en práctica cuando nace la relación laboral, ya que habrá que garantizar el lícito respeto a los derechos fundamentales del trabajador dentro de las obligaciones laborales.

Por tanto, el TC reitera que "la celebración de un contrato de trabajo no implica en modo alguno la privación para una de las partes, el trabajador, de los derechos que la Constitución le reconoce como ciudadano, entre ellos el derecho a su intimidad personal".[32]

El respeto a la intimidad encuentra respaldo en el artículo 10.1 CE, señalando que independientemente de la situación en la que se encuentre cada individuo, la dignidad siempre debe de permanecer inalterada y ser respetada. Por tanto, la STC 89/199, de 19 de julio, resaltó

---

[30] Artículo 4.3 de 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 (en adelante ET) (BOE núm. 255, de 24 de octubre de 2015).

[31] STC 126/2003, de 30 de julio (BOE núm. 181, de 30 de julio de 2003). (disponible en http://hj.tribunalconstitucional.es/es/Resolucion/Show/4901; última consulta 1/04/ 2019).

[32] STC 196/2004, de 15 de noviembre (BOE núm. 306, de 21 de diciembre de 2004). (disponible en http://hj.tribunalconstitucional.es/es/Resolucion/Show/5201; última consulta 1/04/ 2019).

que a pesar del control empresarial y poder del empresario, no podrán limitarse o vulnerarse los derechos fundamentales de los trabajadores de manera injustificada.[33]

En segundo lugar, la necesidad de unificación en materia de protección de datos de los estados miembros de la Unión Europea y el aumento significativo del uso de la tecnología fueron los principales impulsores que hicieron necesario la creación del nuevo Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 (en adelante RGPD), relativo a la protección de las personas físicas en lo que respeta al tratamiento de datos personales y a la libre circulación de estos datos, que entró en vigor el pasado 25 de mayo de 2018.

El RGPD es de aplicación directa a los estados miembros de la Unión Europea, aunque permite que las directrices del mismo puedan ser especificadas o restringidas cuando "sea necesario por razones de coherencia y para que las disposiciones nacionales sean comprensibles para sus destinatarios".[34]

Así se promulgó la nueva Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPD), en la que se desarrollan determinados aspectos del RGPD, sustituyendo a la antigua Ley orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal

La promulgación de una nueva ley interna surge como resultado de una necesaria adecuación y actualización conforme el nuevo reglamento comunitario.

Sin embargo, la nueva LOPD no solo desarrolla y se adapta el RGPD, sino que también proyecta los derechos digitales y se centra en una regulación específica en materia laboral.

---

[33] STC 89/1985, de 19 de julio (BOE núm. 194, de 14 de agosto de 1985) (disponible en http://hj.tribunalconstitucional.es/es/Resolucion/Show/469 ; última consulta el 1/04/ 2019).

[34] 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, (en adelante RGPD) (DO L 191 de 4 de mayo de 2016)

Además, la nueva LOPD pretende "adaptar la norma a las nuevas realidades creadas por internet y la transformación digital de la sociedad". [35]

Por último, cabe mencionar la importante labor de la nueva LOPD en protección laboral al regular los nuevos derechos digitales en el ámbito laboral, protegiendo al trabajador ante la revolución digital.

Finalmente, en la CE, no se recoge de manera directa el derecho a la protección de datos, pero si de manera implícita en su artículo 18.4. [36]

[35] Blázquez Agudo, E. M., "Novedades laborales en la nueva Ley orgánica de protección de datos", *Wolters Kluwer*, núm 50, 2019, p.2 (disponible en https://www.smarteca.es/my-reader/SMT2015106_00000000_20190201000000500000?location=pi-5028&searchHighlight=proteccion%20de%20datos%20laboral ; última consulta 1/04/ 2019).

[36] *Vid. infra*., apartado 2.2.1

## 2.3 Consentimiento

Al estudiar la protección de datos en el ámbito laboral, se tiene que partir de la base de la existencia de una relación contractual previa entre empleador y empleado.

Por ello, se entiende que todo aquel tratamiento de datos que mantenga una relación estrecha con el desempeño de la actividad laboral no necesitará recabar el consentimiento del trabajador.

De tal forma, que únicamente el empresario deberá de contar con el consentimiento del trabajador cuando el tratamiento de datos trate sobre materias que se sitúan fuera del objeto de la prestación laboral. Esto ocurre en el caso de prevención de riesgos laborales o afiliación sindical.

En este sentido, así lo afirma la STC 39/2016, de 26 de marzo:

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

Finalmente, como una breve conclusión, no se requerirá el consentimiento expreso del trabajador cuando el tratamiento de datos personales sea necesario como consecuencia del desarrollo de la actividad laboral, sin embargo, se deberá de cumplir con el deber de informar al trabajado sobre el tratamiento de sus datos.

# 3 PROTECCIÓN DE DATOS Y GARANTÍAS DIGITALES EN EL ÁMBITO LABORAL

## 3.1 Uso de dispositivo de videovigilancia

### *3.1.1 Concepto de videovigilancia*

En primer lugar, la Real Academia Española define videovigilancia como: "vigilancia por medio de un sistema de cámaras, fijas o móviles".[37]

Por tanto, entendemos como videovigilancia la instalación de un sistema de control y vigilancia integrado por un sistema de seguridad electrónico que combina el mecanismo de captación de imágenes y grabación de sonidos.

Hoy en día, como afirma Goñi Sein, el uso de la videovigilancia por parte de las empresas está en aumento debido a las ventajas económicas y su uso eficaz que reporta.[38]

### *3.1.2 Facultad de vigilar empresario*

Recoge el artículo 38 CE:

> Se reconoce la libertad de empresa en el marco de la economía de mercado. Los poderes públicos garantizan y protegen su ejercicio y la defensa de la productividad, de acuerdo con las exigencias de la economía general y, en su caso, de la planificación. [39]

Por tanto, observamos que la CE reconoce la libertad de empresa, dotando al empresario de determinados poderes relacionados con el ejercicio de la función de control y de dirección de la actividad laboral, donde "podrá adoptar las medidas que estime más oportunas de vigilancia e inspección para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales".[40]

---

[37] Real Academia Española (disponible en https://dle.rae.es/?id=bmtXm9x; última consulta 23/03/2019).

[38] Goñi Sein, J.L. *La videovigilancia empresarial y la protección de datos personales*, Aranzadi, Navarra, 2007, p.16

[39] Artículo 38 CE

[40] Jiménez-Castellanos Ballesteros, I., "Videovigilancia laboral y derecho fundamental a la protección de datos", *Revista andaluza de trabajo y bienestar social*, núm. 136, 2017, p. 131

Junto al artículo 38 CE, resaltamos la importancia del artículo 20.3 ET:

> El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad y teniendo en cuenta, en su caso, la capacidad real de los trabajadores con discapacidad.[41]

De tal forma que el artículo 20.3 ET permite al empresario adoptar las medidas oportunas de vigilancia y control para verificar el cumplimento de las obligaciones contractuales por parte del trabajador y para ello se podrán usar los correspondientes medios e instrumentos de control para verificar el cumplimento de dichas obligaciones.

Por otro lado, se tiene que respetar la intimidad personal reconocida en el artículo 87 de la nueva LOPD, que se tendrá que respetar "unos estándares mínimos de protección de su intimidad de acuerdo con los usos sociales u los derechos reconocidos constitucional y legalmente"[42]

A pesar de que el empresario cuenta con las facultades empresariales de control y vigilancia del artículo 20.3 ET, la nueva LOPD ha añadido un nuevo precepto en materia de garantías digitales, por ello en el artículo 20 bis de ET se recoge que:

> Los trabajadores tienen derecho a la intimidad en el uso de los dispositivos digitales puestos a su disposición por el empleador, a la desconexión digital y a la intimidad frente al uso de dispositivos de videovigilancia y geolocalización en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales"[43]

Con la redacción de este nuevo artículo, la ley pretende delimitar la barrera entre la esfera privada del trabajador y el ámbito de trabajo, para así poder respetar la intimidad personal del trabajador.

---

41 Artículo 20. 3 ET

[42]Blázquez Agudo, E. M., *op. cit.,* p.6

[43] Artículo 20 bis ET

Como señala Jiménez-Castellanos Ballesteros es muy importante que el poder de control por parte del empresario debe de respetar los derechos fundamentales mediante la utilización de medios respetuoso de los mismos y "de circunscribir esta actividad a la comprobación de aquellas cuestiones estrictamente vinculadas con la prestación de trabajo".[44]

Será en el artículo 89 de la nueva LOPD donde se reconozca el derecho a los empleadores a utilizar las imágenes que se hayan obtenido con los sistemas de videovigilancia para que ejerzan las facultades relativas al poder de dirección. No obstante, dichas facultades nunca podrán vulnerar el marco legal ni los limites inherentes al mismo.[45]

### *3.1.3 Límites*

De ningún modo podrán limitarse los derechos que tengan reconocidos constitucionalmente cada trabajador por el hecho de haber firmado un contrato de trabajo y quedar sometidos a las facultades empresariales. Esto se debe a que por el mero hecho que exista un contrato de trabajo no justifica un recorte en el ejercicio de los derechos fundamentales, puesto que el trabajador no pierde la condición de ciudadano al ejercer una prestación laboral.

Sin embargo, los derechos fundamentales sí que sufren una modulación, pero "sólo se producirá en la medida estrictamente imprescindible para el correcto y ordenado desenvolvimiento de la actividad productiva.[46]"

A raíz de lo anterior, el empresario tendrá como objetivo principal respetar la intimidad y la dignidad de los trabajadores de una forma compatible con el correcto desarrollo de la actividad laboral.

