Roj: **SJSO 281/2019** - ECLI: **ES:JSO:2019:281**

Id Cendoj: **31201440032019100001**
Órgano: **Juzgado de lo Social**
Sede: **Pamplona/Iruña**
Sección: **3**
Fecha: **18/02/2019**
Nº de Recurso: **875/2018**
Nº de Resolución: **52/2019**
Procedimiento: **Social**
Ponente: **CARLOS GONZALEZ GONZALEZ**
Tipo de Resolución: **Sentencia**

JUZGADO DE LO SOCIAL Nº 3

Plaza del Juez Elío/Elío Epailearen Plaza, Planta 1 Solairua

Pamplona/Iruña 31011

Teléfono: 848.42.40.94 - FAX 848.42.42.88

Email.: jsocpam3@navarra.es

SENT2

Sección: B Procedimiento: **DESPIDOS / CESES EN GENERAL**

Nº Procedimiento: 0000875/2018

NIG: 3120144420180003043

Materia: Despido

Resolución: **Sentencia** 000052/2019

En la ciudad de Pamplona/Iruña, a DIECIOCHO DE FEBRERO DE DOS MIL DIECINUEVE.

El Ilmo. Sr. D. CARLOS GONZALEZ GONZALEZ, Magistrado-Juez del Juzgado de lo Social Nº 3 de los de Navarra

EN NOMBRE DEL REY

Ha dictado la siguiente

SENTENCIA

Vistos los presentes autos número 0000875/2018 sobre Despido iniciado en virtud de demanda interpuesta por Víctor contra NUCAP EUROPE SL,

ANTECEDENTES DE HECHO

PRIMERO.- El día 31 de octubre de 2018 la parte actora interpuso demanda ante el Juzgado Decano de Pamplona, turnada a éste el día 2 de noviembre de 2018 en los términos que figura en la misma, la cual fue admitida a trámite, señalándose el acto del juicio oral para el día 6 de febrero de 2019 al que previa citación en legal forma comparecieron el demandante D. Víctor asistido por el Letrado D. EUSEBIO GIMENA RAMOS, y el Letrado Sr. BARRERO JIMÉNEZ en representación y defensa de la empresa demandada NUCAP EUROPE SL; quienes hicieron las alegaciones que estimaron pertinentes, proponiéndose la prueba que, una vez admitida por S.Sª., se practicó con arreglo a derecho y desarrollándose la sesión conforme se refleja en el soporte de grabación audiovisual que obra unido a los autos.

SEGUNDO.- En la tramitación de estos autos se han observado las prescripciones legales de procedimiento.

HECHOS PROBADOS

PRIMERO.- El demandante D. Víctor viene prestando su servicios profesionales por cuenta de la empresa demandada Nucap Europe SL desde el 29 de enero de 2018, en virtud de relación laboral indefinida, y con la categoría de ajustador/matricero, conforme a un salario regulador diario de 79,63 euros (hecho conforme).

SEGUNDO.- El actor no es ni ha sido representante legal o sindical de trabajadores.

TERCERO.- Con fecha 21 de septiembre de 2018 la empresa demandada **entrega al actor carta de despido disciplinario** , con efectos del mismo día, en la que se le imputa las infracciones previstas en el art.54.2 c) del Estatuto de los Trabajadores y del art. 58 letra h) del Convenio Colectivo para la Industria Siderometalúrgica de la Comunidad Foral de Navarra , y todo ello con referencia a hechos ocurridos a las 13,55 horas del sábado 15 de septiembre de 2018, en el que el actor participó en una **pelea, con puñetazos y golpes, con otro trabajador de la empresa** , llamado Zaide Attary (carta de despido disciplinario que obra unida a los autos y que se da aquí por reproducida).

CUARTO.- Han quedado acreditados los hechos de la carta de despido y, en concreto, que el sábado 15 de septiembre de 2018 el demandante tuvo una discusión en el centro de trabajo con otro trabajador, identificado como Zaide Attary. Dicha discusión estaba motivada por una orden concreta de trabajo. En este contexto, durante la discusión producida en el centro de trabajo, y dentro de la jornada de trabajo, el demandante siguió al otro trabajador por el centro y en tono amenazante le dijo que a la salida se verían.

En efecto, concluida la jornada, estando en el parking de la empresa, tanto el actor como Zaide Attary **se enzarzaron en una pelea, en el transcurso de la cual el actor, que llevaba una fusta, golpeó al otro contrincante, y a su vez Zaide Attary le golpea con un casco demoto que llevaba en la mano, propinándose ambos puñetazos,** y continuando la pelea hasta que fueron separados por otro trabajador presente en el lugar.

QUINTO.- Al actor le entregó la carta de despido disciplinario el responsable o jefe de personal de la empresa demandada, que instruyó expediente contradictorio, y a quien el otro trabajador implicado y el testigo presencial, D. Luis Miguel , le reconocieron la existencia de la pelea producida.

SEXTO.- Se celebró el preceptivo acto de conciliación el 26 de octubre de 2018, instado el 17 de octubre de 2018, concluyendo sin avenencia.

SÉPTIMO.- Por burofax remitido al demandante se le aclaró la carta de despido en el sentido de que la fecha que se hace constar en un párrafo es el 15 de septiembre en lugar del 17 de septiembre, en ambos casos referido al año 2018.

OCTAVO.- La mercantil Consulting & Estrategy GFM SL remitió comunicación a la Agencia Española de Protección de Datos sobre designación del delegado de protección de datos por cuenta de la empresa Nucap Europe SL.

Los formularios remitidos a la Agencia Española de Protección Datos indican, marcándose la casilla referida al *"conocimiento de los deberes del solicitante"* , que *"los datos de carácter personal que pudieran constar en esta comunicación serán incorporados al sistema de tratamiento "Registro de Delegados de Protección de Datos" , del que es responsable la Agencia Española de Protección de Datos (AEPD) para el ejercicio de potestades públicas. Los datos serán tratados para gestionar la comunicación del delegado de protección de datos y como punto de contacto del responsable o encargado del tratamiento. Los datos de contacto relativos al delegado de protección de datos se publicarán en la Web de la AEPD y, en su caso, serán comunicados a las autoridades de* control pertenecientes a la UE en el marco del desarrollo de las acciones conjuntas que se establecen en el Capítulo VII del RGPD. Los datos serán suprimidos cuando el cese como DPD de la entidad que representa haya sido comunicado y hayan dejado de ser necesarios. Tiene derecho a acceder, rectificar y suprimir los datos, así como los demás derechos que le otorga la normativa de protección de datos ante la Agencia Española de Protección de Datos, C/Jorge Juan, 6, 28001 -Madrid- o en la dirección de correo electrónico dpd@agpd.es".

Asimismo la empresa Consulting & Estrategy GFM SL **emite un certificado de adecuación al Reglamento General de Protección de Datos** , haciendo constar que presta sus servicios de adecuación y mantenimiento al Reglamento UE 2016/679, del Parlamento Europeo y del Consejo, del 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y que entre los servicios de adecuación y mantenimiento al reglamento que proporciona la empresa se encuentran las funciones definidas en el art. 39 del Reglamento de Protección de Datos Personales como delegado de protección de datos de la empresa Nucap Europe SL.

En dicho certificado se hace constar en relación a Nucap Europe SL, lo siguiente :

· Se ha generado una evaluación de riesgos completa.

· Se ha generado el Registro de Actividades de Tratamiento.

· Se ha generado el protocolo de medidas de seguridad con descripción de las medidas técnicas, físicas, lógicas y organizativas que debe implementar la empresa para mitigar riesgos.

· Se han previsto procedimientos de tutela de derechos de los interesados y un registro de incidencias técnicas, así como un procedimiento para notificar las brechas y violaciones de seguridad.

· Se han identificado los encargados del tratamiento de datos personales y se han generado modelos de contrato ad hoc que definen y regulan esa relación.

· La empresa dispone de avisos legales, políticas de privacidad y formularios de recogida de datos de clientes para garantizar el cumplimiento del deber de informar.

· Toda la documentación citada se almacena en un entorno *icloud* seguro donde se mantiene actualizada periódicamente con su correspondiente historial de versiones que permita acreditar, a su vez, un historial de cumplimiento normativo.

Concluye indicando que la adecuación y revisión es de fecha 25 de mayo de 2018.

Obra unido a los autos y se da aquí por reproducido el anexo de la empresa demandada referida al **registro de actividades de tratamiento** , en el que constan los datos de contacto del responsable y del delegado de protección de datos. Dentro de este registro de datos de tratamiento **figura el referido a videovigilancia, con indicación de que los *fines* son "videovigilancia de las instalaciones/o bienes".**

En el epígrafe correspondiente a **categorías de interesados** se hace referencia a "personas que acceden a las instalaciones videovigiladas", y cita dentro de las categorías a ***empleados*** ; clientes y usuarios; y proveedores. Respecto a la **categoría de datos personales** se indica "la ***identificación de imagen/voz"*** . En categorías de destinatarios se menciona a las fuerzas y cuerpos de seguridad y a tribunales y juzgados.

Expresamente se indica que no hay transferencias de datos a terceros países u organizaciones internacionales. En orden a los plazos previstos para supresión de los datos personales se hace mención a que **"los datos se suprimirán a los treinta días, salvo comunicación a fuerzas y cuerpos de seguridad y/o juzgados y tribunales".**

La empresa demandada, en efecto, **tiene instaladas cámaras de vigilancia en su centro de trabajo, que cuentan con el correspondiente cartel identificativo de zona videovigilada y con referencia a la Ley Orgánica 15/1999 de Protección de Datos, indicando que cabe ejercitar los derechos ante Nucap Europe SA** (fotografías unidas a los folios 53, 54 y 55 de los autos que se dan aquí por reproducidas).

FUNDAMENTOS DE DERECHO

PRIMERO.- Pretensiones de la demanda y posición de las partes.

1. Demanda.

En la demanda iniciadora del presente juicio se ejercita una acción declarativa de condena, propia del proceso de despido, considerando la parte demandante que constituye un **despido improcedente** el que ha comunicado la empresa demandada con efectos del 21 de septiembre de 2018, afirmando que no son ciertos los hechos y que en todo caso no tienen entidad como para dar lugar a la sanción máxima del despido disciplinario. También alega el trabajador que tiene serias dudas de quién ha firmado la carta de despido y, en concreto, si es un representante de la empresa con poder para comunicar el despido disciplinario.

En el acto del juicio, además de **impugnar las grabaciones con sistema de videovigilancia** que quería aportar al acto del juicio la empresa, indicó que en todo caso los hechos que se imputan al demandante habrían ocurrido fuera del centro de trabajo y de la jornada, con la consecuencia de que no son sancionables por la empresa.

2. Contestación de la empleadora.

La empresa demandada compareció al acto del juicio y se opuso a la acción ejercitada, señalando que puede acreditar los hechos que imputa al demandante y que los mismos están correctamente calificados, constituyendo un incumplimiento laboral muy grave que justifica la imposición de la sanción máxima del despido disciplinario.

3. Valoración probatoria. Inadmisión de prueba videográfica.

Los hechos declarados probados resultan acreditados con el **examen y valoración conjunta de la prueba practicada** , consistente en los **documentos** aportados por las partes litigantes **y la prueba testifical** practicada en el acto del juicio.

Debe destacarse que **existe conformidad entre las partes litigantes en los hechos referidos al tiempo de prestación de servicios, categoría profesional y salario regulador** .

Los **hechos de la carta despido han quedado plenamente acreditados con las declaraciones testificales del responsable o jefe de personal de la empresa demandada y de un trabajador, que fue testigo presencial de los hechos.** El primer testigo, el Sr. Antonio , como jefe de personal de la empresa demandada, ratificó todos los documentos que ha aportado la empresa demandada y lo actuado en el expediente previo a la comunicación de la carta de despido disciplinario. Destacó con total claridad y rotundidad, sin incurrir en dudas ni contradicciones, que efectivamente los testigos presenciales de los hechos ratificaron cómo ocurrió la pelea entre el actor y otro trabajador, ratificando los datos del lugar y motivo de la discusión. También ratificó que fue él el que entregó al demandante la carta de despido en su condición de responsable de responsable de Recursos Humanos.

Además, también declaró **el testigo presencial de los hechos** , Sr. Luis Miguel quien, de la misma manera, con esa rotundidad y contundencia del testimonio antes destacada, declaró que efectivamente los hechos ocurrieron tal y como constan en la carta de despido disciplinario. Afirma que los dos trabajadores se enzarzaron en la pelea, y que ambos -el actor y el otro trabajador-, se propinaron puñetazos, golpeando el actor al otro contendiente con una fusta y éste al actor con un casco de moto. El relato pone de manifiesto la riña o pelea mutua, en la que los dos trabajadores despedidos se propinaron puñetazos y golpes hasta que el propio testigo logró separarlos. También ratificó que los hechos ocurrieron en el parking de la empresa y que todo vino motivado por una previa discusión referida a una orden de trabajo durante la jornada laboral, en cuyo transcurso, también dentro de las instalaciones de la empresa o centro de trabajo, fue el propio demandante el que avisó al contendiente que se verían fuera al concluir la jornada, como así ocurrió.