Las medidas adoptadas por el empresario deben de ser idóneas y proporcionales en relación a la finalidad que persigue con el control. En ningún caso el ejercicio de las facultades

---

[44] Jiménez-Castellanos Ballesteros, I., *op. cit.,* p.131

[45] Blázquez Agudo, E. M., *op. cit.,* p.9

[46] STC 98/2000, de 18 de mayo (FJ 7) (BOE núm. 119, de 18 de mayo de 2000). (disponible en http://hj.tribunalconstitucional.es/es/Resolucion/Show/4082 ; última consulta el 6/04/2019).

disciplinarias por parte del empleador puede ocasionar resultados lesivos de los derechos fundamentales del trabajador.

Por tanto, el empresario deberá de respetar en todo momento los derechos fundamentales de los trabajadores y en ningún caso podrá dañar los mismos.

Concretamente, el empresario tiene como límite principal al poder de control el respeto a la dignidad humana, específicamente deberá respetar el derecho a la intimidad del trabajador.[47]

Y así, se recoge en la STC 88/1985, de 19 de julio señala que:

> ni las organizaciones empresariales forman mundos separados y estancos del resto de la sociedad, ni la libertad de empresa legitima que quienes prestan servicios en aquéllas por cuenta y bajo la dependencia de sus titulares deban soportar despojos transitorios o limitaciones injustificadas de sus derechos fundamentales y libertades públicas, que tienen un valor central y nuclear en el sistema jurídico-constitucional.[48]

Según el artículo 64.1 ET:

> 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[49]

Por tanto, será a su vez necesario que los representantes de los trabajadores sean informados previamente a la implantación de sistemas de videovigilancia. [50]

Incluso, se recomienda avisar a los representantes de los trabajadores para aquellos casos en los que se opte por grabar con cámaras ocultas.[51]

---

[47] Jiménez-Castellanos Ballesteros, I., *op. cit.,* p.138

[48] STC 88/1985, de 19 de julio (BOE núm. 194, de 14 de agosto de 1985) (disponible en http://hj.tribunalconstitucional.es/es/Resolucion/Show/468 ; última consulta el 2/04/2019).

[49] Artículo 64.1 ET

[50] Mercader Uguina, J. R., *op. cit. p*.124

[51] Blázquez Agudo, E. M., *op. cit.,* p.9

### *3.1.4 Información*

La Instrucción 1/2006, de 8 de noviembre de la AEPD, en materia del tratamiento de los datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras, señala la importancia de cumplir con la obligación de colocar al menos un distintivo informativo que sea visible en aquellas zonas expuestas a un sistema de videovigilancia. Sin embargo, dentro del ámbito laboral será estrictamente necesario que se informe de manera individualizada a cada trabajador y con carácter previo acerca del uso de los sistemas de videovigilancia como medida de control empresarial.

Por tanto, observamos en primer lugar que, como señala Blázquez Agudo, la información al trabajador de los sistemas de videovigilancia debe ser: "previa, expresa, precisa e inequívoca" [52].

Por tanto, el trabajador deberá ser informado previamente de la implantación de los sistemas de videovigilancia empleados como medio de control laboral, aunque, como se analizará a continuación, se produce un cambio respecto al derecho de información con la STC 39/2016, de 3 de marzo por la cual desaparece la necesidad de información previa, sustituyendo dicha información con la colocación del correspondiente distintivo informativo en un lugar visible.

En segundo lugar, en cuanto al dispositivo informativo, señala Blázquez Aguado que deberá de contener, como mínimo, lo siguiente:" de la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos anexos al tratamiento de los datos". [53]

Además de: "ser informados de la finalidad de la recogida de los datos, de los destinatarios de la información, de la identidad y de la dirección del responsable del tratamiento".[54]

---

[52] Blázquez Agudo, E. M., *op. cit.* p.8

[53] Blázquez Agudo, E. M., *op. cit.* p.9

[54] Mercader Uguina, J. R.,*op. cit.* p 120

Para concluir, resumimos que los responsables del sistema de videovigilancia deberán de colocar al menos un distintivo informativo situado en una zona que cuente con suficiente visibilidad.

El plazo máximo de cancelación será de un mes desde la captación de las imágenes.[55]

### *3.1.5 Comentarios STC 39/2016, de 3 de marzo*

En esta sentencia del TC se analiza la procedencia del despido disciplinario a una trabajadora por la apropiación indebida de dinero de la caja captando dichas conductas, sobre las que existían sospechas fundadas acerca de las sustracciones, con un sistema de cámaras de videovigilancia que instaló la empresa para vigilar la caja e investigar las irregularidades contables.

Dicha instalación no fue comunicada por la empresa a los trabajadores previamente, si no que pusieron un distintivo informativo de zona videovigilada en un lugar visible en el escaparate como recoge la Instrucción 1/2006.[56]

En este caso concreto, el Tribunal consideró oportuno que no existiese una notificación a los trabajadores de la instalación de las cámaras puesto que era el único medio por el cual el empresario podría comprobar las irregularidades de manera evidente y así no alterar la conducta del trabajador que realizaba los actos defraudatorios.

A continuación, vamos a tratar el consentimiento.

El consentimiento se entiende implícito en la relación laboral cuando el tratamiento de datos sea necesario para el cumplimiento del contrato. Tal y como señala el Tribunal:

> [...]Por ello un tratamiento de datos dirigido al control de la relación laboral debe entenderse amparado por la excepción citada, pues está dirigido al cumplimiento de la misma. Por el contrario,

---

[55] Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras. ( BOE núm. 296 de 12 de Diciembre de 2006).

[56] Instrucción 1/2006 AEPD *op. cit.*

> el consentimiento de los trabajadores afectados sí será necesario cuando el tratamiento de datos se utilice con finalidad ajena al cumplimiento del contrato. [57]

Por tanto, la dispensa del consentimiento se refiere, así, a los datos necesarios para el mantenimiento y cumplimiento de la relación laboral, lo que abarca, sin duda, las obligaciones derivadas del contrato de trabajo.

Además, será innecesario el consentimiento para el tratamiento de las imágenes de las cámaras que tenga como finalidad la seguridad o el control:

> Aplicando la doctrina expuesta al tratamiento de datos obtenidos por la instalación de cámaras de videovigilancia en el lugar de trabajo, que es el problema planteado en el presente recurso de amparo, debemos concluir que el empresario no necesita el consentimiento expreso del trabajador para el tratamiento de las imágenes que han sido obtenidas a través de las cámaras instaladas en la empresa con la finalidad de seguridad o control laboral, ya que se trata de una medida dirigida a controlar el cumplimiento de la relación laboral y es conforme con el art. 20.3 del texto refundido de la Ley del estatuto de los trabajadores, que establece que «el empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana». Si la dispensa del consentimiento prevista en el art. 6 LOPD se refiere a los datos necesarios para el mantenimiento y el cumplimiento de la relación laboral, la excepción abarca sin duda el tratamiento de datos personales obtenidos por el empresario para velar por el cumplimiento de las obligaciones derivadas del contrato de trabajo. El consentimiento se entiende implícito en la propia aceptación del contrato que implica reconocimiento del poder de dirección del empresario. [58]

En consideración a la vulneración del artículo 18.4 CE, entendemos que para su procedencia deberemos de analizar el principio de proporcionalidad.

En esta sentencia, se considera que el artículo 18.4 CE no ha sido vulnerado debido a que la trabajadora tenía conocimiento previo del uso de un sistema de videovigilancia al encontrarse situado en el escaparate del comercio un distintivo informativo, como así indica la Instrucción 1/2006. Por tanto, el Tribunal estima que:

> en consecuencia, teniendo la trabajadora información previa de la instalación de las cámaras de videovigilancia a través del correspondiente distintivo informativo, y habiendo sido tratadas las

---

[57]STC 39/2016, de 3 de marzo (FJ 3) *(BOE núm. 85, de 08 de abril de 2016). (disponible en http://hj.tribunalconstitucional.es/es/Resolucion/Show/24845 ; última consulta 3/04/2019).*

[58] STC 39/2016, de 3 de marzo (FJ 5) *op. cit.*

> imágenes captadas para el control de la relación laboral, no puede entenderse vulnerado el art. 18.4 CE.

En cuanto al principio de proporcionalidad por parte del empresario a la hora de adoptar a la medida, la sentencia fija:

> debe ponderarse así el derecho a la protección de datos y las eventuales limitaciones al mismo justificadas en el cumplimiento de las obligaciones laborales y las correlativas facultades empresariales de vigilancia y control reconocidas en el art. 20.3 del texto refundido de la Ley del estatuto de los trabajadores, en conexión con los arts. 33 y 38 CE.

Por lo tanto, el Tribunal considera que la medida es justificada, idónea, necesaria y equilibrada ya que:

> era una medida justificada (ya que existían razonables sospechas de que alguno de los trabajadores que prestaban servicios en dicha caja se estaba apropiando de dinero); idónea para la finalidad pretendida por la empresa (verificar si algunos de los trabajadores cometía efectivamente las irregularidades sospechadas y en tal caso adoptar las medidas disciplinarias correspondientes); necesaria (ya que la grabación serviría de prueba de tales irregularidades); y equilibrada (pues la grabación de imágenes se limitó a la zona de la caja), por lo que debe descartarse que se haya producido lesión alguna del derecho a la intimidad personal consagrado en el art. 18.1 CE.[59]

En este caso, el Tribunal entiende que para ponderar si se respeta el principio de proporcionalidad habrá que atender a la relación existente entre los sistemas de videovigilancia instalados y el derecho a la intimidad personal de los trabajadores. Por tanto, entendió el Tribunal que la medida era proporcional puesto que era una medida justificada en sospechas de apropiación de dinero y tenía como objetivo comprobar si dicha conducta era verídica.

Para concluir, lo más destacable de esta sentencia determina que no será necesario informar de manera adicional a los trabajadores acerca del uso de sistema de videovigilancia, cuando tenga como objetivo controlar el cumplimiento de las obligaciones contractuales. Será suficiente con colocar el distintivo de zona videovigilada en un lugar suficientemente visible. Además, el consentimiento no será necesario cuando la finalidad del tratamiento de datos guarde una

[59] STC 39/2016, de 3 de marzo (FJ 5) *op. cit.*

relación directa con el control de la relación contractual, en este caso el dato fue utilizado para el control de las obligaciones laborales.