Debe destacarse que en el acto del juicio la empresa demandada propuso la prueba de visualización de las grabaciones captadas por las cámaras de videovigilancia instaladas en la empresa y que captaron la pelea. Esta prueba de las grabaciones de videovigilancia fueron expresamente impugnadas por el demandante por no respetar los derechos fundamentales que le afectan y, tras el traslado para alegaciones al proponente, se inadmitió a trámite al valorar este magistrado que vulneraba derechos fundamentales del demandante y por eso era una prueba nula. A continuación procede ampliar los razonamientos expresados en el acto del juicio para inadmitir la prueba que, a la postre, se ha revelado en todo caso innecesaria para acreditar los hechos que la empresa imputaba al demandante para justificar el despido disciplinario.

SEGUNDO.- Nulidad de la prueba de video vigilancia en el centro de trabajo por vulnerar el derecho a la intimidad y a la protección de datos personales del trabajador.

1. Normativa sobre la prueba nula por vulneración de los derechos fundamentales.

En relación con el **art. 24.2 de la Constitución Española** , el art. **90.1 de la Ley Reguladora de la Jurisdicción Social** , regula la **admisibilidad de los medios de prueba** , disponiendo que las partes, previa justificación de la utilidad y pertinencia de las diligencias propuestas, podrán servirse de cuantos medios de prueba se encuentren regulados en la ley para acreditar los hechos controvertidos o necesitados de prueba, incluidos los **procedimientos de reproducción de la palabra, de la imagen y del sonido** o de archivo y reproducción de datos, que deberán ser aportados por medio de soporte adecuado y poniendo a disposición del órgano judicial los medios necesarios para su reproducción y posterior constancia de autos.

El **art. 90.2** de la misma norma procesal añade que **no se admitirán pruebas que tuvieran su origen o que se hubieran obtenido, directa oindirectamente, mediante procedimientos que supongan violación de derechos fundamentales o libertades públicas** . Esta cuestión podrá ser suscitada por cualquiera de las partes o de oficio por el tribunal en el momento de la proposición de la prueba, salvo que se pusiese de manifiesto durante la práctica de la prueba una vez admitida. A tal efecto, se oirá a las partes y, en su caso, se practicarán las diligencias que se puedan practicar en el acto sobre este concreto extremo, recurriendo a diligencias finales solamente cuando sea estrictamente imprescindible y la cuestión aparezca suficientemente fundada. Añade el precepto que **contra la resolución que se dicte sobre la pertinencia de la práctica de la prueba** y en su caso de la unión a los autos de su resultado o del elemento material que incorpore la misma, **sólo cabrá recurso de reposición** , que se interpondrá, se dará traslado a las demás partes y se resolverá oralmente en el mismo acto del juicio o comparecencia **, quedando a salvo el derecho de las partes a reproducir la impugnación de la prueba ilícita en el recurso que, en su caso, procediera contra la sentencia.**

A su vez, completa esta regulación el art.90.4 de la Ley Reguladora de la Jurisdicción Social al establecer que cuando sea necesario a los fines del proceso el acceso a documentos o archivos, en cualquier tipo de soporte, que puedan afectar a la intimidad personal u otro derecho fundamental, el juez o tribunal, siempre que no existan medios de prueba alternativos, podrá autorizar dicha actuación, mediante auto, previa ponderación de los intereses afectados a través del juicio de proporcionalidad y con el mínimo sacrificio, determinando las

condiciones de acceso, las garantías de conservación y aportación al proceso, obtención y entrega de copias e intervención de las partes o de sus representantes y expertos, en su caso.

La normativa citada no es sino desarrollo y determinación en el ámbito del proceso social de lo que establece el **art.11.1 de la LOPJ** . al disponer, tras indicar que en todo tipo de procedimiento se respetarán las reglas de la buena fe, que ***"no surtirán efecto las pruebas obtenidas, directa o indirectamente, violentando los derechos o libertadas fundamentales"*** . Como cabe observar en el ámbito del proceso laboral ya no es que se indique que no producen efecto las pruebas que hayan vulnerado derechos fundamentales, **sino que incluso no deben admitirse esas pruebas,** sin duda pensando el legislador que **debe evitarse la contaminación del juez o magistrado** que deba resolver el asunto si ha estado en contacto con un material probatorio que, en definitiva, vulnera los derechos fundamentales de los implicados en el proceso. Similar regulación se contiene en el art. 287 de la LEC .

En el caso que se enjuicia se ha propuesto por la empresa demandada el visionado de las grabaciones de las cámaras de videovigilancia que tiene establecidas en la empresa, **prueba que impugnó de forma expresa el demandante** al considerar que vulneraba sus derechos fundamentales y que no cumplía las exigencias establecidas para respetar el derecho a la intimidad y el derecho a la protección de los datos personales, haciendo así referencia a los derechos que consagra el art.18.1 y 18.4 de la Constitución Española y a la jurisprudencia sobre el alcance de estos derechos en el ámbito del control empresarial de la actividad de los trabajadores.

2. Requisitos para la validez probatoria de las grabaciones con las cámaras de video vigilancia.

A fin de motivar la inadmisión de la prueba propuesta por la empresa demandada, referida al visionado de las grabaciones e imágenes captadas con las cámaras de videovigilancia que se disponen en el exterior de la empresa, debemos **recordar cuál ha sido la evolución en esta materia y las exigencias para la admisión de este tipo de pruebas** cuando colisiona con los derechos fundamentales a la intimidad y a la protección de datos personales. Además, **habiendo invocado la empresa la nueva regulación de la Ley Orgánica 3/2018** , de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, debe examinarse si la doctrina aplicable a esta materia ha quedado afectada por la nueva regulación legal **y si la ley española respeta las exigencia del reglamento europeo de protección de datos personales** .

Si en el control empresarial de los medios informáticos y tecnológicos la jurisprudencia ha establecido criterios más o menos consolidados sobre los requisitos del acceso y las condiciones que permitirán utilizar los datos obtenidos como prueba válida a los efectos de acreditar los incumplimientos laborales -ahora afectados por la **doctrina "Barbulescu II", Sentencia de la Gran Sala del TEDH de 5 de septiembre de 2017** , que anula la anterior, dictada el 12 de enero de 2016, por el propio Tribunal-, no ocurre lo mismo cuando el control empresarial de la conducta de los trabajadores se realiza a través de sistemas de video vigilancia. La escasa regulación legal en esta materia no ha permitido hasta ahora obtener una respuesta segura sobre los límites de la facultad empresarial. Esta anomia legal ha dado lugar a una **jurisprudencia vacilante** y a la adopción de criterios por parte del Tribunal Constitucional que no siempre han sido bien recibidos por la doctrina científica y por los interlocutores sociales.

La **dificultad para encontrar un criterio pacífico** se explica en parte porque el TC y el TS han construido la mayoría de sus criterios examinando la incidencia de la videovigilancia en los derechos fundamentales a la intimidad y a la propia imagen (art. 18.1 CE). Pero cuando se invoca la vulneración del derecho a la protección de datos en los casos de videovigilancia (art. 18.4 CE) el conflicto jurídico adquiere otra dimensión, precisamente por la **exigencia estructural de este derecho de que se cumpla necesariamente el deber informativo a los trabajadores** como único medio de conseguir una protección eficaz del derecho de autodeterminación informativa inherente al derecho a la protección de datos.

Podemos analizar la evolución de la jurisprudencia en esta materia, **fijando los hitos más característicos** , y la incidencia **del Reglamento 2016/679** del Parlamento Europeo y del Consejo, del 27 de abril de 2016 y de **la regulación de la videovigilancia en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales,** que invocó la empresa demandada como argumento a favor de la admisión de la prueba de video vigilancia.

Para mayor claridad en la exposición de esta difícil cuestión planteada, **podemos distinguir como principales aspectos a desarrollar los siguientes** : a) La doctrina constitucional hasta las SSTC 29/2013 y 39/2016 ; b) Vigilancia y protección de datos: el deber informativo en la doctrina de las SSTC 29/2013 y 39/2016 ; c) La prohibición de la videovigilancia encubierta en la doctrina de la STEDH de 9-01-2018 (caso "López Ribalda y otras v. España"); d) El deber informativo como requisito imprescindible para la validez de las grabaciones audiovisuales y de los otros medios tecnológicos de control empresarial y la incidencia del Reglamento

2016/679, del Parlamento Europeo y del Consejo, del 27 de abril de 2016 y e) El deber informativo en la LO 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales.

A) La doctrina constitucional hasta las SSTC 29/2013 y 39/2016 .

Las **STC 98/2000** , de 10 de abril y la **186/2000** , de 10 de julio , son las que establecen los principales criterios aplicativos en esta materia, y respecto de sus conclusiones vino a introducir correcciones importantes la **STC 29/2013** , de 11 de febrero . No obstante, debe tenerse en cuenta que en las dos primeras sentencias el conflicto se plantea exclusivamente desde la perspectiva del derecho a la intimidad (Art. 18.1CE), quedando al margen del debate el derecho a la autodeterminación informativa que se integra en el derecho a la protección de los datos personales, que es, cabalmente, el que tuvo en cuenta la STC 29/2013 .

La **STC 98/2000** resuelve el supuesto de la **utilización en un casino de micrófonos** en determinadas dependencias del centro de trabajo (secciones de caja y ruleta francesa) **donde eran grabadas las conversaciones de los trabajadores** . La sentencia estima el recurso de amparo y **reconoce la vulneración del derecho a la intimidad personal** del trabajador recurrente, sin admitir que la actuación de la empresa tuviera en el caso concreto amparo en las facultades de vigilancia y control reconocidas al empresario por la normativa laboral (Art. 20.3 ET). Aunque el caso se refiere a la grabación de sonido y no de imágenes, sin embargo, **la doctrina que establece tiene alcance general en la fijación de criterios en la resolución del conflicto por la colisión que pueda producirse entre los medios de control empresariales y los derechos fundamentales de los trabajadores** . De hecho la STC 186/2000 -que sí resuelve el caso de un despido disciplinario en el que se utiliza como prueba de cargo las grabaciones de video vigilancia- se funda precisamente en esos criterios aplicativos y en la doctrina establecida en la sentencia 98/2000 .

Veamos de forma resumida los **criterios a tener en cuenta** para resolver el conflicto entre el derecho a la intimidad y los medios de control empresarial de la actividad laboral conforme a lo declarado por la **STC 98/2000** :

i. Las facultades empresariales de control empresarial que incidan en los derechos fundamentales de los trabajadores sólo pueden derivar, bien del hecho de que la propia naturaleza del trabajo contratado implique la restricción del derecho, bien de una acreditada necesidad o interés empresarial, sin que sea suficiente su mera invocación para sacrificar el derecho fundamental del trabajador.

ii. El ejercicio de las facultades organizativas y disciplinarias del empleador no puede servir, en ningún caso, a la producción de resultados inconstitucionales, lesivos de los derechos fundamentales del trabajador, ni a la sanción del ejercicio legítimo de tales derechos por parte de este.

iii. Necesidad de preservar el equilibrio entre las obligaciones dimanantes del contrato para el trabajador y el ámbito - **modulado por el contrato, pero en todo caso subsistente-** de su libertad constitucional. Dada la posición preeminente de los derechos fundamentales en nuestro ordenamiento, **la modulación sólo se producirá en la medida estrictamente imprescindible para el correcto y ordenado desenvolvimiento de la actividad productiva en la empresa** .

iv. **Las limitaciones o modulaciones** de los derechos fundamentales del trabajador **tienen que ser las indispensables y estrictamente necesarias** para satisfacer un interés empresarial merecedor de tutela y protección, de manera que si existen otras posibilidades de satisfacer dicho interés menos agresivas y afectantes del derecho en cuestión, habrá que emplear estas últimas y no aquellas otras más agresivas, en razonable aplicación del **principio de proporcionalidad** .

En el caso que accede al amparo constitucional **se estima el amparo y se anulan las Sentencias** dictadas en el orden social, valorando que la instalación de los micrófonos que permiten grabar las conversaciones de los trabajadores y de los clientes en determinadas zonas del casino **no se ajusta a las exigencias** indispensables del respeto del **derecho a la intimidad** ni a los **principios de proporcionalidad e intervención mínima** que rigen la modulación de los derechos fundamentales por los requerimientos propios del interés de la organización empresarial. Razona que aunque la instalación de aparatos de captación y grabación del sonido en dos zonas concretas del casino -la caja y la ruleta francesa- fuesen de utilidad para la organización empresarial, **la mera utilidad o conveniencia para la empresa no legitima sin más su instalación** , habida cuenta de que la empresa ya disponía de otros sistemas de seguridad que el sistema de audición pretende complementar. **No considera acreditado que la instalación del sistema de captación y grabación de sonidos sea indispensable para la seguridad y buen funcionamiento del casino** . Concluye el TC que el uso de un sistema que permite la audición **continuada e indiscriminada de todo tipo de conversaciones** , incluidos comentarios privados -ajenos por completo al interés empresarial y por tanto irrelevantes desde la perspectiva de control de las obligaciones laborales-, tanto de los propios trabajadores, como de los clientes del casino, constituye una **actuación que**

rebasa ampliamente las facultades que al empresario otorga el artículo 20.3 LET y supone una intromisión ilegítima en el derecho a la intimidad (Art. 18.1 CE).

La segunda resolución a tener en cuenta - **STC 186/2000** - sí que se enfrenta a un despido disciplinario en el que se imputa al trabajador la sustracción de dinero de la caja de un economato, **habiendo utilizado la empresa para acreditar la conducta las grabaciones del sistema de video vigilancia que instaló para comprobar sus sospechas** . En concreto, el trabajador afectado prestaba servicios como cajero del economato de la empresa (ENSIDESA), y como consecuencia de un **descuadre llamativo en los rendimientos** del economato, la empresa contrató con una empresa de seguridad la **instalación de un circuito cerrado de televisión** que enfocase únicamente a las tres cajas registradoras y al mostrador de paso de las mercancías desde el techo, en el radio de acción aproximado que alcanzaba el cajero con sus manos. El resultado de la vigilancia realizada en diferentes fechas de abril y mayo de 1995 determinó el despido disciplinario del recurrente en amparo. Las cintas de vídeo grabadas revelaron que **el trabajador** realizó de forma reiterada maniobras en el cobro de artículos a los clientes del economato, **sustrayendo diferentes cantidades de la caja** .

Los Tribunales declararon **procedente el despido** y no se apreció vulneración del derecho a la intimidad del trabajador por la instalación de las cámaras de vigilancia. El TC **desestima el recurso de amparo** , considerando que en el caso se respetó el derecho fundamental del trabajador a la intimidad ***-no fue objeto del amparo el derecho a laprotección de datos-*** y que las pruebas videográficas eran válidas. **Tal vez su afirmación más importante se concreta en la exclusión de la necesidad de informar a los trabajadores de la instalación de las cámaras, pero debe insistirse que sólo se realiza dicha afirmación respecto del derecho fundamental a la intimidad, sin referirse al derecho que consagra el artículo 18.4 de la CE .**

Reitera el tribunal de garantías la doctrina de la STC 98/2000 y fija como **principios esenciales** a tener en cuenta los siguientes:

i. **El derecho a la intimidad es aplicable al ámbito de las relaciones laborales. Pero no es un derecho absoluto** , pudiendo ceder ante intereses constitucionalmente relevantes, siempre que el recorte que aquél haya de experimentar se revele como **necesario** para lograr el fin legítimo previsto, **proporcionado** para alcanzarlo y, en todo caso, **sea respetuoso con el *contenido esencial* del derecho** (reiterando la doctrina de las SSTC 57/1994, FJ 6 , y 143/1994 , FJ 6).

ii. **El poder de dirección del empresario** , imprescindible para la buena marcha de la organización productiva (organización que refleja otros derechos reconocidos constitucionalmente en los **arts. 33 y 38 CE**) y reconocido expresamente en el Art. 20 ET , atribuye al empresario, entre otras facultades, la de **adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento del trabajador de sus obligaciones laborales** , respetando la dignidad del trabajador (arts. 4.2 c) y 20.3 ET).

iii. **El empresario no queda apoderado para llevar a cabo** , so pretexto de las facultades de vigilancia y control que le confiere el Art. 20.3 ET , **intromisiones ilegítimas** en la intimidad de sus empleados en los centros de trabajo.

iv. La constitucionalidad de cualquier medida restrictiva de derechos fundamentales viene determinada por la **estricta observancia del principio de proporcionalidad.**

v. Para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los **tres requisitos** siguientes: si tal medida es susceptible de conseguir el objetivo propuesto (**juicio de idoneidad**); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (**juicio de necesidad**); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (**juicio de proporcionalidad en sentido estricto**). Reitera así una doctrina clásica que ya desarrolló en las SSTC 66/1995, de 8 de mayo, FJ 5 ; 55/1996, de 28 de marzo, FFJJ 6, 7, 8 y 9; 207/1996, de 16 de diciembre, FJ 4 e), y 37/1998, de 17 de febrero , FJ 8.

vi. La validez de la prueba derivada de la grabación con las cámaras **no exige informar previamente a los trabajadores ni al Comité de empresa de la instalación de las cámaras de seguridad o de vigilancia , al menos** como exigencia derivada del **contenido esencial** de los derechos a la intimidad y a la propia imagen.

vii. En definitiva, el **control jurisdiccional** de la medida de control empresarial **exige ponderar** adecuadamente si la instalación y empleo de medios de captación y grabación de imágenes por la empresa **ha respetado** en cada caso el **derecho a la intimidad** personal del trabajador, de conformidad con las exigencias del **principio de proporcionalidad** .

De ser correcta esta afirmación de la STC 186/2000 sobre la **exclusión del deber informativo previo como parte del contenido esencial del *derecho a la intimidad* en supuestos de utilización de cámaras de seguridad**

o de vigilancia , habría una clara diferencia con la doctrina del Tribunal Europeo de Derechos Humanos y del TS sobre el control empresarial de otros medios tecnológicos o informáticos que utilicen los trabajadores. En efecto, para el control de estos otros medios ambos Tribunales exigen **eliminar la expectativa de intimidad o secreto que pudiera tener el trabajador, imponiendo a la empresa un deber informativo a los trabajadores sobre la existencia del control empresarial y los medios utilizados** (Sentencia TEDH de 3 de abril de 2007 en el asunto Copland versus Reino Unido -TEDH 2007, 23-: afirma que la expectativa de intimidad y confidencialidad de los trabajadores **sólo desaparece si la empresa *advierte* de la fiscalización** .-; **en el mismo sentido las SSTS 26/09/2007** -RJ 2007, 7514 -, **y 08/03/2011** -RJ 2011,932-). No obstante la jurisprudencia previa del TS, que acoge sin excepción la doctrina del TEDH, en la posterior **STS de 06-10-2011** -RJ 2011,7699 **-, se introduce una excepción al deber informativo previo cuando no existe tolerancia empresarial** en el uso por los trabajadores de los medios tecnológicos o informáticos para usos particulares y se ha establecido una regla de prohibición absoluta. *Razona que es cierto que la STS de 26-09-2007 exigíainformar a los trabajadores de la existencia de control empresarial ylos medios utilizados, pero esta concreta exigencia la califica de* mero "obiter dicta", que **no es aplicable en supuestos de prohibición absoluta** del uso de los medios tecnológicos en los que no concurre expectativa alguna de confidencialidad o intimidad por parte de los trabajadores que haya podido ser sorprendida con la actuación fiscalizadora de la empresa. En el mismo sentido cabe citar la **STC 170/2013** , de 7 de octubre -RTC 2013,170- para un supuesto en el que el convenio colectivo tipifica como infracción los usos extra laborales de las herramientas informáticas, considerando que esta previsión implica una prohibición expresa que conlleva la facultad de la empresa para controlar la utilización de las herramientas informáticas sin necesidad de previa información a los trabajadores.

En todo caso, para la **STC 186/2000** en el supuesto que accede al amparo se cumplieron las condiciones para la validez de la prueba videográfica. Descarta que se haya producido la lesión del derecho a la intimidad personal y a la propia imagen consagrados en el artículo 18.1 CE y afirma que **la instalación del circuito cerrado de televisión** que controlaba la zona de trabajo **era una medida justificada** (ya que existían razonables sospechas de la comisión por parte del recurrente de graves irregularidades en su puesto de trabajo); **idónea** para la finalidad pretendida por la empresa (verificar si el trabajador 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 y a una duración temporal limitada, la suficiente para comprobar que no se trataba de un hecho aislado o de una confusión, sino de una conducta ilícita reiterada).

Además, **destaca** de forma especial que en este caso la medida no obedeció al propósito de vigilar y controlar **genéricamente** el cumplimiento por los trabajadores de las obligaciones que les incumben, a diferencia del caso resuelto en la STC 98/2000 , en el que la empresa, existiendo un sistema de grabación de imágenes pretendía decidió instalar un sistema de grabación de sonido para mayor seguridad, sin quedar acreditado que este nuevo sistema se instalase como consecuencia de la detección de una quiebra en los sistemas de seguridad ya existentes y sin que resultase acreditado que el nuevo sistema, que permitiría la audición continuada e indiscriminada de todo tipo de conversaciones, resultase indispensable para la seguridad y buen funcionamiento del centro de trabajo (un casino). **Por el contrario** , **en el caso que resuelve la STC 186/2000 previamente se habían advertido irregularidades** en el comportamiento de los cajeros y un acusado **descuadre contable** . Y se adoptó la medida de vigilancia de modo que **las cámaras únicamente grabaran el ámbito físico estrictamente imprescindible** , como eran las cajas registradoras.

B) Vigilancia y protección de datos: deber informativo en la doctrina de las SSTC 29/2013 y 39/2016

Como vemos, en los casos citados, el TC resolvió el conflicto entre el derecho a la intimidad personal (Art. 18.1 CE) y las facultades de control empresarial de la actividad laboral con la aplicación estricta del principio de proporcionalidad. Pero **la doctrina va a ser corregida en la STC 29/2013** , de 11 de febrero , que establece condiciones adicionales para la validez de la utilización de las cámaras de vigilancia en los centros de trabajo, **exigiendo con rigor el cumplimiento del deber de información previo a los trabajadores para admitir las grabaciones como prueba** del comportamiento del trabajador. Hay que tener en cuenta, como hemos advertido con anterioridad, que el tribunal constitucional hasta entonces había establecido los principios en esta materia sobre la base de la colisión de las facultades de control de la empresa con el derecho a la intimidad de los trabajadores, sin ninguna referencia al derecho de autodeterminación informativa que consagra el artículo 18.4 CE . En cambio, la **STC 29/2013** sí que atiende específicamente a las exigencias derivadas del respeto al contenido esencial del derecho en materia de protección de los datos de carácter personal.

El caso que accede al amparo en esta ocasión no es un despido disciplinario, sino la **imposición de tres sanciones** de suspensión de empleo y sueldo por infracciones muy graves a un Director de Servicio de la Universidad de Sevilla por incumplir el horario y la jornada de trabajo. Ante la sospechas de la empleadora procedió a reproducir las grabaciones efectuadas por las cámaras de seguridad en donde se veía como el

trabajador firmaba a unas determinadas horas, aunque entraba al establecimiento a otras horas (se declaró probado en la Sentencia del juzgado de lo social que en la mayor parte de los días laborables existía una demora variable en la hora de entrada al trabajo de entre treinta minutos y varias horas). Consta también en el relato de los hechos que el **convenio colectivo aplicable preveía** la posibilidad de **que el *empresario efectuase el control sobre los medios informáticos yaudiovisuales.*** El **Comité de Empresa había sido informado** sobre la adopción de estas medidas y **existían incluso carteles informativos** en donde se avisaba de la existencia de cámaras. Sin embargo, los **trabajadores *no habían sido informados previa y expresamente de lafinalidad*** para la que podían ser recabados esos datos personales derivados de las grabaciones.

La **STC 29/2013** , de 11 de febrero , estima el recurso de amparo al apreciar que se ha **violado el núcleo esencial** del derecho fundamental del artículo 18.4 de la CE por **incumplimiento del deber de informar** a los trabajadores de la existencia de las cámaras de seguridad y la ***finalidad a la que podía destinarse los datos personales.*** **Declara la nulidad de las sanciones** porque habiéndose acordado con base en una lesión del artículo 18.4 CE **no podrían dejar de calificarse como nulas de acuerdo con la calificación nacida de las SSTC 88/1985** , de 19 de julio, FJ 4 ; **o 134/1994** , de 9 de mayo , FJ 5.

Es necesario destacar que en la determinación del contenido esencial del derecho de autodeterminación informativa sigue aquí la doctrina de la Sentencia del Pleno del TC 292/2000, de 30 de noviembre , que resuelve el recurso de inconstitucionalidad respecto de los arts. 21.1 y 24.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal . La **STC 292/2000 diferencia el contenido del derecho a la intimidad personal y del derecho de protección de los datos de carácter personal** . Subraya que la función del derecho fundamental a la intimidad del artículo 18.1 CE es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad. En cambio, el **derecho fundamental a la protección de datos** persigue garantizar a esa 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. Añade que "ese poder de disposición sobre los propios datos personales nada vale si el afectado desconoce qué datos son los que se poseen por terceros, quiénes los poseen, *y con qué fin* ".

La doctrina que establece la STC 29/2013 cabe resumirla en los siguientes apartados :

i. La habilitación legal para recabar los datos personales sin necesidad de consentimiento en el ámbito de las relaciones laborales **no exime del derecho de información del trabajador** , dado que es **complemento indispensable del derecho fundamental del artículo 18.4 CE** la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo. Una cosa es la necesidad o no de autorización del afectado y otra, diferente, el deber de informarle sobre su poseedor y el propósito del tratamiento.

ii. El **derecho de información** solo podría venir limitado por Ley y en el ámbito de las relaciones laborales **no existe habilitación legal expresa que permita su omisión** ni tampoco puede justificarse la misma en el control de la actividad laboral.

iii. **El derecho de información no puede ser suplido o subsanado** por la existencia de anuncios sobre la instalación de las cámaras o porque se hubiera notificado la creación del fichero a la Agencia Española de Protección de Datos.

iv. **Lesiona el artículo 18.4 CE la utilización** para verificar el cumplimiento de las obligaciones laborales **de medios encubiertos** que niegan al trabajador la información exigible.

v. **Alcance del deber informativo** :

· Será necesaria una **información previa y expresa, precisa, clara e inequívoca** a los trabajadores **de la finalidad de control** de la actividad laboral a la que la captación podía ser dirigida. A nadie se le escapa que en la redacción del artículo 89 de la LO 3/2018, de 5 de diciembre , de protección de datos personales y garantía de los derechos digitales, está muy presente esta doctrina al regular la videovigilancia de los trabajadores en los centros de trabajo.