Por tanto, basta con que los trabajadores tengan un conocimiento genérico de la existencia del uso de cámaras de videovigilancia a través del distintivo informativo, como ocurre en este caso, donde la empresa cumplió con el deber de información previa al colocar el distintivo informativo en el escaparate.

### *3.1.6 Comentario STC 29/2013, de 11 de febrero*

La STC 39/2016, de 3 de marzo anteriormente analizado abre una nueva línea jurisprudencial de acuerdo a la necesidad o no de información previa.

En la sentencia 29/2013, de 11 de febrero considera que será necesario informar previamente al trabajador y de forma "expresa, precisa, clara e inequívoca" [60]de la finalidad del control laboral por parte del sistema de videovigilancia instalado. Por tanto, a diferencia del giro jurisprudencial del año 2016, se obliga al empresario a comunicar e informar a los trabajadores de la instalación de dichos sistemas y los fines para los que pueden usarse los datos grabados, incluido si pueden ser utilizados como medio para "la imposición de sanciones disciplinarias por incumplimientos del contrato de trabajo".[61]

De tal forma que no solo será necesario la puesta en conocimiento del uso de sistemas de videovigilancia, sino que también deberá informar acerca de la finalidad del control y de las posibles consecuencias de los datos recabados.

Finalmente, observamos que con la STC 39/2016, de 3 de marzo se produce un cambio en la doctrina del deber de información respecto de las cámaras de vigilancia a los trabajadores, mientras que anteriormente era necesario una información explicita, ahora solamente será

---

[60]STC 29/2013, de 11 de febrero *(BOE núm. 61, de 12 de marzo de 2013). (disponible en http://hj.tribunalconstitucional.es/es/Resolucion/Show/23284 ; última consulta 3/04/2019).*

[61] STC 39/2016, de 3 de marzo (FJ 8) *op. cit.*

necesario una información de carácter general a través de la colocación de un distintivo informativo.

Además, el control del empleador debe de estar sujetos a ciertos límites. En primer lugar, el respeto a la dignidad humana y los derechos fundamentales, y en segundo lugar las medidas adoptadas deben de ser idóneas y proporcionales respecto de la finalidad que se pretende lograr.

Por tanto, observamos que se produce un nuevo giro jurisprudencial ya que en la STC 29/2013, de 11 de febrero sostiene que la omisión del deber de información es un acto lesivo de los derechos fundamentales de los trabajadores, mientras que en la STC 39/2016, de 3 de marzo manifiesta que no será necesario la información expresa, preciosa e inequívoca con anterioridad ya que estropeará el fin de empresario de obtener la prueba de las conductas contrarias a las obligaciones contractuales. Por tanto, como establece la Instrucción 1/2006 de la AEPD será suficiente para cumplir con el deber de información colocar el distintivo informativo en un lugar visible.

## 3.2 Sistemas de geolocalización

### *3.2.1 Concepto de geolocalización*

Según la Directiva 2002/58/CE en su artículo 2, entendemos por datos de localización "cualquier dato tratado en una red de comunicaciones electrónicas que indique la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas disponible para el público".[62] Por tanto, los datos de geolocalización tienen la consideración de datos de carácter personal debido a que los mismos permiten identificar al individuo.

A tenor de lo dispuesto en la Propuesta de Reglamento de privacidad electrónica (e-privacy) de la Unión Europea, que sustituirá a la actual Directiva 2002/58/CE, se proyecta un mayor nivel de precisión para garantizar una protección predecible y efectiva de los derechos que no están cubiertos con la suficiente precisión en el RGPD.

En la propuesta de este nuevo Reglamento, se refuerza la importante protección de los datos de localización geográfica al contener información delicada y de carácter personal, tal y como se indica en su considerando segundo.[63]

Nos encontramos ante un método de control laboral que permite al empresario controlar la situación geográfica de sus trabajadores durante el desarrollo de la jornada laboral permitiéndole conocer la ubicación geográfica exacta del trabajador en tiempo real.[64] Así, el empresario puede controlar el debido cumplimiento de la prestación laboral en el lugar y horario establecido en el contrato, mediante los sistemas implantados en los "dispositivos móviles, GPS en vehículos microchips insertados en tarjetas identificativas o incluso implantados bajo la propia piel del empleado."[65]

---

[62] Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (DO L 201 de 31 de julio de 2002).

[63] Propuesta de Reglamento Del Parlamento Europeo y Del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas (10 de enero de 2017).

[64] Blázquez Agudo, E. M., op. *cit.,* p.11

[65] Rojas Rosco, R., López Carballo, D. "El impacto del RGPD en el ámbito del control laboral y la era de la innovación"**,** *Wolters Kluwer*, núm. 5, 2010, p. 17

Sin embargo, no fue hasta la nueva LOPD cuando se regula el derecho a la intimidad frente al uso de sistemas de geolocalización.

La nueva LOPD regula en su artículo 90 la utilización de los sistemas de geolocalización el ámbito laboral:

1. Los empleadores podrán tratar los datos obtenidos a través de sistemas de geolocalización para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respectivamente, en el artículo 20.3 del Estatuto de los Trabajadores y en la legislación de función pública, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo.

2. Con carácter **previo**, los empleadores habrán **de informar** de forma expresa, clara e inequívoca a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de la existencia y características de estos dispositivos. Igualmente deberán informarles acerca del posible ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión.

### *3.2.2 Información*

En primer lugar, los empleados y sus representantes deberán ser informados previamente sobre el uso de los sistemas de geolocalización y de manera expresa, clara e inequívoca" De tal forma que el trabajador deberá tener conocimiento acerca de quien posee sus datos personales y el propósito por el que se realiza el tratamiento de los mismos.

No solo deberán de ser informados claramente de la existencia de estos sistemas, sino que además deberán de ser informados de la posibilidad del ejercicio de sus derechos de acceso, rectificación, limitación del tratamiento y supresión. Por tanto, la adecuada información de la implementación del sistema y de la finalidad del mismo será estrictamente necesario ya que si no nos encontraremos ante una vulneración de los derechos de la intimidad del trabajador.

No obstante, se observa que no será necesario el consentimiento del trabajador cuando el tratamiento de los datos obtenidos tenga como finalidad el cumplimiento de la relación laboral y no sobrepase el límite del contrato de trabajo.

Por tanto, para sintetizar, solo será necesario informar previamente al trabajador acerca de la implantación de las medidas de localización y de los derechos que le corresponde, pero no será necesario el consentimiento para el tratamiento de datos.

Con todo lo anterior, se observa que los datos de localización gozan de la consideración de datos personales debido a que se refieren a una "persona física identificada o identificable".[66]

### *3.2.3 Vehículos*

En este apartado se analizará el caso de los vehículos utilizados por los trabajadores**,** donde la recogida de datos proviene de la instalación de un sistema de seguimiento de GPS en el vehículo. Como se ha mencionado, el empresario debe de informar claramente al trabajador de la instalación del dispositivo que registrará los movimientos del vehículo durante el uso del vehículo por parte del trabajador. Sin embargo, no será necesario tener el consentimiento del trabajador.

En este supuesto, el trabajador no posee la facultad de oposición, puesto que en virtud del artículo 20.3 ET, se encuentra dentro de las potestades de dirección y control del empresario y al existir una relación contractual, el empresario tiene la facultad de implantar esta medida para vigilar el cumplimiento de las obligaciones contractuales.

Y así lo señala la AEPD en su informe 193/2008 donde vuelve a mencionar que será necesario el conocimiento por parte del trabajador antes de que los mecanismos se implementen y cuando la empresa use dicho sistema. [67]

Para facilitar el conocimiento a los trabajadores, el Grupo de Trabajo del Artículo 29 recomienda que en cada vehículo se situé en un lugar visible la información relativa al uso de un sistema de geolocalización.[68]

---

[66] Mercader Uguina, J. R., *op. cit. p. 128*

[67] Informe 193/2008 de la AEPD, consulta del tratamiento de datos emitidos por el sistema de GPS instalados en los vehículos

[68] El Grupo de trabajo del Artículo 29 fue creado por la Directiva 95/46/CE, de 24 de octubre de 1995, como un órgano consultivo independiente del que son miembros las Autoridades de Protección de Datos de todos los Estados miembros, el Supervisor Europeo de la Protección de Datos y la Comisión Europea.

El Grupo de Trabajo del Artículo 29 tiene entre sus funciones, de conformidad con el artículo 30 de la Directiva, emitir dictámenes y recomendaciones así como estudiar toda cuestión relativa a la aplicación de las disposiciones

Por tanto, el trabajador sujeto a dicho control debe de tener conocimiento a lo largo de la jornada laboral de que está siendo vigilados, y los datos relacionados con la conducción y localización están siendo almacenados.

Será en la sentencia del TSJ de Asturias 3058/2017, de 27 de diciembre, donde se fijen los límites del empresario y la facultad de control y dirección recogida en el artículo 20.3 ET. En esta sentencia se establece que una vez haya finalizado la jornada laboral, el trabajador deja de prestar servicios laborales a la empresa y por tanto deberá de funcionar cualquier sistema de control o vigilancia que tenga como finalidad el control del desarrollo de la actividad laboral e intervenga con la intimidad personal de empleado[69].

Para el caso del vehículo, el empresario no dispondrá de la legitimación para emplear los dispositivos de control que le permitan recoger los datos relativos al uso del vehículo por parte del trabajador una vez haya finalizado la jornada laboral.