· Información que **debe concretar las características y el alcance del tratamiento de datos** que iba a realizarse. Esto es, en qué casos las grabaciones podían ser examinadas, durante cuánto tiempo ***y con qué propósitos.***

· **Explicitando** muy particularmente **que podían utilizarse para la imposición de sanciones** disciplinarias por incumplimientos del contrato de trabajo.

Dos precisiones adicionales conviene resaltar de la STC 29/2013 . La primera, que destaca que **el deber informativo es exigible también cuando el control empresarial incide en el derecho a la intimidad personal** (Art. 18.1 CE), **y no sólo cuando está en juego el derecho a la protección de datos de carácter personal**

(Art. 18.4 CE). Argumenta que, no obstante la doctrina de la STC 186/2000 , **el artículo 18.1 de la CE impone** como regla de principio y, de forma añadida al resto de sus garantías, **un deber de información** que protege frente a intromisiones ilegítimas en la intimidad. La segunda, para la STC 29/2013 tampoco podría situarse el fundamento de una exención del deber informativo al trabajador en el interés empresarial de controlar la actividad laboral a través de **sistemas sorpresivos o no informados** de tratamiento de datos que aseguren la máxima eficacia en el propósito de vigilancia.

Considera la Sentencia citada que "esa lógica fundada en la utilidad o conveniencia empresarial haría quebrar la efectividad del derecho fundamental, **en *su núcleo esencial*** . En efecto, **se confundiría la legitimidad del fin** (en este caso, la verificación del cumplimiento de las obligaciones laborales a través del tratamiento de datos, art. 20.3 LET en relación con el art. 6.2 LOPD/1999) **con la constitucionalidad del acto** (que exige **ofrecer previamente la información necesaria** , art. 5 LOPD/1999), cuando lo cierto es que cabe proclamar la legitimidad de aquel propósito (incluso sin consentimiento del trabajador, art. 6.2 LOPD/1999) pero, del mismo modo, declarar que **lesiona el artículo18.4 CE la utilización para llevarlo a cabo de medios encubiertos que niegan al trabajador la información exigible** ".

Sin embargo, esta doctrina del TC va a ser modificada en la **STC 39/2016, de 3 de marzo** . En efecto, el TC desestima el recurso de amparo y **modifica la doctrina de la STC 29/2013** , **delimitando el alcance del deber informativo a los trabajadores** , **que considera cumplido cuando la empresa coloca los distintivos informativos en las condiciones que establece la Instrucción 1/2006** , de 8 de noviembre , de la AEPD. Parece evidente que el Pleno del TC **ha cambiado la doctrina de la STC 29/2013** . Sin embargo, en el voto particular de la sentencia se llama la atención sobre el hecho de que no se mencione ese trascendente cambio, a pesar que la recurrente en amparo fundaba gran parte de su recurso precisamente en el deber informativo de la empresa respecto del trabajador que resulta del artículo 18.4 CE , tal y como había sido interpretado por la sentencia 29/2013 citada.

Los **hechos más relevantes a destacar** son los siguientes:

· La trabajadora prestaba sus servicios como dependienta en un centro comercial de la empresa Bershka BSK España, S.A. y es despedida en 21 de junio de 2012 por transgresión de la buena fe contractual.

· La empresa a raíz de instalar un nuevo sistema de control informático de caja, detectó que en la caja de la tienda donde prestaba sus servicios la demandante existían múltiples irregularidades, de lo que podría desprenderse una apropiación dineraria por parte de alguno de los trabajadores que trabajaban en dicha caja, entre ellos la demandante.

· Por ello encargó a una empresa de seguridad la instalación de una cámara de videovigilancia que controlara la caja registradora.

· **La cámara se instaló sin que se comunicase a los trabajadores** , si bien en el escaparate del establecimiento, en un lugar visible, se colocó el distintivo informativo correspondiente.

· En la carta de despido se imputaba a la trabajadora la apropiación de efectivo de la caja de la tienda, en diferentes fechas y de forma habitual.

· En concreto, se señalaba los días y horas en los que se había apropiado del importe de 186,92 euros, habiendo realizado para ocultar dicha apropiación las operaciones falsas de devoluciones de venta de prendas.

La trabajadora presentó demanda de despido contra la empleadora, solicitando la nulidad del despido por atentar contra su honor, intimidad y dignidad, y subsidiariamente la declaración de improcedencia. ***Nótese que no se menciona el artículo 18.4 CE*** **.** Pero sí alegaba que en el centro de trabajo no existían carteles comunicativos de la existencia de cámaras de videograbación, ni tampoco comunicación a la Agencia de Protección de Datos, ni autorización por la Sección de Seguridad Privada de la Comisaría de Policía, ni tampoco informe previo del comité de empresa sobre la instalación de la videograbación.

En primera instancia la Sentencia del Juzgado de lo Social núm. 2 de León de 11 de marzo de 2013 desestima la demanda y declara procedente el despido. Consideró probados los hechos con las declaraciones del responsable de recursos humanos y de la dirección de la empresa, quienes manifestaron que la propia trabajadora reconoció los hechos cuando se le leyó la carta y pidió perdón, justificando su conducta por una mala racha económica que duraba mucho tiempo. Por lo que se refiere a la instalación de la cámara de videovigilancia razona la Sentencia que *"en la instalación y grabación se cumplió escrupulosamente la normativa al respecto. En efecto, con arreglo a la STC 186/2000, de 10 de julio , concurría la situación precisa para el control oculto, esto es sin notificar expresamente la colocación de la cámara a los trabajadores, porque era, en principio, el único medio posible dicho control para satisfacer el interés empresarial de saber fehacientemente quien estaba realizando los actos defraudatorios de los que indiciariamente ya se tenían conocimiento".* Interpuesto recurso de suplicación se desestima por Sentencia dictada por el TSJ de Castilla y León de 24 de julio de 2013.

La trabajadora accede al amparo constitucional, invocando como vulnerados los artículos 14 , 15 , 18.1 , 18.4 y 24 CE . Destaca que en el ámbito del contrato de trabajo cuando se impone una sanción basada en imágenes captadas por las cámaras de videovigilancia instaladas en el puesto de trabajo, deben respetarse la protección de datos de carácter personal y el derecho a la información que ampara al trabajador. La instalación de cámaras y la captación de imágenes exigen para su validez la necesidad de información previa, expresa, precisa, clara e inequívoca a los trabajadores sobre la captación de imágenes, su finalidad de control de la actividad laboral y su posible utilización para la imposición de sanciones disciplinarias por incumplimientos del contrato de trabajo. De no hacerse así, a su juicio, se vulnera el artículo 18.4 CE .

Por su parte el Fiscal informó que no apreciaba la vulneración del artículo 18.4 CE y que el caso era radicalmente distinto al que se contempla en la STC 29/2013 , identificándose por el contrario con el resuelto en la STC 186/2000 . A diferencia de lo que sucede en la STC 29/2013 donde se trataba de la instalación de un mecanismo de grabación que forma parte de un sistema de seguridad o control que se presenta con un propósito de cierta fijeza o permanencia en el tiempo, en el presente recurso lo que se examina es la instalación puntual de un mecanismo de captación de imágenes, que con carácter transitorio, se emplea para confirmar o descartar previas sospechas debidamente fundadas en relación con el comportamiento de un o unos trabajadores. Por eso entiende que no puede subsumirse el supuesto de hecho en el ámbito que protege el artículo 18.4 CE en cuanto que no se trata de la instalación de sistemas aptos para la recopilación sistemática y general de datos de carácter personal, y por eso no puede pretenderse que se diera conocimiento al trabajador vigilado y que se comunicara un pretendido fichero inexistente a la Agencia Estatal de Protección de Datos.

Planteados en estos términos el debate en amparo, la **STC de 3 de marzo de 2016 establece la siguiente doctrina** sobre la colisión entre las facultades de control empresarial a través de la videovigilancia y los derechos a la intimidad y a la protección de los datos de carácter personal:

i. El derecho fundamental a la protección de datos personales comprende el derecho del afectado a consentir la recogida y uso de sus datos personales y a saber de los mismos.

ii. Para hacer efectivo ese contenido **resulta esencial el reconocimiento del derecho del afectado a ser informado** de quién posee sus datos personales ***y con qué fin,*** y el derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos (sigue aquí la doctrina de la STC 292/2000).

iii. Aunque el **consentimiento del afectado** es el elemento definidor del sistema de protección de datos de carácter personal, **la propia LOPD/1999 excepciona** los supuestos en que concurra habilitación legal para que los datos puedan ser tratados sin dicho consentimiento, como ocurre precisamente en el ámbito de las relaciones laborales (conforme a lo dispuesto en el artículo 6.2 de la LOPD/1999).

iv. **La dispensa del consentimiento abarca a los datos necesarios para el mantenimiento y cumplimiento de la relación laboral, incluyendo a las obligaciones derivadas del contrato de trabajo (** artículo 6.2 de la LOPD/1999 **)** . Por ello, un tratamiento de datos dirigido al control de la relación laboral debe entenderse amparado por la excepción, pues está dirigido al cumplimiento de la misma. Por el contrario, el consentimiento de los trabajadores afectados sí será necesario cuando el tratamiento de datos se utilice con finalidad ajena al cumplimiento del contrato.

v. **Aunque no sea necesario el consentimiento en los casos señalados, el deber de información sigue existiendo** , pues este deber permite al afectado ejercer los derechos de acceso, rectificación, cancelación y oposición y conocer la dirección del responsable del tratamiento o, en su caso, del representante (Art. 5 LOPD).

vi. Para valorar si se ha vulnerado el derecho a la protección de datos por incumplimiento del deber de información, la dispensa del consentimiento al tratamiento de datos en determinados supuestos debe ser un elemento a tener en cuenta dada la estrecha vinculación entre el deber de información y el principio general de consentimiento.

vii. **En todo caso** , **el incumplimiento** del deber de requerir el consentimiento del afectado para el tratamiento de datos o **del deber de información previa sólo supondrá una vulneración del derecho fundamental a la protección de datos tras una ponderación de la proporcionalidad de la medida adoptada.**

viii. **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 artículo 20.3 ET .

ix. La relevancia constitucional de la ausencia o deficiencia de información en los supuestos de videovigilancia laboral exige la consiguiente **ponderación en cada caso de los derechos y bienes constitucionales en conflicto**

; a saber, por un lado, el derecho a la protección de datos del trabajador y, por otro, el poder de dirección empresarial imprescindible para la buena marcha de la organización productiva, que es reflejo de los derechos constitucionales reconocidos en los artículos 33 y 38 CE .

x. **El deber informativo previo al trabajador se entiende cumplido con la colocación de los distintivos informativos previstos en la Instrucción 1/2006** , de 8 de noviembre, de la AEPD, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras.

xi. **Cuando se cumple con la exigencia de la información previa** de la instalación de las cámaras de videovigilancia a través del correspondiente distintivo informativo no puede entenderse vulnerado el artículo 18.4 CE , y **el control que debe realizarse** consistirá en **determinar** si la instalación y empleo de medios de captación y grabación de imágenes por la empresa **ha respetado el derecho a la intimidad personal** , de conformidad con las exigencias del **principio de proporcionalidad** (cita expresamente las SSTC 186/2000 y 98/2000).

A la vista de esta doctrina resuelve el recurso el TC. Entiende que se cumplió el deber informativo que pesaba sobre la empresa porque que la cámara estaba situada en el lugar donde se desarrollaba la prestación laboral, enfocando directamente a la caja, y en el escaparate del establecimiento, en un lugar visible, se colocó el distintivo informativo exigido por la Instrucción 1/2006. Con esa información la trabajadora podía conocer la existencia de las cámaras y la finalidad para la que habían sido instaladas. **En estas condiciones concluye que la trabajadora conocía que en la empresa se había instalado un sistema de control por videovigilancia, *sin que haya que especificar, más alláde la mera vigilancia, la finalidad exacta* que se le ha asignado a ese control.**

Respecto del **juicio de proporcionalidad** también considera la Sentencia que concurren las condiciones que permitían a la empresa la instalación de cámaras de vigilancia. Así, se concluye que la medida de instalación de cámaras de seguridad que controlaban la zona de caja donde la demandante de amparo desempeñaba su actividad laboral era una medida **justificada** (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 artículo 18.1 CE .