Por tanto, al finalizar la jornada laboral, y ante la falta de consentimiento de los trabajadores que impide al empresario recoger datos de localización fuera del horario de trabajo, la empresa está obligada a desactivar el sistema de posicionamiento global instalado de forma que no capte datos fuera del horario de trabajo. Se recoge lo siguiente en la sentencia: "la empresa demandada a que garantice a los representantes de los trabajadores que el dispositivo de geolocalización implantado en los vehículos de motor utilizados por los trabajadores no estará operativo a partir del momento en que finalice la jornada laboral".[70]

---

nacionales tomadas para la aplicación de la mencionada Directiva con vistas a contribuir a su aplicación homogénea. El Dictamen del Grupo de Trabajo del Artículo 29 citado es la consecuencia de la petición realizada por la Comisión Europea el 6 de mayo de 2014 invitándola a "emitir recomendaciones sobre cómo gestionar los asuntos relativos a la privacidad y protección de datos a nivel europeo y qué acciones deberían tomarse para subrayar el establecimiento de un marco adecuado" con vistas a proveer indicaciones prácticas a los legisladores y reguladores, tanto a nivel europeo como nacional, incluyendo a las autoridades civiles de aviación, hasta el público en general.

[69]STSJ 3058/2017, de 27 de diciembre (disponible en http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=AN&reference=8283089&links=veh%C3%ADculo%20Y%20telecomunicación&optimize=20180208&publicinterface=true ; última consulta 4/04/2019)

[70] STSJ Asturias 3058/2017, de 27 de diciembre *op. cit.*

De tal forma, que la solución que ofrece el TSJ Asturias será que el sistema GPS pueda ser desactivado cuando la jornada laboral finalice.

### *3.2.4 ¿Qué datos pueden ser recabados?*

Conforme la Resolución de Archivo de la AEPD del E/742/2008, los datos que se podrán recabar con el sistema GPS serán los siguientes:

> Hora de arranque de la furgoneta;
> Hora de aparcamiento de la furgoneta;
> Puntos de paso y paradas de la furgoneta;
> Velocidad de las furgonetas, tanto máxima como media;
> Consumos del vehículo, siendo esto una simulación en función de los kilómetros recorridos;
> Horas de funcionamiento de la furgoneta y horas en las que está parada;
> Kilómetros realizados por jornada;
> Desviación de horas de la furgoneta en función de un horario de trabajo configurable.[71]

### *3.2.5 Limites*

Los empresarios están legitimados para emplear el sistema GPS para controlar a sus trabajadores de acuerdo con el artículo 20.3 ET.

Sin embargo, dicha facultad de control se limita al horario laboral. Por tanto, una vez finalice la jornada laboral, como hemos visto anteriormente, se deberá de desactivar el sistema GPS.

Al dejar de estar operativo, el empresario no estará cometiendo infracciones ilegitimas en la intimidad de sus empleados, respetando sus derechos fundamentales.

Además, según el Grupo de Trabajo del Artículo 29 en el Dictamen 5/2005, sobre el uso de los datos de localización, impone otro limite, al reducir el ámbito de tratamiento de los datos, ya que "el tratamiento de datos de localización relativos a empleados ha de corresponder a una necesidad específica de la empresa que guarde relación con su actividad".[72]

---

[71] Informe E/742/ 2008 AEPD, en Mercader Uguina, J. R., *op. cot.,* p. 131

[72] Dictamen 5/2005 sobre el uso de los datos de localización con vistas a prestar servicios con valor añadido del Grupo de Trabajo del Artículo 29 (WP 115, 25 de noviembre de 2005).

En cuanto al juicio de proporcionalidad, para que el empresario no cometa una vulneración del derecho fundamental del artículo 18.4 CE, la recogida de datos de carácter personal deberá de ser "adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido".

Habrá que atender al Dictamen 5/ 2005 del Grupo de Trabajo del Artículo 29 sobre el uso de los datos de localización con vistas a prestar servicios con valor añadido, en el cual se recoge que:

> El Grupo considera que el tratamiento de datos de localización relativos los empleados ha de corresponder a una necesidad especifica de la empresa que guarde relación con su actividad…. Por el contrario, el Grupo considera que el tratamiento de datos es excesivo en el caso de que los empleados puedan organizar libremente sus planes de viajes o cuando se lleve a cabo con el único fin de controlar el trabajo de un empleado, siempre que pueda hacerse por otros medios…. En cualquier caso, el requisito relativo a la finalidad implica que un empresario no debería recoger los datos de localización en relación con un empleado fuera de su tiempo de trabajo. Por consiguiente, el Grupo recomienda que se dote a los equipos puestos a disposición de los empleados, y especialmente a los vehículos que también puedan ser utilizados como fines privados, de un sistema que les permite desactivar la función de localización.[73]

De tal manera que se deberá estudiar la relación existente entre la implementación de un sistema de localización y los fines perseguidos por el empresario, siempre respetando que el horario de seguimiento esté limitado al horario de trabajo para así no vulnerar los derechos fundamentales del trabajado sujeto a esta medida.

En referencia a la **conservación** de los datos de localización, de acuerdo con las previsiones del RGPD, deberán de ser "adecuados, pertinentes y limitados a lo necesario para los fines para los que sean tratados". Deberán de ser cancelados cuando se haya logrado la finalidad para la cual fueron obtenidos y por tanto será importante" [74], garantizar que se limite a un mínimo estricto su plazo de conservación para proteger al ciudadano de un uso ilícito de sus datos.

Además, como señala el Grupo de Trabajo del artículo 19 en el dictamen 13/2011, el periodo de retención de los datos que se hayan obtenido de servicios de geolocalización, no será

---

[73] Dictamen 5/2005 sobre el uso de los datos de localización con vistas a prestar servicios con valor añadido del Grupo de Trabajo del Artículo 29 (WP 115, 25 de noviembre de 2005)

[74] RGPD

"superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente.".[75]

Como consecuencia, los datos deberán de ser suprimidos cuando haya transcurrido un periodo de tiempo justificado.

## 3.3 Uso de dispositivos digitales

### *3.3.1 Concepto de correo electrónico*

Hoy en día, el correo electrónico es considerado como el principal "medio de comunicación en la empresa", convirtiéndose en un "instrumento de trabajo por los trabajadores".[76]

El correo electrónico se ha convertido en un instrumento de trabajado de uso diario, siendo una herramienta necesaria para el desarrollo de la actividad laboral, siempre y cuando se reserve su uso a fines laborales y no a los personales.

La STC 170/2013, de 7 de octubre señala que al tener el correo electrónico naturaleza corporativa empresarial, destinado a usos laborales, no podrá considerarse de uso propio o intimo por parte del trabajador, solo como uso profesional.[77]

De tal forma es conveniente analizar los problemas que surgen cuando los medios electrónicos proporcionados por la empresa destinados a un uso profesional, en cambio son utilizados para actividades privadas. Ya que el indebido uso de los medios informáticos por parte del trabajador en el ámbito laboral implica una trasgresión de la buena fe contractual.[78]

Además, el Tribunal Europeo de Derechos Humanos, (en adelante TEDH) en su sentencia del

---

[75] Dictamen 13/2011sobre los servicios de geolocalización en los dispositivos móviles inteligentes del Grupo de Trabajo sobre protección de datos establecido por el Artículo 29 (16 de mayo de 2011)

[76] Cardona Rubert, M. B., "Las relaciones laborales y el uso de las tecnologías informáticas"**,** *Lan Harremanak*, núm. 1, 2003, p. 166.

[77] STC 170/2013, de 7 de octubre (BOE núm. 267, de 07 de noviembre de 2013). (disponible en http://hj.tribunalconstitucional.es/es/Resolucion/Show/23616 ; última consulta 5/04/2019).

[78] Martínez Fons, D., *El poder de control del empresario en la relación laboral*, Consejo Económico y Social, Madrid, 2002 p.143

3 de abril de 2007 protege los correos electrónicos enviados desde el centro de trabajo al incluirlos "en el ámbito de protección del art. 8 CEDH, por cuanto pueden contener datos sensibles que afecten a la intimidad y al respeto a la vida privada"[79]

### *3.3.2 Dirección de correo electrónico*

La dirección de correo electrónico es considerada como dato personal de acuerdo el Informe 039/2007 de la AEPD, señalando que a pesar de que no muestren características referentes al comportamiento de las personas, sin embargo, sí que permiten su identificación.

Además, tendrán la consideración de dato personal no solo aquellas direcciones de correo electrónico que reflejen información del titular como el nombre o los apellidos, sino que también las direcciones de correo que sean "una denominación abstracta, o una combinación de números y letras sin significado".[80]

### *3.3.3 Facultad del empresario*

Martínez Fons justifica que el control del empresario es "un control legalmente reconocido circunscrito a la actividad de verificación en los términos o medios permitidos"[81]. Por tanto, es un control reconocido al amparo del artículo 20.3 ET para verificar si el trabajador usa los medios electrónicos de la empresa de manera correcta a través de las medidas legales pertinentes.

Como hemos visto anteriormente, dicha facultad viene limitada por el respeto de la dignidad del trabajador mediante el establecimiento de unas garantías que bloqueen sobrepasar los derechos fundamentales de los trabajadores.

---

[79] STEDH de 3 de abril de 2007**,** asunto Copland contra Reino Unido, núm. 62617/00 (disponible en https://hudoc.echr.coe.int/spa#{%22fulltext%22:[%22\%22CASE%20OF%20COPLAND%20v.%20THE%20UNITED%20KINGDOM%20-%20[Spanish%20Translation]%20by%20the%20Spanish%20Ministry%20of%20Justice\%22%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22]}; última consulta el 5/04/2019).

[80] Mercader Uguina, J. R., *op. cit.* p 110

[81] Martínez Fons, D., *op. cit*. p. 25

Además, según la STC 170/2013, de 7 de octubre, los mensajes que han sido enviados por el correo corporativo serán considerados como prueba igualmente lícita.

### *3.3.4 Limites*

De nuevo, hay que tener como referencia el principio de proporcionalidad como parámetro para ajustar el control empresarial al respeto de los derechos fundamentales del trabajador en todo momento.