La STC 39/2013, de 3 de marzo , cuenta con el voto particular de un magistrado que llama la atención sobre lo que considera la **mutación constitucional** derivada de la STC de 3 de marzo de 2016 sobre el contenido esencial del derecho que reconoce el artículo 18.4 CE y la ausencia de motivación sobre las razones del cambio en la jurisprudencia constitucional. Destaca la "insólita forma" con la que la Sentencia se separa de la jurisprudencia ya elaborada sobre el derecho a la protección de datos de carácter personal en supuestos de video- vigilancia laboral, contenida de manera señalada en la STC 29/2013 , y que se articula sin hacer esfuerzo alguno por abrir un diálogo en divergencia, **ofreciendo al menos explicaciones** , aun cuando fueran de manera sumaria pero fundada, **de los motivos de tan relevante alteración de doctrina** . Razona que el proceso de cambio doctrinal se ha llevado a cabo sin aportar la obligada argumentación jurídico- constitucional sobre las razones que conducen a abandonar una jurisprudencia cuyo objetivo, primero y esencial, fue el fijar los límites del contenido esencial del derecho fundamental que el artículo 18.4 de la CE confiere a los trabajadores. Concluye llamando la atención de la falta de motivación: "En relación con este **silente modo de introducir un drástico giro en la doctrina** establecida por este Tribunal, **no me parece impertinente recordar la obligación de motivar** , en particular en caso de apartamiento de nuestros propios precedentes".

No está de más señalar que el nuevo criterio aplicativo sobre las condiciones exigibles para la validez de las pruebas obtenidas con las cámaras de seguridad había sido también mantenido con anterioridad por algún Tribunal de la jurisdicción social, a pesar de la doctrina de la STC 29/2013 y de la STS 13-5-2014 -que también exige con rigor el cumplimiento del deber de información previo a los trabajadores para admitir las grabaciones como prueba del comportamiento del trabajador-. Así en la STSJ de Cataluña de 11-10-2013 (AS 2013,3149) o del Juzgado nº tres de los Social de Elche de fecha 14-5-2014, que delimitan y distinguen los **supuestos de instalación fija de las cámaras de seguridad** o video vigilancia (que requiere respetar el deber informativo previo ex art. 18.4 CE) **de los casos de instalación puntual de videocámaras** (que requiere respetar el artículo 18.1 CE y el test de proporcionalidad) en la que la falta de información previa es el único medio de constatar un grave incumplimiento laboral.

En definitiva, con la nueva doctrina del tribunal constitucional queda rebajada la exigencia **informativa de la libertad de autodeterminación informativa** que deriva del derecho de protección de datos de carácter personal

(Art. 18.4 CE), al menos tal y como la entendió la Sentencia del Pleno del Tribunal Constitucional 292/2000, de 30 de noviembre , y la STC 29/2013 al determinar el contenido esencial del derecho fundamental **.**

El propio TS aplica esta doctrina de la STC 39/2016 en las sentencias de 31 de enero de 2017 (Rec. 3331/2015), 1 de febrero de 2017 (Rec. 3252/2015) y de 2 de febrero de 2017 (Rec. 554/2016), **considerando suficiente para el cumplimiento del deber de información con la mera exposición en un lugar visible del cartel distintivo** .

En otros ámbitos del derecho el legislador ha decidido regular los medios de prueba derivados de las nuevas tecnologías. Así, de forma destacada, **la reciente LO 13/2015, de 5 de octubre, que modifica la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, exigiendo en la adopción de las mismas el respeto de los principios de idoneidad, excepcionalidad, necesidad y proporcionalidad.** La oportunidad de que el legislador interviniera para regular el ejercicio de las facultades empresariales de control cuando se encuentra en juego la adecuada protección de los derechos fundamentales de los trabajadores ha quedado plasmada en la aprobación de la **LO 3/2018, de 5 de diciembre** , que regula la videovigilancia en el ámbito de las relaciones laborales. La empresa ha invocado para justificar la validez de las grabaciones como medio probatorio del incumplimiento que imputa al trabajador la doctrina de la STC 39/2016 y la nueva regulación legal. Debe determinarse por ello si la nueva regulación legal respeta la exigencia informativa en esta materia conforme resulta de la doctrina del Tribunal Europeo de Derechos Humanos (TEDH), que consagra con carácter general la prohibición de los sistemas de videovigilancia ocultos o encubiertos.

C) La prohibición de la videovigilancia encubierta en la doctrina de la STEDH de 9-01-2018 (caso "López Ribalda y otras v. España")

En la determinación de las exigencias para la validez de las medidas de control de la actividad de los trabajadores a través de la videovigilancia acaba de hacer acto de presencia el Tribunal de Estrasburgo, que dentro de las exigencias que extrae del derecho a la vida privada (artículo 8 del convenio de Roma), en su manifestación del necesario respeto del derecho a la protección de los datos personales, expresamente **condiciona la validez de estas medidas a que se cumpla con rigor el deber informativo previo al trabajador de la finalidad de la instalación de las cámaras, excluyendo expresamente la licitud de las grabaciones encubiertas o no informadas.**

Es importante atender a los hechos ocurridos y que dan lugar a la doctrina del TEDH. Los hechos afectan a cinco demandantes que trabajaban como cajeros en una **cadena de supermercados** . Ante la constatación en 2009 de **desajustes** entre las ventas diarias y el inventario, **el empresario instaló cámaras de vigilancia en el establecimiento** , de dos tipos: unas **visibles** , dirigidas al control de posibles hurtos por parte de los clientes, y otras **ocultas** , focalizadas sobre las cajas, dirigidas a controlar a las trabajadoras. La empresa **informó** a los trabajadores de la instalación de las primeras cámaras, *pero **no de las** segundas* que controlaban directamente a los trabajadores que prestaban servicios en las cajas de los supermercados. Tampoco informó a la representación de los trabajadores. Detectado por el servicio de videovigilancia instalado los comportamientos irregulares por parte de cinco trabajadoras (**apropiarse de productos sin pagar** , cancelar compras sin devolver el dinero, no exigir el pago de determinados productos a clientes y compañeros a quienes se les permitía llevárselos sin abonarlos), la empresa se reunió de forma individualizada con cada uno de los trabajadores grabados cometiendo estas irregularidades. Los trabajadores primero y segundo, que **no firmaron acuerdos transaccionales** , fueron **despedidos disciplinariamente** y su despido fue considerado procedente por el Juzgado de lo Social y por el Tribunal Superior de Justicia de Cataluña. Los trabajadores tercero, cuarto y quinto **firmaron acuerdos transaccionales** en cuya virtud se comprometieron a no recurrir el despido decidido a cambio de que el empresario no emprendiera contra ellos acciones penales por hurto. Ello no obstante, con posterioridad impugnaron sus despidos, alegando coacción al firmar los acuerdos transaccionales. Se desestimó la demanda y el Juzgado de lo Social consideró que los acuerdos transaccionales fueron suscritos libre y voluntariamente. El TEDH acumula los asuntos y dicta la sentencia comentada. Que está pendiente de recurso ante la Gran Sala del propio Tribunal.

La STEDH del caso **" *López Ribalda y otras v. España"* de 9 de enero de 2018** declara la vulneración del artículo 8 del CEDH por parte del Estado español en la ***utilización de sistemas de video vigilanciaencubierta*** conforme a estas conclusiones:

1. La videovigilancia encubierta de un empleado en su lugar de trabajo, debe ser considerada, como tal, como una **importante intromisión en su vida privada** . Supone la documentación grabada y reproducible de la conducta de una persona en su lugar de trabajo, que no puede evitar al estar obligado por el contrato de trabajo a desempeñar su trabajo en dicho lugar (véase STEDH de 5 de octubre de 2010, asunto Kopke v. Alemania, nº 420/07).

2. Recalca la STEDH que adoptar un sistema de video vigilancia **sin informar previamente al trabajador** supone "una intrusión considerable en su vida privada, y una **ilegitima privación del derecho a disponer de los propios datos** , ya que el trabajador se ve privado de saber si le están grabando y qué se hace con esas imágenes, perdiendo todo poder de control y disposición sobre sus propios datos".

3. A pesar de que el propósito del artículo 8 del Convenio de Roma es esencialmente proteger al individuo contra las injerencias arbitrarias del poder público, **el Estado no debe simplemente abstenerse de tal injerencia: además de este compromiso primordialmente negativo, pueden existir obligaciones positivas inherentes a un efectivo respeto por la vida privada.**

4. Estas obligaciones pueden implicar la adopción de medidas destinadas a respetar la vida privada **incluso en el ámbito de las relaciones de los individuos entre sí.**

5. El Tribunal debe examinar si el Estado, en el marco de sus obligaciones positivas en virtud del artículo 8 del Convenio de Roma , ponderó un justo equilibrio entre el derecho de los demandantes al respeto de su vida privada y el interés tanto del empresario en la protección de su organización y el derecho a gestionar sus derechos de propiedad, como del interés público en la adecuada administración de Justicia (**véase STEDH caso *Barbulescu de 5-09-2017*).**

6. La videovigilancia llevada a cabo por el empresario, que se prolongó durante un largo periodo de tiempo, **no cumple con los requisitos establecidos en el artículo 5 de la Ley de Protección de Datos de Carácter Personal de 1999 .**

7. En particular incumplió la obligación de ***informar previamente*** a los interesados **de modo expreso, preciso e inequívoco sobre la existencia y características particulares de un sistema de recogida de datos de carácter personal** .

8. Las demandantes tenían derecho a ser informadas "previamente de modo expreso, preciso e inequívoco" de "la existencia de un fichero o tratamiento de datos de carácter personal, ***de lafinalidad de la recogida de éstos*** y de los destinatarios de la información; del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas; de las consecuencias de la obtención de los datos o de la negativa a suministrarlos; la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición; y de la identidad y dirección del responsable del tratamiento, o en su caso, de su representante".

9. Los derechos del empresario **podrían haber sido protegidos** , por lo menos hasta cierto grado, ***por otros medios,*** en especial, informando previamente a las demandantes, **incluso de una manera general** , sobre la instalación de un sistema de videovigilancia **y dotándolos de la información establecida en la Ley de Protección de Datos de Carácter Personal.**

10. No es de aplicación lo valorado en la STEDH del caso ***Köpke*** porque en ese caso, en el tiempo en que el empresario llevó a efecto la videovigilancia encubierta tras las sospechas de robo contra dos empleadas, todavía no se habían establecido en la legislación alemana las condiciones en las que un empresario podía utilizar la videovigilancia de un empleado para investigar un delito, a diferencia de lo que ocurre con la legislación española. **En una situación donde se hallaba claramente regulado y protegido por ley el derecho del sujeto de observación a ser informado de la existencia, objetivo y modo de la videovigilancia encubierta, las demandantes tenían una expectativa razonable de respeto a su privacidad.**

11. Además , en el presente asunto y **a diferencia de *Köpke*** , **la videovigilancia encubierta no era la consecuencia de una sospecha justificada** contra las demandantes y, en consecuencia, **no iba dirigida específicamente a ellas** , **sino a todo el personal** que trabajaba en las cajas registradoras, **durante semanas** , **sin límite de tiempo y durante todas las horas del trabajo. En *Köpke* la medida de vigilancia estuvolimitada en el tiempo -se llevó a cabo durante dos semanas-, y sólo dos empleados fueron el objetivo de la medida** . **En el presente caso, sin embargo, la decisión de adoptar medidas de vigilancia se basó en una sospecha general contra todo el personal** en vista de las irregularidades que habían sido previamente detectadas por el encargado de la tienda.

12. En una situación donde se hallaba claramente regulado y protegido por ley el **derecho del sujeto de observación a ser informado de la existencia, objetivo y modo de la videovigilancia encubierta** , las demandantes tenían una expectativa razonable de respeto a su privacidad.

Es evidente que este pronunciamiento tiene una fuerza aplicativa importante y que no cabe desconocer. Es necesario atender a la **vinculación que tienen los jueces y tribunales españoles respecto de la doctrina del Tribunal Europeo de Derechos Humanos.** El artículo 10.2 de la CE establece que "Las normas relativas a los derechos fundamentales y a las libertades que la Constitución reconoce **se interpretarán de conformidad con la Declaración Universal de Derechos Humanos y los tratados y acuerdos internacionales sobre las**

mismas materias ratificados por España". Entre ellos, se encuentra al máximo nivel el Convenio de Roma, cuya interpretación corresponde al TEDH.

La vinculación a la jurisprudencia del TEDH llega hasta el punto de que **cabe revisar una sentencia española firme** que haya vulnerado un derecho fundamental conforme a lo declarado por el TEDH. El actual **artículo 5 bis de la LOPJ** - reformada por la LO 7/2015, de 21 de julio- establece: "Se **podrá interponer recurso de revisión** ante el Tribunal Supremo contra una resolución judicial firme, con arreglo a las normas procesales de cada orden jurisdiccional, **cuando el Tribunal Europeo de Derechos Humanos haya declarado que dicha resolución ha sido dictada en violación de alguno de los derechos reconocidos en el Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales y sus Protocolos** , siempre que la violación, por su naturaleza y gravedad, entrañe efectos que persistan y no puedan cesar de ningún otro modo que no sea mediante esta revisión".

Por su parte, el **artículo 219.2 de la LRJS** admite **invocar como sentencia de contradicción** en el recurso de casación para unificación de doctrina las Sentencias del Tribunal Europeo de Derechos Humanos. Dispone que " **Podrá alegarse como doctrina de contradicción** la establecida en las **sentencias** dictadas por el Tribunal Constitucional y los **órganos jurisdiccionales instituidos en los Tratados y Acuerdos internacionales** en materia de derechos humanos y libertades fundamentales ratificados por España, siempre que se cumplan los presupuestos del número anterior referidos a la pretensión de tutela de tales derechos y libertades. La sentencia que resuelva el recurso se limitará, en dicho punto de contradicción, a conceder o denegar la tutela del derecho o libertad invocados, en función de la aplicabilidad de dicha doctrina al supuesto planteado. Con iguales requisitos y alcance sobre su aplicabilidad, **podrá invocarse la doctrina establecida en las sentencias del Tribunal de Justicia de la Unión Europea en interpretación del derecho comunitario".**

Como consecuencia de este valor jurídico parece razonable entender que la jurisprudencia constitucional, y por supuesto el Tribunal Supremo, y demás órganos jurisdiccionales, **deberán adaptar sus criterios a las exigencias informativas que resultan de la doctrina del TEDH** plasmada en la sentencia de 9-01-2018, del caso "López Ribalda ".

No está de más señalar que la misma senda sobre el deberinformativo es la que recorre el Consejo de Europa en laRecomendación CM/Rec (2015)5 sobre el procesamiento de datos decarácter personal en el ámbito del trabajo, aprobada el 1 de abril de 2015 por el Comité de Ministros del Consejo de Europa. Destaca que una descripción particularmente clara y completa de las categorías de datos de carácter personal que pueden recogerse a través del TIC, tales como la videovigilancia, y su posible utilización **debería ser informada** (10.3). **La información deberá proporcionarse de una forma accesible ymantenerla actualizada** . Dicha información, en cualquier caso, **debería ser proporcionada antes de que el empleado ejerza efectivamente la actividad** o acción prevista y ser puesta a disposición de los sistemas de información habitualmente utilizados por el empleado" (10.4). En el apartado **15 se refiere a los "Sistemas y tecnologías de la información para el control de empleados, incluyendo la video vigilancia".** Señala que la introducción y uso de sistemas y tecnologías de la **información cuya *finalidad directa y principal* es el control de la actividad y el comportamiento de los empleados no debería ser permitido** . Cuando su introducción y su utilización **son necesarios para otros fines legítimos** como la protección de la producción, de la salud, la seguridad o la gestión eficaz de una organización y conducen ***indirectamente* a la posibilidad de controlar la actividad de los trabajadores** , **debe ser sometida a los requisitos adicionales contemplados en el principio 21** , incluyendo la consulta de los representantes de los trabajadores (15.1). Los sistemas y tecnologías de la información que controlan la actividad y el comportamiento de los empleados en forma indirecta deben ser especialmente diseñados y colocados para no perjudicar sus derechos fundamentales. No se permite el uso de la video vigilancia para el control de los lugares relacionados con la vida íntima de los trabajadores" (15.2). En el apartado **21 concreta las "Garantías complementarias",** exigiendo que los empresarios respeten la garantía de ***informar previamente* a los empleados de la introducción de sistemas y tecnologías de la información para el control de su actividad, *incluyendo el propósitodel dispositivo*** , la duración de la conservación, la existencia o no de derechos de acceso y rectificación, y la manera en que dichos derechos pueden ser ejercitados. Impone que el empresario tome las medidas internas adecuadas con respecto al tratamiento de los datos **y que se notifiquen previamente a los empleados** . Prevé también como garantía que se consulte a los representantes de los trabajadores con arreglo a la legislación y práctica nacionales antes de la introducción de un sistema de vigilancia o cuando un sistema ya existente debe modificarse. Cuando el procedimiento de consulta revela la posibilidad de una violación del derecho al respeto de la privacidad y la dignidad humana del trabajador, se deberá buscar el acuerdo de los representantes. Por último, consultar, con arreglo a la legislación nacional, a las autoridades nacionales de control en el tratamiento de datos de carácter personal".

D) El deber informativo como requisito imprescindible para la validez de las grabaciones audiovisuales y de los otros medios tecnológicos de control empresarial. Incidencia del Reglamento 2016/679, del Parlamento Europeo y del Consejo, del 27 de abril de 2016

La STEDH comentada **es una llamada de atención en relación a la doctrina del Tribunal Constitucional y del Tribunal Supremo sobre el limitado alcance del deber informativo en materia de video vigilancia** , imponiendo, por el contrario, el **carácter absoluto del deber informativo** vinculado a las garantías propias del derecho a la protección de datos en los términos que establecía el Art. 5 de la Ley 15/1999 , y actualmente el artículo 11 de la **LO 3/2018, de 5 de diciembre, sobre Protección de Datos Personales y garantía de los derechos digitales** y en los artículos 12 , 13 y 14 del **Reglamento 2016/679** del Parlamento Europeo y del Consejo, del 27 de abril de 2016, sobre tratamiento de datos personales y su libre circulación (RGPD).

Cabe entender que es necesario volver al origen de la doctrina del TC, que quedó plasmada en la STC 29/2013 y exigir en el control empresarial un deber informativo previo, concreto y preciso, que incluya la finalidad del sistema implantado, sin reducir su contenido a las menciones de las reglas prohibitivas generales que existan en las empresas o a la mera colación del cartel informativo. Al menos mientras nuestra legislación regule el derecho de autodeterminación informática con el alcance actual, ***y especialmente a la vista de laregulación del Reglamento 2016/679, que no excepciona el deberinformativo en supuestos de video vigilancia.***

No parece, por otra parte, que puedan desvincularse los pronunciamientos de los casos "Barbulescu II" - STEDH de 5-09-2017 , Barbulescu contra Rumanía- **y "López Ribalda"** porque, aunque el primero se refiera al secreto de las comunicaciones y a la intimidad en mensajes enviados por un trabajador a través del sistema *"Yahoo Messenger"* y el segundo a la video vigilancia encubierta, **en ambos casos se razona con fundamento en el mismo derecho, el consagrado en el artículo 8 de Convenio europeo de derechos humanos , a saber, el derecho a la vida privada , con su contenido complejo que comprende el derecho a la intimidad, al secreto de la correspondencia, a la inviolabilidad domiciliaria y a la protección de datos de los datos personales.**

La idea de la que se debe partir al determinar el contenido esencial del derecho que consagra el artículo 18.4 de la CE es que si la legislación reconoce unas determinadas garantías vinculadas al derecho fundamental a la protección de datos de carácter personal, **necesariamente deberán respetarse por el empleador, sin que el control empresarial sea legítimo ni válido si se aplica desconociendo tales garantías. En este caso, se deberá respetar el deber informativo previo que permita tener cabal conocimiento de quién posee los datos personales y para qué se utilizan** . Sólo así podrá el trabajador manifestar su consentimiento o solicitar la rectificación, limitación, cancelación o supresión de los datos.

Por otra parte, **no cabe desconocer que la doctrina** "flexibilizadora" sobre cumplimiento del deber informativo del Tribunal Constitucional y del Tribunal Supremo **queda afectada por las nuevas exigencias que derivan del Reglamento 2016/679** del Parlamento Europeo y del Consejo, del 27 de abril de 2016, sobre protección de datos personales, que en la regulación de la transparencia y del deber informativo **impone unas exigencias que no cabe obviar** y que, además, extiende su ámbito aplicativo al control empresarial de la actividad laboral a través de otros medios tecnológicos.

Como sabemos **la norma europea es de directa aplicación** (Art. 288 TFUE). Al ser un Reglamento de la Unión Europea es predicable de él dos concretos efectos jurídicos: a) la **aplicación directa** , tanto en las relaciones verticales como en las horizontales, constituyendo una norma jurídica perfectamente invocable ante los Tribunales de Justicia; b) la **primacía frente a las normas de los Estados miembros que lo contradigan** , debiendo el juez nacional inaplicar cualquier norma interna que incurra en dicha contradicción.

Conforme a la jurisprudencia comunitaria **cabe distinguir tres manifestaciones principales de la primacía del Derecho de la Unión Europea:**

a) **Prevalencia del derecho originario sobre el derecho interno en términos absolutos y globales,** de manera que en caso de contradicción entre las normas nacionales infraconstitucionales y el Derecho de la Unión, **el juez nacional tiene la obligación de inaplicar la ley interna por su propia autoridad** , sin esperar a su previa depuración por el propio legislador o la jurisdicción constitucional (SSTJCE 09/03/1978 asunto "Simmenthal ", ap. 17; 22/06/2010 (TJCE 2010, 439), asunto "Melki y Abdeli", ap. 43 ; y 05/10/2010 (TJCE 2010, 287), asunto "Elchinov ", ap. 31. **La obligación de inaplicar la norma nacional incompatible vincula a todos los jueces y tribunales ordinarios *ya sea la norma anterior o posterior a la norma delDerecho de la Unión* , y con independencia del nivel jurisdiccional en que se plantee la cuestión).**

b) **Prevalencia o primacía de la jurisprudencia comunitaria sobre la doctrina o jurisprudencia de los tribunales de los países miembros en la interpretación o aplicación de los preceptos y disposiciones del Derecho de la Unión Europea** , porque de conformidad con lo que establece el artículo 267 del TFUE la doctrina establecida por el TJUE, al resolver cuestiones prejudiciales, ***esvinculante para el juez español. También para el Tribunal***

Supremo yha de acatarla (como recuerda la STS 23-03-2015, en rcud 2057/14 (RJ 2015, 1250), y declararon las STJCE 14-12-1982, asunto Waterkeyn; 5- 03.1996, asuntos Brasserie du pêcheur y Factortame, C-46/93 y C-48/93). ***Hoy consagra la vinculación del juez español a lajurisprudencia comunitaria el Art. 4 bis de la LOPJ .***

c) Obligada interpretación de la normativa interna a la luz de la legislación y jurisprudencia comunitarias -la llamada "interpretación conforme"-.

Pues bien, **el RGPD establece unos principios y unas exigencias aplicables para garantizar la tutela del derecho a la protección de los datos personales que no cabe desconocer en el enjuiciamiento de la validez de los distintos medios de control empresarial de la actividad de los trabajadores** . A la vista de la concepción amplísima de las nociones de *dato personal* y *tratamiento* que se contiene en el RGPD difícilmente puede considerarse que la información a la que se accede en el control empresarial de los medios tecnológicos e informáticos que utilizan los trabajadores no constituya, cabalmente, un "dato personal" y que tal actividad sea, al mismo tiempo, " *tratamiento* ". De la misma forma que la imagen -sistemas de videovigilancia- constituye un dato personal, también lo es la información a la que se accede cuando se controla la navegación por Internet, los ordenadores y los correos electrónicos La consecuencia jurídica no es otra que **extender al control empresarial de los medios tecnológicos las mismas exigencias que el Reglamento europeo -sin excepción alguna aplicable a las relaciones laborales-, impone al tratamiento de los datos personales** . Como sabemos, entre dichas exigencias se encuentra la **transparencia en el tratamiento y el deber informativo previo** a realizar la actividad.

El artículo 4 del RGPD define los "datos personales" como ***todainformación sobre una persona física identificada o identificable*** ("el interesado"). Y se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona".

El mismo precepto define el concepto de tratamiento con tal amplitud que necesariamente debemos entender que comprende el acceso a la información del trabajador que se obtenga en el análisis o examen de los ordenadores y demás medios tecnológicos. Señala que "tratamiento" es "cualquier operación o conjunto de operaciones realizadas **sobre datos personales** o conjuntos de datos personales, ya **sea por procedimientos automatizados o no** , como la ***recogida*** , registro, organización, estructuración, conservación, adaptación o modificación, ***extracción*** , ***consulta*** , ***utilización*** , comunicación por transmisión, difusión o ***cualquier otra forma de habilitación de acceso*** , cotejo o interconexión, limitación, supresión o destrucción".

El **deber de transparencia e informativo se regula en los artículos 12, 13 y 14 del RGPD.** Por lo que ahora interesa, cabe destacar que el RGPD hace **más exigente el deber informativo** , que se **debe cumplir a través de capas o niveles, el básico y el adicional. Además de la información por capas,** se establece una lista exhaustiva de la información que debe proporcionarse a los interesados (más amplia que la que reflejada en la LOPD de 1999) y que comprende: la información sobre el responsable del tratamiento; ***la finalidad del tratamiento*** ; la legitimación o título que legitima el tratamiento; los destinatarios de las cesiones o transferencias de los datos; los derechos de las personas; los datos del Delegado de Protección de Datos y la procedencia o fuente de los datos.

Es importante resaltar que este régimen jurídico y los requisitos vinculados al deber informativo son aplicables en todo caso, con carácter vinculante en todos los Estados Miembros. Y **que no se prevé excepción alguna aplicable a las relaciones laborales. Por lo tanto, si no es por aplicación directa de la doctrina del TEDH, en cualquier caso los tribunales españoles deberán aplicar las mismas exigencias informativas como una consecuencia obligada de lo que impone el RGPD al regular el deber informativo.**

Los artículos 12, 13 y 14 del RGPD imponen a todo responsable del tratamiento de datos personales el deber de transparencia e informativo, y **tal deber comprende el informar al interesado de la finalidad de la obtención de los datos** . **No establece ninguna excepción aplicable alas relaciones laborales.** Por lo que al empresario se le impone conforme al RGPD y la jurisprudencia del TEDH cumplir con la exigencia informativa de la finalidad de los sistemas de video vigilancia.