Debemos de atender a la finalidad que pretende lograr dicho control por parte del empresario, por ello, el contrato de trabajo limitada la facultad de control al no poder sobrepasar aquellos aspectos de la vida personal que no tengan una relación directa con el contrato de trabajo. [82]

Es muy importante intentar alcanzar una solución en la que se mantenga un equilibrio entre el legítimo ejercicio de la potestad de control y la intimidad del trabajador. Es por ello que el Dictamen 2/2017 del Grupo de Trabajo del Artículo 29 resalta la importancia de que los empresarios deben tener en cuenta el principio de minimización de datos a la hora de decidir sobre el despliegue de nuevas tecnologías. [83]

Para solucionar el posible conflicto que puede producirse entre la facultad de control y los derechos fundamentales del trabajador, la STS 966/2006, de 26 de septiembre establece que el respeto a los derechos fundamentales del trabajador no puede

> convertirse en un impedimento permanente del control empresarial, porque, aunque el trabajador tiene derecho al respeto a su intimidad, no puede imponer ese respeto cuando utiliza un medio proporcionado por la empresa en contra de las instrucciones establecidas por ésta para su uso y al margen de los controles previstos para esa utilización y para garantizar la permanencia del servicio.[84]

Es de suma importancia mencionar que respeto al secreto de las comunicaciones no se entenderá como vulnerado cuando exista una prohibición expresa previa del uso privado o

---

[82] Goñi Sein, J.L., *El respeto a la esfera privada del trabajador*. Civitas, Madrid, 1988, p.116 y 117.

[83]Dictamen 2/2017 sobre el tratamiento de datos en el trabajo del Grupo de Trabajo del Artículo 29 (WP 249, 8 de junio de 2017)

[84]STS 966/2006, de 26 de septiembre (FJ 4) (disponible en https://www.iustel.com/diario_del_derecho/noticia.asp?ref_iustel=1025408 ; última consulta 6/04/2019).

personal de la cuenta de correo electrónico facilitada al trabajador. [85]

### *3.3.5 Información*

La información al trabajador acerca de medidas de monitorización al uso del correo electrónico debe ser esencial.

Sin embargo, al existir una relación laboral el consentimiento no será necesario recabar el consentimiento expreso para el control del uso del correo electrónico, aunque dicha intromisión deberá de estar debidamente justificada.

Por tanto, la información que reciban los trabajadores acerca de las políticas de la empresa en materia de uso del correo electrónico debe de ser clara, pero "no se trata en absoluto de que el trabajador conozca el detalle de políticas de seguridad que pueden afectar a ámbitos que la empresa necesita proteger" [86].

Lo más importante es que los trabajadores deben de conocer las condiciones de uso de los medios informáticos de los que dispone cada trabajador, Toscani Giménez y Calvo Morales, resaltan la importancia de que el trabajador sea conocedor de que:

> la conducta debe estar prohibida expresamente y debe quedar meridianamente explícito qué conductas están permitidas y cuáles no. Si no es así, la empresa deberá comunicar previamente la prohibición antes de poder fiscalizar el correo electrónico de los trabajadores y solo podrá utilizar la información que haya conseguido para los fines que hubiera comunicado al trabajador. [87]

Finalmente, comentar que para que el control sea lícito la empresa debe de establecer las "reglas de uso de los medios" y proporcionar la debida información "a los trabajadores de que va existir control y de los medios que han de aplicarse en orden a comprobar la corrección de los usos,

---

[85] STC 170/2013, de 7 de octubre *op. cit.*

[86] Mercader Uguina, J. R. *op., cit.* p 112

[87] Toscani Gimenez, D. y Calvo Morales, D. "El uso de internet y el correo electrónico en la empresa: límites y garantías" *Nueva Revista Española de Derecho del Trabajo,* núm. 165, 2014, p. 206

así como de las medidas que han de adoptarse en su caso para garantizar la efectiva utilización laboral del medio cuando sea preciso"[88]

Por otro lado, según la Recomendación CM/Rec (2015)5 del Comité de Ministros del Consejo de Europa a los Estados miembros relativa al tratamiento de datos personales en el contexto del empleo, prevé en su apartado 10.2 que la información que el empleador debe proporcionar a sus empleados debe ser la siguiente:

- las categorías de datos personales que deben tratarse y una descripción de los fines del tratamiento
- los destinatarios o categorías de destinatarios de los datos personales
- los medios de que disponen los trabajadores para ejercer los derechos enunciados en el apartado 11 de la presente Recomendación, sin perjuicio de los más favorables previstos en la legislación nacional o en su ordenamiento jurídico
- cualquier otra información necesaria para garantizar un tratamiento justo y legal. [89]

### *3.3.6 Comentario TEDH caso Barbulescu II*

Esta sentencia será incorporada en nuestro ordenamiento jurídico como principal criterio interpretativo para nuestros tribunales españoles a la hora de establecer los requisitos para un control del correo electrónico por parte del empresario lícito y no lesivo de los derechos fundamentales del trabajador.

Se analiza el despido disciplinario de un trabajador que utilizaba la cuenta de mensajería creada por la empresa para el desarrollo de su actividad laboral, en la que se incluía responder a las consultas de los clientes, pero el trabajador utilizó el servicio de mensajería para fines personales, no respetando el uso exclusivamente profesional. Por tanto, la empresa procede al despido disciplinario por no haber cumplido la normativa interna de la empresa en la cual se prohibía el uso de recursos empresariales para fines personales.

En este caso, a diferencia de todas las instancias precedentes, si se procede a estimar la demanda interpuesta por el Sr. Barbulescu, donde se aprecia la violación del art. 8 del CEDH al no ser

---

[88] STS 966/2006, de 28 de septiembre *op. cit.*

[89] Recomendación CM/Rec (2015) 5, sobre el tratamiento de datos personales en el contexto del empleo, Comité de Ministros del Consejo de Europa (1 de abril de 2015) (disponible en https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c3f7a ; última consulta 7/0472019)

concluyente que "hubiera sido informado con antelación del alcance y naturaleza de la supervisión efectuada por su empleador o de la posibilidad de acceder al contenido de sus comunicaciones."[90]

Esta sentencia da un paso más en la monitorización de las comunicaciones de los trabajadores, estableciendo los requisitos que deben ponderarse para que no se proceda a una vulneración de los derechos protegidos por el artículo 8 CEDH.

Los requisitos del juicio de proporcionalidad son los siguientes:

a) el grado de intromisión del empresario;
b) la concurrencia de legítima razón empresarial justificativa de la monitorización
c) la inexistencia o existencia de medios menos intrusivos para la consecución del mismo objetivo
d) el destino dado por la empresa al resultado del control
e) la previsión de garantías para el trabajador[91]

Por tanto, observamos que el TEDH dicta unos requisitos rígidos, aumentando así las garantías de protección a la privacidad del empleado. De tal forma que siempre que respete los requisitos establecidos por el TEDH podrá el empresario vigilar los correos.

De acuerdo con lo anterior, resaltamos la importancia de una comunicación previa a los empleados acerca de la posible monitorización del correo electrónico y siempre justificando la existencia de un motivo que lleve al empresario a adoptar esta medida para así garantizar una relación equilibrada entre el control empresarial y la privacidad del trabajador.

En cuanto a lo ocurrido en esta sentencia, se estima que no se protegieron debidamente el respeto a la vida privada ya que no se produjo una comunicación previa acerca de la monitorización de las comunicaciones y antes del establecimiento de la misma.

---

[90] STEDH 61496/08 de 5 de septiembre de 2017, asunto Barbulescu II contra Rumania (disponible en https://hudoc.echr.coe.int/spa#{%22fulltext%22:[%22barbulescu%20II%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-177082%22]} ; última consulta el 5/04/2019).

[91] STEDH 61496/08 de 5 de septiembre de 2017, asunto Barbulescu II contra Rumania *op. cit.*

El TEDH resalta que cuando el empresario tome medidas de monitorización deben de ser lo más adecuadas posibles a la finalidad que se pretende lograr, para así proteger los derechos de los empleados frente a abusos y vulneración de los derechos humanos.

La doctrina del TEDH se puede articular en 3 conceptos fundamentales que deben de cumplirse caso por caso para así salvaguardar el derecho a la vida privada del trabajador frente al control empresarial.

En primer lugar, debe de existir un principio de transparencia, consistente en proporcionar al trabajador la información previa y "[92]clara" sobre las medidas de monitorización. Por tanto, la información debe de ser previa al inicio de la posible monitorización.

En segundo lugar, hay que justificar que existen sospechas fundadas para vigilar las comunicaciones del trabajador.

En tercer y último lugar, como se ha mencionado anteriormente, habrá que cumplir con los requisitos del juicio de proporcionalidad.

Así se observa que la Gran Sala pretende dotar a los trabajadores de una mayor seguridad jurídica y protección al garantizar una mayor efectividad en la protección de los derechos fundamentales del trabajador en su puesto de trabajo.

[92] SEDH 61496/08, de 5 de septiembre *op. cit.*

## 3.4 Control biométrico

### *3.4.1 Concepto de datos biométrico*

El RGPD define a los datos biométricos en el punto 14 de su artículo 4 de la siguiente forma:

> datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos.[93]

La huella dactilar es un elemento identificable atribuible en exclusiva a una única persona que permite identificar de manera univoca a un individuo.

Como ejemplos de datos biométricos, mencionamos los más utilizados entre los que se encuentran "las huellas dactilares, los modelos retinales, la estructura facial, las voces, pero también la geometría de la mano, las estructuras venosas e incluso determinada habilidad profundamente arraigada u otra característica del comportamiento."[94]

Es por ello, que al ser los datos biométricos un elemento de identificación único de la persona, se convierte necesario que el nuevo RGPD en el punto 1 del artículo 9, incluya los datos biométricos dentro de la categoría especiales de datos personal y de carácter general, su tratamiento estará prohibido cuando tenga como finalidad identificar de manera univoca a una persona.

Así lo establece dicho artículo:

> Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física.[95]

---

[93] Artículo 4. 14 RGPD

[91] Mercader Uguina, J. R., *op. cit.,* p.133

[95] Artículo 9.1 RGPD

Pero, al encontrarnos dentro del ámbito laboral se deberá de prestar especial atención a las exenciones del punto 2 del mismo artículo.