La anterior conclusión es relevante tenerla en cuenta al analizar el contenido de la reciente **Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales** , en la medida que ahora contiene una regulación expresa de las medidas de control empresarial que afectan al derecho fundamental a la intimidad de los trabajadores y al derecho a la protección de datos. Como la norma española **sólo puede complementar el reglamento europeo en aquello que este permite, y sin contradecir en ningún caso la regulación esencial del propio reglamento** -aplicable de forma directa y con eficaz primacía frente a las normas nacionales-, cabe concluir sin dificultad que ***en ningún caso la ley española puede rebajar***

las exigencia del deberinformativo que establece el RGPD en los términos señalados. Y si lo hace **el juez español deberá simplemente inaplicar la norma española** contradictoria como consecuencia de la primacía del reglamento europeo.

Aclarar, por último, **que las previsiones del artículo 88 del RGPD no autorizan** que el legislador español -ni tampoco los convenios colectivos- pueda excepcionar el régimen del deber de transparencia e informativo que incumbe al responsable del tratamiento de los datos personales porque **la llamada que realiza a los ordenamientos nacionales *en el ámbito de las relaciones laborales queda circunscritaal establecimiento de garantías adicionales o más específicas, nuncaa reducirlas*** , y mucho menos en un aspecto tan esencial en la configuración del derecho a la protección de datos como es el deber informativo previo al tratamiento, que no deja de ser consecuencia de su propia razón de ser como **cancerbero fiel de los otros derechos fundamentales, adelantando las medidas de protección para evitar que se lesionen los derechos a la intimidad, a la imagen o al secreto de las comunicaciones** .

En efecto, el artículo 88 del RGPD dispone que los Estados miembros podrán, **a través de disposiciones legislativas o de *convenios colectivos* ,** establecer ***normas más específicas*** para ***garantizar*** la protección de los derechos y libertades en relación con el **tratamiento de datos personales de los trabajadores *en el ámbitolaboral*** , en particular a efectos de contratación de personal, ejecución del contrato laboral, incluido el cumplimiento de las obligaciones establecidas por la ley o por el convenio colectivo, gestión, planificación y organización del trabajo, igualdad y diversidad en el lugar de trabajo, salud y seguridad en el trabajo, protección de los bienes de empleados o clientes, así como efectos del ejercicio y disfrute, individual o colectivo, de los derechos y prestaciones relacionados con el empleo y a efectos de la extinción de la relación laboral. Pero esa llamada a la regulación nacional específica **no deja una libertad regulatoria absoluta** , sino que dispone que dichas normas incluirán medidas adecuadas y específicas para **preservar** la **dignidad** humana de los interesados, así como sus intereses legítimos **y sus derechos fundamentales, prestando especial** atención a la **transparencia** del tratamiento, a la transferencia de los datos personales dentro de un grupo empresarial o una unión de empresas dedicadas a una actividad económica conjunta y a los **sistemas de supervisión en el lugar de trabajo.**

Como vemos **el margen del legislador nacional no alcanza a restringir los derechos esenciales vinculados a la eficaz protección de los datos personales y mucho menos a degradar las exigencias del deber informativo previo** , lo que pone en cuestión las previsiones limitativas de la **Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales** . Especialmente al regular la videovigilancia en las relaciones laborales.

E) El deber informativo en la LO 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales

Teniendo en cuenta los límites señalados cabe analizar las previsiones de la **Ley Orgánica 3/2018, que la empresa demandada ha invocado como argumento adicional de refuerzo de la validez de la prueba de grabación que propuso en el acto del juicio** .

Por primera vez en nuestro ordenamiento jurídico se regula el control empresarial de la actividad de los trabajadores cuando colisiona con los derechos fundamentales a la intimidad y a la protección de los datos personales.

Regula de forma expresa el **derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos *en ellugar de trabajo* (Art. 89).** Lo primero que llama la atención es que sólo mencione el derecho a la intimidad, obviando la estrecha vinculación de la videovigilancia con el derecho a la protección de datos. Tampoco proporciona la exposición de motivos explicación alguna sobre las razones por las que no se menciona el derecho que consagra el artículo 18.4 de la CE .

Previamente, al regular con carácter general los sistemas de videovigilancia para la seguridad de las personas, instalaciones y bienes, expresamente dispone que **el tratamiento por el *empleador* de datos obtenidos a través de sistemas de cámaras o videocámaras se somete a lo dispuesto en el artículo 89 de la ley orgánica** (Art. 22.8 de la LO 3/2018).

Dada la novedad de esta regulación, no está de más transcribir cómo queda redactado el artículo 89 de la LO 3/2018 :

*1. "Los empleadores **podrán tratar las imágenes** obtenidas a través de sistemas de cámaras o videocámaras 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*** .

Los empleadores ***habrán de informar con carácter previo*** *, y de forma* ***expresa, clara y concisa*** *, a los trabajadores o los empleados públicos y, en su caso, a sus representantes,* ***acerca deesta medida*** *.*

En el supuesto de que se haya captado la comisión flagrante de un ***acto ilícito*** *por los trabajadores o los empleados públicos* ***seentenderá cumplido el deber de informar cuando existiese almenos el dispositivo al que se refiere el artículo 22.4 de esta leyorgánica*** *.*

2. ***En ningún caso*** *se admitirá la instalación de sistemas de grabación de sonidos ni de videovigilancia en lugares destinados al descanso o esparcimiento de los trabajadores o los empleados públicos, tales como* ***vestuarios, aseos, comedores y análogos*** *.*

3. La utilización de sistemas similares a los referidos en los apartados anteriores para la **grabación de sonidos** en el lugar de trabajo **se admitirá únicamente cuando resulten relevantes los riesgos para la seguridad** de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo **y siempre respetando el principio de proporcionalidad, el de intervención mínima y las garantías previstas** en los apartados anteriores. La **supresión de los sonidos** conservados por estos sistemas de grabación se realizará atendiendo a lo dispuesto en el apartado 3 del artículo 22 de esta ley".

De forma natural **surgen dudas importantes sobre esta regulación** . Entre otras, determinar los límites inherentes al ejercicio de las funciones de control empresarial, o qué significación y alcance tiene la referencia del legislador al deber de informar al trabajador " *acerca de esta medida*" . Pueden existir dudas sobre si es exigencia legal concretar la finalidad o finalidades para las que se establecen las medidas de control empresarial, y si incluye la finalidad sancionadora para el caso de que se graben incumplimientos laborales. Tampoco aclara la ley si la información previa va referida a una antelación general desde que se adopta la medida o a una antelación específica si la videovigilancia se concreta en uno o varios trabajadores, o si quedan absolutamente prohibidas las grabaciones encubiertas. **Queda indeterminado o no definido el concepto de acto ilícito** , y no se expresan las razones que justificaron que de la redacción inicial del proyecto de ley del Gobierno -que se refería a la ***captación de un delito*** - se haya pasado en la redacción final del precepto a la referencia a la captación por las cámaras de vigilancia de la comisión fragante de un ***acto ilícito*** a los efectos de exigir sólo para cumplir las exigencias de protección del derecho y la validez de la prueba que el empresario hubiera colocado el cartel informativo sobre zona videovigilada. Parece a primera vista que el hecho de que se entienda cumplido el deber informativo con el dispositivo *"zona videovigilada"* cuando se capta un acto ilícito significa que la prueba es válida y se puede sancionar al trabajador. Pero entonces, **¿para qué se exige la información "previa, expresa, clara y concisa" acerca de la medida de videovigilancia si en todo caso tendrá valor probatorio aunque se omitan tales exigencias informativas?**

En definitiva, **es necesario pronunciarse si esta regulación se acomoda a las exigencias del derecho fundamental a la privacidad y a la protección de datos personales conforme a la doctrina del TEDH, y si respeta las exigencias del deber informativo que impone el Reglamento europeo de protección de datos personales** .

Cabe dar una respuesta jurídica a estas cuestiones tomando como fundamento la doctrina del TEDH en las Sentencias "Barbulescu II" y "López Ribalda" y las exigencias derivadas del reglamento europeo de protección de datos. Es importante destacar que esta doctrina no puede entenderse de forma separada, considerando que la primera sólo es aplicable al control de las comunicaciones del trabajador -"Yahoo Messenger" en el caso- y la segunda sólo a la videovigilancia. En realidad **ambas se construyen sobre la base del derecho a la privacidad** que consagra el artículo 8 del Convenio de Roma , que comprende el derecho a la protección de los datos personales, de manera que aunque se deba introducir matizaciones según el medio de control utilizado por la empresa, sin embargo, **en los aspectos esenciales la doctrina del TEDHdescansa sobre unos mismo mimbres conceptuales** vinculados al concepto amplio de privacidad, y por ello presenta un efecto de irradiación que no cabe desconocer. Tampoco puede sorprender esta estrecha relación si se tiene en cuenta que en el control de las comunicaciones, de los correos electrónicos, de la navegación por Internet o de los datos obtenidos de los ordenadores y demás medios tecnológicos en general, **se acceda a información que constituye dato personal** conforme a la definición del artículo 4 del Reglamento europeo de protección de datos, y con ello deben ser aplicables sus garantías y exigencias. Entre ellas, por lo que ahora interesa destacar, el cumplimiento del deber informativo. Precisamente por ello, **además de la doctrina del TEDH, necesariamente habrá que tener en cuenta las disposiciones del reglamento y el conjunto de principios y exigencias que establece dada su eficacia directa y la primacía sobre las normas de los Estados miembros** .

Se hace mención a la anterior cuestión porque si hasta ahora el TEDH en la sentencia López Ribalda razonó la vulneración del artículo 8 del Convenio de Roma porque la grabación encubierta suponía desconocer el derecho que incumbe al trabajador a ser informado antes del tratamiento de sus datos conforme a lo previsto en la LOPD española de 1999 (otorgando relevancia a la regulación del derecho a la vida privada tal y como se

hubiera configurado en la legislación nacional), **actualmente la normativa directamente aplicable no es otra que el reglamento *europeo*** -desde el 25 de mayo de 2018-, **sin que la norma española pueda contradecir sus mandatos esenciales, entre los que se encuentra, sin duda alguna, el preceptivo deber informativo y las exigencias de transparencia del tratamiento , no exceptuadas para las relaciones laborales cuando el empleador utiliza medidas de control de la actividad laboral** .

Por eso, no parece posible apreciar un resquicio a la prohibición de las cámaras ocultas con la cita que la sentencia del caso López Ribalda hace a la STEDH de 5 de octubre de 2010, del asunto Kopke v. Alemania, nº 420/07. En primer lugar, porque la propia sentencia ya recoge que en el tiempo en que el empresario llevó a efecto la videovigilancia encubierta tras las sospechas de robo contra dos empleadas, todavía no se habían establecido en la legislación alemana las condiciones en las que un empresario podía utilizar la videovigilancia de un empleado para investigar un delito; y, en segundo, lugar, porque ***actualmente es de aplicación elreglamento europeo de protección de datos personales, que consagrasin excepciones el deber de transparencia e informativo.***

Tampoco hay que perder de vista que tanto el derecho a la privacidad como el derecho a la protección de datos personales tienen consagración en los **artículos 7 y 8 de la Carta europea de derechos fundamentales** , cuyo **valor jurídico es el propio del derecho originario** de la Unión Europea, y sus preceptos deben ser aplicados e interpretados conforme a la doctrina del TEDH.

En efecto, el artículo 7 de la **Carta de los Derechos Fundamentales de la Unión Europea** dispone que "Toda persona tiene **derecho al respeto de su vida privada** y familiar, de su domicilio **y de sus comunicaciones** ". El **artículo 8** consagra el **derecho a la protección de datos personales** . Establece que "Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan (Art. 8.1). Exige que los datos "se tratarán de modo leal, *para fines concretos* y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación" (art. 8.2).

Por otra parte, el **valor jurídico de la Carta de Derechos Fundamentales de la Unión Europea** viene establecido sin límite alguno en el Art. 6.1 del TUE . El precepto **no deja margen de duda sobre la consideración de esos derechos y principios de la Carta como parte integrante del derecho primario y como tal de aplicación directa, no sólo en su eficacia vertical sino también en la horizontal o en litigios entre particulares.** Dispone que "La Unión reconoce los derechos, libertades y principios enunciados en la Carta de los Derechos Fundamentales de la Unión Europea de 7 de diciembre de 2000, tal y como fue adaptada el 12 de diciembre de 2007 en Estrasburgo, la cual tendrá el mismo valor jurídico que los Tratados".

Hay dos aspectos especialmente relevantes que deben tenerse en cuenta en la aplicación e interpretación de los derechos que reconoce la Carta. En primer lugar, que **cualquier limitación** del ejercicio de los derechos y libertades que reconoce **deberá ser establecida por la ley** y respetar el **contenido esencial** de dichos derechos y libertades. Además, dentro del respeto del principio de proporcionalidad, **sólo podrán introducirse limitaciones cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás** (garantía de reserva de ley, respecto del contenido esencial y necesidad de la limitación que consagra el artículo 52.1 de la Carta). En segundo lugar, que en la medida en que la Carta consagra derechos que correspondan a derechos garantizados por el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, **su sentido y alcance serán iguales a los que les confiere dicho Convenio** (Art. 52.3 de la Carta). Y lógicamente ese alcance lo determina el **Tribunal Europeo de Derechos Humanos** .