Hasta ahora los datos biométricos se encontraban en el nivel bajo de protección, pero el nuevo RGPD dota a los datos biométricos de una protección adicional catalogándolos como datos especialmente protegidos. Como consecuencia, se exigirá un mayor nivel de diligencia y de seguridad en el tratamiento de los datos biométricos, asegurando al empleado una protección más intensa de sus datos. Dentro de esta reforzada protección, el empresario deberá de configurar unas medidas de protección de carácter adicional.

Como novedad, el RGPD faculta a los Estados Miembros a introducir o limitar nuevas disposiciones específicas en materia de tratamientos de datos especialmente protegidos.

### *3.4.2 Facultad del empresario*

A tenor del artículo 20. 3 ET, el uso del control biométrico se encuentra dentro de las facultades de control por parte del empresario cuando sea proporcional a la naturaleza de la actividad, por lo que habrá que "tener en cuenta la naturaleza de la actividad y de las instalaciones para cuyo acceso se requiere"[96].

Se permite el uso de control de la actividad laboral con control biométrico siempre y cuando, el empresario tenga como finalidad comprobar el cumplimiento del horario laboral fijado en el contrato de trabajo a través del registro de la hora concreta de la entrada y salida del trabajador de las instalaciones de la empresa.

En relación a lo anterior, así lo considera el TSJ de Murcia 47/2010, de 25 de enero de 2010:

> El control de acceso a las instalaciones de la empresa constituye una finalidad legitima, concreta y que fue suficientemente puesta de manifiesto a los trabajadores y que tal medida de control, que vincula la lectura de las huellas digitales a los datos de identidad de los trabajadores existentes en la

[96] Mercader Uguina, J. R., *op. cit.,* p.134

empresa, es adecuada, pertinente y no excesiva.[97]

Habrá que tener en cuenta que para la oportuna implantación de esa medida será necesario cumplir con el principio de minimización, limitando a aplicar esta medida de control cuando sea "necesario, justo para el interesado y transparente".[98]

Antes de la implantación de este instrumento de control, el empresario deberá de estudiar la posibilidad de implantar otros "métodos alternativos de tratamiento menos intrusivos para la vida privada y siempre que su tratamiento se acompañe de las garantías apropiadas debiendo basarse además el medio de tratamiento en métodos científicamente reconocidos y sometidos a las exigencias estrictas de seguridad y proporcionalidad".[99]

Por ello, sería recomendable proceder a una valoración previa de la necesidad de la implantación de la medida para estudiar la relación entre la finalidad y el uso.

### *3.4.3 Limites*

Previamente, a tenor del artículo 35. 3 b) RGPD, se deberá de realizar una evaluación del impacto en la protección de datos (en adelante EIPD) con anterioridad al tratamiento cuando se proceda al " tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1".[100]

Por tanto, la empresa deberá de proceder a un análisis de riesgo donde se contemple todos los posibles riesgos y las medidas de actuación.

De acuerdo con el artículo 35.7 RGPD, la evaluación de impacto deberá incluir lo siguiente:

> a) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento

---

[97] STSJ Murcia 47/2010, de 25 de enero (disponible en http://www.poderjudicial.es/search/doAction?action=contentpdf&databasematch=AN&reference=5144272&links=biometrico&optimize=20100325&publicinterface=true ; última consulta el 5/04/2019).

[98] Mercader Uguina, J. R., *op. cit.,* p.134

[99] Mercader Uguina, J. R., *op. cit.,* p.135

[100] Artículo 35. 7 RGPD

b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad
c) una evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1
d) las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas. [101]

Por tanto, lo que se pretende con la EIPD es realizar un completo análisis de todos los posibles riesgos y peligros que podrían producirse a la hora del tratamiento de datos a gran escala y así anticiparse a la resolución de los mismo con las medidas previstas.

De tal forma, el EIPD permite "identificar, evaluar y tratar los riesgos asociados al tratamiento de datos personales, y así, poder asegurar los principios de protección de los datos garantizando los derechos y libertades de los interesados".[102]

La finalidad del EIPD será esclarecer y determinar qué medidas se deberían adoptar si reducir los posibles riegos y así reducir el impacto negativo en los derechos fundamentales de los interesados, actuando de manera preventiva y anterior al tratamiento.

Concretamente, si nos encontramos dentro de una empresa multinacional que cuenta con una gran plantilla de cientos de empleados, podemos decir que en el caso de que la empresa se expanda a gran escaña regional o que cuente con un gran colectivo, si será necesario procederá una evaluación del impacto.

Por otro lado, en el RGPD, no se enumeran cuáles son las medidas de protección específica para los datos biométricos, si no que se deberán de adoptar las apropiadas en función del volumen de trabajadores de la empresa.

### *3.4.4 Información*

A pesar de que en el artículo 9.1 RGPD se prohibía el tratamiento de datos biométricos que permitan identificar unívocamente a una persona, sin embargo, en el punto 2, letra b de ese

[101] Artículo 35. 7 RGPD

[102] Guía del derecho fundamental a la protección de datos de carácter personal *op. cit*

mismo artículo se excepciona cuando el tratamiento sea necesario al mediar una relación laboral y se deban cumplir con las obligaciones y derechos de la relación contractual existente.

Además, la AEPD, admite el tratamiento de datos biométricos por parte del empleador para comprobar el cumplimiento de las obligaciones laborales, así lo recoge en su informe 0324/2009:

> En efecto, en el ámbito de la relación jurídica que existe entre los trabajadores y el empresario al que prestan sus servicios, debe entenderse adecuado que éste recabe los datos que sean precisos para el normal desenvolvimiento de la misma y, dentro de estos datos, parece adecuado que se recaben del trabajador los necesarios para su identificación, a efectos de garantizar las medidas de seguridad que se consideren oportunas por parte de la empresa para que por la misma se pueda comprobar el grado de cumplimiento de las obligaciones que competen a los trabajadores.[103]

A diferencia del artículo 6.2 RGPD que prevé que "cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento".

Sin embargo, con el nuevo RGPD los datos biométricos obtienen la calificación de datos especialmente protegidos y por ello se refuerza su protección y sus garantías.

En cuanto a la información que deben de recibir los empleados, será requisito indispensable para que el control del empresario no sea considerado como intromisión ilegítima, la debida advertencia e información con carácter previo de la instalación de la medida.

Finalmente, al destinar al uso laboral los datos biométricos, no será necesario el consentimiento del trabajador, pero si la pertinente información previa. Si, por el contrario, el uso fuese otro distinto que el control laboral, entonces el consentimiento si se convertirá necesario para el tratamiento de los datos personales.

---

[103] Informe 0324/2009 de 28 de febrero de 2006 de la AEPD, consulta de implantar un sistema para el control horario de los trabajadores basado en la lectura de la huella digital.

## 3.5 Bring your own device

### *3.5.1 Concepto*

Bring your own device o trae tu propio dispositivo, es una práctica empresarial donde se permite a los trabajadores hacer uso de sus propios dispositivos portátiles personales para cumplir con sus tareas laborales y acceder a información corporativa.[104]

Por tanto, se compatibiliza un uso mixto ya que el mismo dispositivo será utilizado para fines personales y corporativos.

### *3.5.2 Riesgos*

Con carácter habitual, en un solo dispositivo se suelen almacenar datos personales y datos corporativos.

Para proteger los datos corporativos, el Instituto Nacional de Ciberseguridad, recomienda al empleado la incorporación de unas medidas de seguridad en los dispositivos utilizados por la empresa. Se observa que se pretende proteger el almacenamiento de información sensible y privada garantizando una fuerte protección mediante el uso del cifrado.[105]

Por tanto, el cifrado es una medida esencial para impedir el acceso a la información en caso de pérdida del dispositivo o robo.

Para separar los datos personales y privados de los corporativos, el Grupo de Trabajo del Artículo 29 en el dictamen 2/2017 indica que deberán de "establecerse medidas adecuadas para distinguir el uso privado y corporativo del dispositivo" y serán los empleados los que deben de

---

[104] Fernández Burgueño, P., "La obligación de cifrado de la información en el Reglamento Europeo de Protección de datos", *Diario La Ley Legal Management*, núm.3, 2017, p. 27

[105] Instituto Nacional De Ciberseguridad (INCIBE), *Dispositivos móviles personales para uso profesional (BYOD): una guía de aproximación para el empresario*, Madrid, 2017

"implementar métodos por los cuales sus propios datos sean transferidos de forma segura entre esos dispositivos y su red".[106]

### *3.5.3 Medidas de protección*

Al tratarse de dispositivos móviles con conexión a internet, uno de los principales riesgos al que se expone es el acceso a redes inalámbricas desconocidas. Debido a esa conexión, el dispositivo queda expuesto a ciberataques, sin embargo, el Centro Criptológico Nacional (en adelante CNN-CERT) recomienda adoptar "mecanismos de cifrado fuerte", como el uso de VPN.[107]

Además, para evitar el acceso a los datos en caso de robo o extravío, el CNN- CERT sugiere "el uso de contraseñas de acceso, bloqueo de dispositivos, cifrado de información, así como el derecho institucional a borrar remotamente los datos corporativos del equipo". [108]

De tal forma que, aunque se pierda el control sobre el dispositivo, el empresario y el trabajador cuentan con las medias de seguridad oportunas para impedir el acceso a los datos por personas no autorizadas, protegiendo la confidencialidad de los mismo.

Finalmente, será el empresario el que deba de redactar e implantar las medidas necesarias acerca del uso de los dispositivos dentro del ámbito laboral para asegurar un entorno altamente protegido. Con el desarrollo de las políticas de uso y los requisitos de utilización, los riesgos para la seguridad serán reducidos y controlados.

### *3.5.4 Control del empresario*

Para evitar controversias en el ejercicio de las funciones de control por parte del empresario en los dispositivos que contengan información de carácter personal, la mejor opción para evitar una vulneración de los derechos fundamentales del trabajador, será utilizar mecanismos o

---

[106] Mercader Uguina, J. R., *op. cit*., p.139

[107] Fernández Burgueño, P., *op. cit.,* p.18

[108] Fernández Burgueño, P., *op. cit.,* p.18

aplicaciones que permitan separar los datos corporativos de la información personal.

De acuerdo con el artículo 20.3 ET el empresario podrá ejercer el control sobre los dispositivos informáticos que les proporciona la empresa para el desarrollo de su actividad laboral. No obstante, en este caso los medios no son proporcionados por el empresario, si no que el propietario es el propio trabajador.

Por lo tanto, debemos preguntarnos donde se encuentra el fundamento que legitime el control empresarial, ya que no será en el artículo 20.3 ET, pero si el artículo 18 ET donde se legitima el control sobre los elementos personales del trabajador solo en circunstancias excepcionales.

## 3.6 Teletrabajo

### *3.6.1 Concepto de teletrabajo*

Con la llegada de las nuevas tecnologías de la información han surgido nuevas modelos a la hora de desarrollar las actividades laborales, como el teletrabajo.

El Acuerdo Marco Europeo sobre Teletrabajo define el teletrabajo como "forma de organización y/o de realización del trabajo, utilizando las tecnologías de la información en el marco de un contrato o de una relación de trabajo, en la cual un trabajo que podría ser realizado igualmente en los locales de la empresa se efectúa fuera de estos locales de forma regular".

### *3.6.2 Derechos del trabajador*

Anteriormente, en el artículo 13 ET no se recogía la facultad de vigilancia del empresario, esto se debe a que al estar desarrollando una actividad laboral no se suprimen las facultades de control y vigilancia por parte del empresario reconocidos en el artículo 20.3 ET.

El artículo 13 ET reconoce los mismos derechos a teletrabajadores que a "los que prestan sus servicios en el centro de trabajo de la empresa, salvo aquellos que sean inherentes a la realización de la prestación laboral en el mismo de manera presencial".

El empresario deberá de garantizar la protección de los datos del teletrabajador en el desarrollo de su actividad laboral y a su vez deberá de "respetar la vida privada del teletrabajador".[109]

### *3.6.3 Facultad del empresario*

En el supuesto de que el empresario implante un sistema de videovigilancia, "éste debe ser proporcional al objetivo perseguido e introducido según lo establecido en la Directiva 90/270 relativa a las pantallas de visualización"[110]

[109] Apartado 5 del Acuerdo Marco Europeo sobre Teletrabajo (16 de julio de 2002, European Social Partners)

[110] Apartado 6 del Acuerdo Marco Europeo sobre Teletrabajo *op. cit.*

Por tanto, el empleador podrá ejercer su facultad de control reconocida en el artículo 20. 3 ET respetando la vida privada del trabajador y protegiendo los datos con los que trabaja el empleado.

El empleador podrá emplear "sistemas de videovigilancia, controles sobre el ordenador, intervención de las conversaciones telefónicas" [111]en el ejercicio del control de la actividad laboral del teletrabajador.

### *3.6.4 Control de la jornada laboral*

A diferencia de los trabajadores en la sede empresarial, los teletrabajadores no pueden quedar sujetos a un control biométrico para registrar la hora de entrada y salida. Por tanto, los teletrabajadores, a diferencia de los trabajadores presenciales, sufren la ausencia de un control directo por parte del empleador.

La controversia surge entorno a la STSJ de Castilla y León de 3 de febrero de 2016, donde se suscita la problemática de contabilizar las horas extraordinarias de los teletrabajadores.

Por un lado, la empresa no había instalado ningún instrumento de control de la jornada laboral. Por lo que la empresa justifica la no adopción de un sistema de control para evitar cualquier vulneración del derecho fundamental a la intimidad e inviolabilidad del domicilio.

El Tribunal declara que "el control del tiempo de trabajo es responsabilidad de la empresa", y también deberá de "establecer las pautas necesarias sobre tiempo de trabajo para garantizar el cumplimiento de los límites de jornada y descansos".[112]

De tal forma, que será la empresa la responsable de fijar unas políticas que regulen el teletrabajo y el control del mismo. En consideración con la anterior, al ser la empresa responsable de

---

[111] Poquet Catala, R., "La protección del derecho a la intimidad del teletrabajador", *Revista jurídica de los Derechos Sociales*, vol.8, núm.1, 2018 p.118

[112]STSJ de Castilla y León, 00198/2016, de 3 de febrero (disponible en http://www.poderjudicial.es/search/doAction?action=contentpdf&databasematch=AN&reference=7602368&links=%222229%2F2015%22&optimize=20160218&publicinterface=true;; última consulta el 8/04/2019).

adoptar las medidas oportunas de control, en este caso deberá a proceder al abono de las horas extraordinarias del teletrabajador al no haber adoptado las medidas oportunas.

Asimismo, se presumirá "*iuris tantum* que la falta de regulación y control del trabajo a distancia puede conllevar la declaración un incumplimiento de laboral, en este caso, sobre la realización de horas extraordinarias por encima del preceptivo límite". [113]

Esta sentencia, sirve de precedente para que las empresas opten por regular los instrumentos de control de la jornada laboral para así evitar reclamaciones de los teletrabajadores por la realización de horas extraordinarias, sin que ello suponga una vulneración de la intimidad del teletrabajador.

[113] Preciado Pérez, I,. "El teletrabajo: luces y sombras de una herramienta de flexibilidad laboral aún por explorar" **,** *Wolters Kluwer,* núm.9159, 2018, p. 6

# 4 INSTITUCIONES REGULADORAS

## 4.1 Agencia Española de Protección de Datos

En este apartado mencionamos la importancia de la AEPD como un órgano de control independiente que tiene como principal objetivo velar por el cumplimiento y aplicación de las normas sobre la protección de datos. A su vez, busca garantizar y proteger ante cualquier tipo de vulneración el derecho fundamental a la protección de datos de carácter personal.

En cuanto al régimen jurídico, la AEPD es un ente de derecho público con personalidad jurídica propia. Es un organismo independiente, que actúa con total independencia en el ejercicio de sus funciones de las Administraciones Publicas.

Al ser una autoridad estatal independiente cuenta con un estatuto propio, aprobado por el Real Decreto 428/1993, de 26 de marzo, donde se desarrolla de nuevo lo recogido en el Titulo VI de la nueva LOPD.

Entre sus principales funciones, resaltamos la importancia de su papel a la hora de garantizar la aplicación y el cumplimiento de la ley en materia de protección de datos, para así defender los derechos fundamentales de los ciudadanos.

Por tanto, cabe destacar la importancia de su función de control, ya que se encarga de velar por la correcta aplicación del RGPD y del resto de normativa aplicable en materia de protección de datos.

Además, la AEPD se encuentra al servicio de los ciudadanos ya que se encarga de resolver las reclamaciones y denuncias planteadas y proporcionar información sobre los derechos que tiene reconocidos por la ley.

# 5 CONCLUSIONES

Primera. El derecho a la protección de datos es configurado como un derecho de carácter fundamental y autónomo que guarda una estrecha relación con el derecho a la intimidad.

Segunda. La firma de un contrato laboral no implica la renuncia del empleado a los derechos fundamentales constitucionalmente reconocidos, sino que experimentan una modulación al estar sujetos al control del empresario, pero las medidas empresariales deberán de superar siempre un triple test de proporcionalidad, por lo que deben de ser idóneas, necesarias y proporcionales.

Tercera. Se observa que el uso de las nuevas tecnologías de la comunicación e información (TIC) han sido determinantes a la hora de desarrollar de un nuevo modo la actividad laboral, generando nuevas controversias entre empleados y empleador. Es por ello, que será necesario una mayor regulación a nivel constitucional y legislativo acerca del uso de las TIC en el desarrollo de la actividad laboral.

Cuarta. El conflicto entre el poder de control del empresario reconocido en el artículo 20.3 ET y los empleados, nace al equiparar que el simple conocimiento del trabajador del posible uso de instrumentos de control sobre el uso de las TIC equivale a su consentimiento. Por tanto, el empresario debe de respetar ciertos límites en las medidas adoptadas para garantizar la no vulneración de los derechos de los trabajadores.

Quinta. La STC 39/2016, de 3 de marzo, crea un giro jurisprudencial respeto del uso de cámaras de videovigilancia al no contemplar que sea necesario información adicional previa a los trabajadores sobre el uso de este sistema como medida de control, ya que estima que será suficiente la colocación de un distintivo informativo en un lugar visible.

Sexta. Para evitar cualquier uso personal del correo electrónico u otro sistema de comunicación, el empleado deberá de haber recibido la información correspondiente sobre la intervención del empresario en los medios de comunicación que estén destinados al uso profesional.

Séptima. El TEDH en su sentencia de 5 de septiembre de 2017, garantiza una mayor seguridad a los trabajadores al fortalecer los requisitos para establecer un control empresarial en las comunicaciones de los empleados. Se estipulan requisitos más estrictos y recomienda el establecimiento previo de unas normas de uso de las herramientas informáticas. Será la propia

sentencia la que determine unas pautas para crear unas medidas de control que respeten los derechos de las dos partes.

Octava. En el caso de que las nuevas tecnologías sigan avanzando a la misma velocidad, será recomendable que nuestra legislación recoja y desarrolle nueva normativa actualizada y completa referente a la evolución tecnológica y su aplicación y uso en el mundo laboral.

Novena. Los instrumentos y métodos de control por parte del empresario deben de ser proporcionados y equilibrados a la finalidad que se pretende lograr. Además, se debe de usar el medio menos invasivo posible.

# 6 REFERENCIAS BIBLIOGRÁFICAS

## 6.1 Legislación

### *6.1.1 Comunitario*


Acuerdo Marco Europeo sobre Teletrabajo (16 de julio de 2002, European Social Partners)

Dictamen 13/2011sobre los servicios de geolocalización en los dispositivos móviles inteligentes del Grupo de Trabajo sobre protección de datos establecido por el Artículo 29 (WP 185, 16 de mayo de 2011)

Dictamen 2/2017sobre el tratamiento de datos en el trabajo del Grupo de Trabajo del Artículo 29 (WP 249, 8 de junio de 2017)

Dictamen 5/2005 sobre el uso de los datos de localización con vistas a prestar servicios con valor añadido del Grupo de Trabajo del Artículo 29 (WP 115, 25 de noviembre de 2005)

Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (DO L 201 de 31 de julio de 2002).

Propuesta de Reglamento Del Parlamento Europeo y Del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas (10 de enero de 2017).

Recomendación CM/Rec (2015) 5, sobre el tratamiento de datos personales en el contexto del empleo, Comité de Ministros del Consejo de Europa (1 de abril de 2015) (disponible en https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c3f7a ; última consulta 7/0472019).

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, (DO L 191 de 4 de mayo de 2016).

### *6.1.2 Nacional*

Constitución española (BOE núm.311, de 29 de diciembre de 1978).

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales («BOE» núm. 294, de 6 de diciembre de 2018).

Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores (BOE núm. 255, de 24/de octubre de2015).

Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras. (BOE núm. 296 de 12 de diciembre de 2006).

Informe 0324/2009 de 28 de febrero de 2006 de la AEPD, consulta de implantar un sistema para el control horario de los trabajadores basado en la lectura de la huella digital.

Informe 193/2008 de la AEPD, consulta del tratamiento de datos emitidos por el sistema de GPS instalados en los vehículos.

## 6.2 Jurisprudencia

### *6.2.1 Tribunal Constitucional*

**STC 53/1985, de 11 de abril** (BOE núm. 119, de 18 de mayo de 1985). (disponible en http://hj.tribunalconstitucional.es/es/Resolucion/Show/433 ; última consulta el 27/03/2019).

**STC 89/1985, de 19 de julio** (BOE núm. 194, de 14 de agosto de 1985) (disponible en http://hj.tribunalconstitucional.es/es/Resolucion/Show/469 ; última consulta el 1/04/ 2019).

**STC 24/1993, de 20 de junio** (BOE núm. 47, de 24 de febrero de 1993). (disponible en http://hj.tribunalconstitucional.es/es/Resolucion/Show/2153 ; última consulta el 27/03/2019).

**STC 98/2000, de 18 de mayo** (BOE núm. 119, de 18 de mayo de 2000). (disponible en http://hj.tribunalconstitucional.es/es/Resolucion/Show/4082 ; última consulta el 6/04/2019)

**STC 292/2000, de 30 de noviembre** (BOE núm. 4, de 04 de enero de 2001) (disponible en http://hj.tribunalconstitucional.es/es/Resolucion/Show/4276 ; última consulta el 29/03/2019).

**STC 126/2003, de 30 de julio** (BOE núm. 181, de 30 de julio de 2003***)***. (disponible en http://hj.tribunalconstitucional.es/es/Resolucion/Show/4901; última consulta el 1/04/ 2019).

**STC 196/2004, de 15 de noviembre** (BOE núm. 306, de 21 de diciembre de 2004). (disponible en http://hj.tribunalconstitucional.es/es/Resolucion/Show/5201; última consulta el 1/04/ 2019).

**STC 29/2013, de 11 de febrero** *(BOE núm. 61, de 12 de marzo de 2013). (disponible en http://hj.tribunalconstitucional.es/es/Resolucion/Show/23284* ; última consulta el *3/04/2019).*

**STC 170/2013, de 7 de octubre** (BOE núm. 267, de 07 de noviembre de 2013). (disponible en http://hj.tribunalconstitucional.es/es/Resolucion/Show/23616 ; última consulta el 5/04/2019).

**STC 39/2016, de 3 de marzo** *(BOE núm. 85, de 08 de abril de 2016). (disponible en http://hj.tribunalconstitucional.es/es/Resolucion/Show/24845 ;* última consulta el *3/04/2019).*

### *6.2.2 Tribunal supremo*

**STS 966/2006, de 26 de septiembre** (disponible en https://www.iustel.com/diario_del_derecho/noticia.asp?ref_iustel=1025408 ; última consulta el 6/04/2019).

### *6.2.3 Tribunal Superior de Justicia*

**STSJ Murcia 47/2010, de 25 de enero** (disponible en http://www.poderjudicial.es/search/doAction?action=contentpdf&databasematch=AN&reference=5144272&links=biometrico&optimize=20100325&publicinterface=true ; última consulta el 5/04/2019).

**STSJ de Castilla y León, 00198/2016, de 3 de febrero** (disponible en http://www.poderjudicial.es/search/doAction?action=contentpdf&databasematch=AN&reference=7602368&links=%222229%2F2015%22&optimize=20160218&publicinterface=true ; última consulta el 8/04/2019).

**STSJ Asturias 3058/2017, de 27 de diciembre** (disponible en http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=A

N&reference=8283089&links=veh%C3%ADculo%20Y%20telecomunicación&optimize=20180208&publicinterface=true ; última consulta el 4/04/2019).

### *6.2.4 Tribunal Europeo de Derechos Humanos*

**STEDH de 3 de abril de 2007,** asunto Copland contra Reino Unido, núm. 62617/00 (disponible en https://hudoc.echr.coe.int/spa#{%22fulltext%22:[%22\%22CASE%20OF%20COPLAND%20v.%20THE%20UNITED%20KINGDOM%20-%20[Spanish%20Translation]%20by%20the%20Spanish%20Ministry%20of%20Justice\%22%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22]}

; última consulta el 5/04/2019).

**STEDH 61496/08 de 5 de septiembre** de 2017, asunto Barbulescu II contra Rumania (disponible en https://hudoc.echr.coe.int/spa#{%22fulltext%22:[%22barbulescu%20II%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-177082%22]} ; última consulta el 5/04/2019).

## 6.3 Obras doctrinales y recursos de internet

Álvarez Vélez, Mª. I. (coord.), *Lecciones de Derecho Constitucional*, Tirant lo Blanch, Valencia, 2014

Blázquez Agudo, E. M., "Novedades laborales en la nueva Ley orgánica de protección de datos", *Wolters Kluwer*, núm 50, 2019, (disponible en https://www.smarteca.es/my-reader/SMT2015106_00000000_20190201000000500000?location=pi-5028&searchHighlight=proteccion%20de%20datos%20laboral ; última consulta 1/04/ 2019). pp. 1-19

Cardona Rubert, M. B., "Las relaciones laborales y el uso de las tecnologías informáticas", *Lan Harremanak*, núm. 1, 2003, pp. 157- 173.

Casas Baamonde, M E., "El derecho a la protección de datos de carácter personal en la jurisprudencia del tribunal constitucional*", Anuario de relaciones laborales de España, núm.6,* 2015, pp. 91- 126

Fernández Burgueño, P., "La obligación de cifrado de la información en el Reglamento Europeo de Protección de datos", *Diario La Ley Legal Management*, núm.3, 2017, pp. 1-40

Fernández Rodríguez, J J. *Secreto e Intervención de las comunicaciones e internet.* Thomson Civitas, Madrid, 2004.

Goñi Sein, J.L. *La videovigilancia empresarial y la protección de datos personales*, Aranzadi, Navarra, 2007

Goñi Sein, J.L., *El respeto a la esfera privada del trabajador*. Civitas, Madrid, 1988

Herrán Ortiz, A. I., "El derecho a la protección de datos personales en la sociedad de la información", *Cuaderno Deusto de Derechos Humano*, núm. 26, 2003, pp. 9- 92

Jiménez-Castellanos Ballesteros, I., "Videovigilancia laboral y derecho fundamental a la protección de datos", *Revista andaluza de trabajo y bienestar social*, núm. 136, 2017, pp. 129- 156

Martínez Fons, D., *El poder de control del empresario en la relación laboral*, Consejo Económico y Social, Madrid, 2002

Medina Guerrero, M., *La protección Constitucional de la intimidad frente a los medios de comunicación*, Tirant to Blanch, Valencia, 2005

Mercader Uguina, J. R., *Protección de datos en las Relaciones Laborales,* Francis Lefebvre, Madrid, 2018

Poquet Catala, R., "La protección del derecho a la intimidad del teletrabajador", *Revista jurídica de los Derechos Sociales*, vol.8, núm.1, 2018 pp. 113- 135

Preciado Pérez, I,. "El teletrabajo: luces y sombras de una herramienta de flexibilidad laboral aún por explorar"**,** *Wolters Kluwer,* núm.9159, 2018, pp. 1- 8

Rojas Rosco, R., López Carballo, D. "El impacto del RGPD en el ámbito del control laboral y la era de la innovación"**,** *Wolters Kluwer*, núm 5, 2010, pp. 1- 17

Sempere Navarro, A. V. y San Martín Mazzucconi, C., *Nuevas Tecnologías y Relaciones*

*Laborales*, Aranzadi, Navarra, 2002

Seone, J.A., "*La ampliación del catálogo de derechos fundamentales*", *Persona y derecho,* vol. 54, 2006, pp. 441- 469 (disponible en http://dadun.unav.edu/handle/10171/14628; última consulta el 23/03/2019).

Suero Salamanca, J. A., "Comentarios a la sentencia del tribunal constitucional 292/2000, de 30 de noviembre", 2001 (disponible en http://www.madrid.org/usupadron/legislacion/protdatos/protecciondatos.pdf; última consulta 2/04/2019).

Toscani Gimenez, D. y Calvo Morales, D. "El uso de internet y el correo electrónico en la empresa: límites y garantías" *Nueva Revista Española de Derecho del Trabajo,* núm. 165, 2014, pp. 197-224

### 6.4 Otros recursos

Instituto Nacional de Ciberseguridad (INCIBE), Dispositivos móviles personales para uso profesional (BYOD): una guía de aproximación para el empresario, Madrid, 2017

Real Academia Española (disponible en https://dle.rae.es/?id=bmtXm9x; última consulta 23/03/2019).

AEPD, Guía del derecho fundamental a la protección de datos de carácter personal (disponible en www.pimemenorca.org/gest-docs/pub/536 ; última consulta el 1/04 2019).