Conforme a lo expresado podemos contestar a las dudas sobre el alcance de la reforma legal en los siguientes términos:

1. Los **límites inherentes al control empresarial** a través de la videovigilancia son, lisa y llanamente, el **necesario respeto de los derechos fundamentales** del trabajador y significadamente los derechos a la intimidad, a la imagen y a la protección de datos personales. Ese respeto conlleva que debe aplicarse la doctrina conocida sobre incidencia de las funciones de vigilancia empresarial en los derechos fundamentales, que **sólo pueden ser objeto de limitaciones en la medida estrictamente necesaria para satisfacer un derecho o un interés legítimo del empleador.** Por lo mismo, la medida de control **sólo es válida si supera el juicio de proporcionalidad** (idoneidad, necesidad y proporcionalidad).

2. Informar **acerca del alcance de la medida** no puede entenderse sino como expresa **información de la finalidad** del sistema instalado.

3. Por eso, **sí que debe concretarse por el empleador que incluye la finalidad sancionadora** si se captan incumplimientos laborales de los trabajadores.

4. En la medida que este modo de controlar la actividad de los trabajadores incide especialmente en su derecho a la protección de datos -la imagen es un dato personal-, cabe entender que **el momento en que debe suministrarse la información sobre la finalidad es precisamente cuando se instalan las cámaras** , y también cada vez que se contrate a un trabajador. Lógicamente **, si la empresa no tenía instalado este sistema, y lo dispone a raíz de sospechas de irregularidades** de algún o algunos trabajadores, **es ese momento cuando deberá informarles** que se instalan las cámaras y que su finalidad incluye el sancionar los incumplimientos laborales. La norma europea no excepciona ningún supuesto que legitime la intervención sin cumplir la exigencia informativa y la doctrina del TEDH tampoco.

5. Efectivamente, dado que existe un deber de informar previamente al trabajador de la instalación de las cámaras de vigilancia, ya no serán posibles y **quedan absolutamente prohibidas las grabaciones encubiertas u ocultas, que es tanto como decir no informadas** . Las **sospechas de irregularidades** graves en el desempeño de la actividad laboral **no legitiman una excepción** del deber de informar de la grabación que afecta al puesto objeto de sospecha, **ni exonera de cumplir las exigencias del RGPD.** La empresa siempre dispone de un medio de defensa de sus intereses, como es el anuncio de la grabación de las imágenes y de la finalidad, que ofrece ya una protección sobre su patrimonio por la función disuasoria que razonablemente debe producir.

6. Por ***acto ilícito*** sólo cabe entender lo que la propia expresión indica: **cualquier acto que contraría el ordenamiento es un acto ilícito.** Es ilícito el acto que constituye delito. También lo es el que constituya una infracción administrativa. Y, por último, los incumplimientos de las obligaciones laborales quedan incluidos en esa noción.

7. No podemos conocer la razón que determinó que de la redacción inicial - ***captación de un delito*** - se haya pasado en el informe de la ponencia del proyecto de la ley orgánica y en el texto definitivo a hacer mención al *" **acto ilícito"*** . La redacción actual es consecuencia de una enmienda que, por desgracia, en su justificación no ofreció argumentos que sirvan al intérprete para orientarle y poder dar una respuesta más segura sobre el alcance de la expresión.

8. En la mente del legislador español parece estar presente el criterio de que en el supuesto de que las cámaras de vigilancia captan actos ilícitos fragantes la prueba obtenida es válida, aunque no se haya cumplido con las exigencias del deber informativo y sólo figure el dispositivo ***"zona videovigilada".*** Ello supondría que el trabajador a quien se refiera la grabación y que realizó el acto ilícito podrá ser sancionado. **Supone volver a la doctrina restrictiva de la STC 39/2016 , claramente superada por la STEDH *"López Ribalda* ".**

9. En efecto, la anterior conclusión plantea la evidente contradicción con la exigencia legal de ofrecer a los trabajadores una **información "previa, clara, precisa y concisa" acerca de la medida de video vigilancia.** Es una previsión legal inane cuando en todo caso tendrá valor probatorio la grabación aunque se omitan tales exigencias informativas.

10. Lo que si podemos concluir es que **excluir la exigencia informativa de la finalidad de la videovigilancia,** que forma parte del contenido esencial del derecho fundamental a la protección de datos personales, supone que la LO 3/2018 **noestá respetando el derecho a la privacidad y a la protección de datos personales conforme a la doctrina del TEDH** .

11. Al mismo tiempo, tampoco respeta las **exigencias del deber informativo que impone el Reglamento europeo de protección de datos personales** . El RGPD establece el deber informativo de la finalidad del tratamiento de los datos personales como instrumento esencial para garantizar la protección eficaz del derecho a la protección de datos y **no permite degradar la exigencia en el ámbito de las relaciones laborales** .

12. La consecuencia obligada para el juez español no puede ser otra que **extraer las consecuencias del incumplimiento del deber informativo** en el tratamiento de los datos que resultan del sistema de video vigilancia del que no se suministró la debida información al trabajador porque la empresa no le instruyó que los datos obtenidos podían ser tratados con finalidad sancionadora **. Determinará que la prueba obtenida es nula de pleno derecho por vulnerar un derecho fundamental** y no debería ser admitida a trámite o, de llegar a practicarse, no podrá atribuirse valor probatorio a las imágenes grabadas.

13. No es necesario que el juez plantee una cuestión de inconstitucionalidad ante el TC ni una cuestión prejudicial ante el TJUE. Podrá simplemente inaplicar la norma nacional que no respeta el derecho originario de la Unión Europea (Carta) y el derecho derivado dotado de eficacia directa y primacía en las relaciones verticales y en las horizontales (RGPD) , extrayendo las consecuencias jurídicas que resultan de las exigencias y garantías de la Carta europea de derechos fundamentales y del reglamento europeo de protección de datos personales. En su caso, si mantuviera una duda razonable siempre podrá plantear la cuestión prejudicial, lo que constituye una obligación si contra la sentencia del tribunal no cabe recurso.

Para finalizar esta cuestión cabe señalar que indudablemente era mucho más clara la **propuesta de un grupo parlamentario** plasmada en una enmienda al proyecto de ley para la regulación del **derecho a la intimidad ante la utilización de sistemas audiovisuales o de geolocalización en el ámbito laboral.** Establecía un escrupuloso respeto del deber informativo en estos términos: " **Con carácter previo** , los empleadores habrán de informar de forma expresa, clara e inequívoca a los trabajadores acerca de la existencia, localización y características de estos dispositivos, *así como del alcance disciplinario que derive de los* datos obtenidos de los mismos".

Por otra parte, **un sector de la doctrina considera que si hay previas sospechas fundadas de la comisión de actos ilícitos por parte del trabajador (hurtos a clientes o empleados) es obvio que el deber de transparencia no puede amparar, ni facilitar al trabajador la comisión de un acto ilícito y tampoco hacer imposible la comprobación de actos ilícitos** . Propugna esta corriente que prevalezca el interés público de la sociedad y las salvaguardias contra la ilegalidad, y con ello admitir la posibilidad de un control oculto mediante cámaras cuando tiene un verdadero carácter defensivo. Se afirma que ese carácter defensivo esta latente en la sentencia nº 186/2000 del TC , que admite el recurso al control oculto con base en los hurtos que se vienen registrando en las cajas de un economato.

Sin embargo, conviene no confundir la legitimidad del fin con laconstitucionalidad del medio para su consecución . Con claridad dejó declarado la doctrina constitucional que "esa lógica fundada en la utilidad o conveniencia empresarial haría quebrar la efectividad del derecho fundamental, **en su núcleo esencial** . En efecto, **se confundiría la legitimidad del fin** (en este caso, la verificación del cumplimiento de las obligaciones laborales a través del tratamiento de datos, art. 20.3 ET en relación con el art. 6.2 LOPD) **con la constitucionalidad del acto** (que exige ofrecer previamente la información necesaria, art. 5 LOPD), cuando lo cierto es que cabe proclamar la legitimidad de aquel propósito (incluso sin consentimiento del trabajador, art. 6.2 LOPD) pero, del mismo modo, declarar que **lesiona el artículo 18.4 CE la utilización para llevarlo a cabo de medios encubiertos que niegan al trabajador la información exigible** " (STC 29/2013).

Por otra parte, **en la hipótesis de sospechas de la comisión de hurtos o de otras conductas delictivas parece que lo más razonable es impetrar el auxilio judicial** , de modo que el empresario debería interponer la correspondiente denuncia y solicitar las medidas de investigación del delito adecuadas, incluida la videovigilancia, que podrá acordarse si resulta eficaz a los fines de la instrucción penal y si concurren los requisitos legales, salvaguardo así los derechos del empleador, sólo que con el amparo y debido control judicial.

La propia Ley 5/2014, de Seguridad Privada, dispone que las grabaciones realizadas por los sistemas de videovigilancia no podrán destinarse a un uso distinto del de su finalidad (Art. 42.4). Previendo que cuando las mismas se encuentren relacionadas con hechos delictivos o que afecten a la seguridad ciudadana, se aportarán, de propia iniciativa o a su requerimiento, a las Fuerzas y Cuerpos de Seguridad competentes, respetando los criterios de conservación y custodia de las mismas para su válida aportación como evidencia o prueba en investigaciones policiales o judiciales. A su vez, exige que la monitorización, grabación, tratamiento y registro de imágenes y sonidos por parte de los sistemas de video vigilancia ***se realice conforme a loprevisto en la normativa en materia de protección de datos decarácter personal,*** y **especialmente conforme a los principios de proporcionalidad, idoneidad e intervención mínima.**

F) Aplicación de las exigencias anteriores al caso enjuiciado

Los anteriores razonamientos determinan que en el presente caso **deba ratificarse la decisión adoptada en el propio acto del juicio de inadmitir la prueba consistente en el visionado de las grabaciones realizadas por las cámaras de seguridad** de la empresa demandada, y ello porque la empresa demandada **no cumplió las exigenciasvinculadas al necesario respeto al derecho de protección de datos que amparaba al trabajador demandante, incluyendo el deber informativo sobre la existencia de sistema de videovigilancia y la propia finalidad para la que se utilizaba , incluyendo la posibilidad de sancionar si captan actos ilícitos o incumplimientos laborales** .

Hay que destacar que los hechos que han dado lugar al despido disciplinario del trabajador son anteriores a la entrada en vigor de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Y, **desde esta perspectiva temporal, ni siquiera la nueva regulación es aplicable al caso enjuiciado a pesar de la alegación realizada en el acto del juicio por la empresa demandada** . Y **tampoco se estima aplicable la doctrina que cita** de la STC 39/2016 porque **en los términos razonados lo cierto es que el deber informativo sobre el alcance de las medidas de videovigilancia, incluyendo la finalidad sancionadora, es una exigencia que se impone en todo caso , más allá de la mera colocación del cartel informativo, *conforme a la jurisprudencia del Tribunal Europeo de DerechosHumanos y el propio Reglamento General de Protección de Datos*** a que se ha hecho referencia, que obligan a su aplicación y a interpretar la propia normativa nacional en los términos que exige el TEDH y que se derivan del Reglamento Europeo, dotado de eficacia directa y primacía frente a la norma nacional que contradiga su contenido, teniendo en cuenta que **en dicho reglamento**

no se establece excepción alguna al deber de transparencia e informativo en materia de protección de datos aplicable a las relaciones laborales .

TERCERO.- Valoración de otras pruebas que acreditan el incumplimiento laboral imputado al trabajador.

El que se haya inadmitido la prueba de la grabación de las cámaras de seguridad no quiere decir que en el presente caso los hechos que se imputaban al demandante en la carta de despido no hayan quedado acreditados con otros medios probatorios que no estén vinculados o relacionados con lo captado en las cámaras de videovigilancia. En concreto, **la prueba testifical practicada en el acto del juicio fue clara** , habiendo declarado los dos testigos las circunstancias en las que se produjo la agresión del demandante y del otro trabajador, viéndose implicados en una pelea que, finalmente, determinó el despido disciplinario de los dos trabajadores.

Declaró en el acto del juicio, como se ha indicado en el fundamento de derecho primero de esta sentencia, **un testigo presencial de los hechos** , y también el responsable de recursos humanos, y tanto uno como otro **confirman la realidad de los hechos imputados al demandante** que, es más que evidente, son de una gran gravedad y **justifican la sanción del despido disciplinario** que le ha impuesto la empresa demandada, sin que pueda admitirse las alegaciones de la parte actora en orden a la inexistencia del hecho imputado o al desconocimiento de la persona que le entregó la carta de despido al quedar plenamente determinado que le fue entregada por el responsable de Recursos Humanos y en representación de la empresa.

Por otra parte, debe tenerse en cuenta que en las faltas laborales que consisten en ofensas verbales o físicas al empresario o a las personas que trabajan en la empresa, la calificación de la conducta como incumplimiento laboral grave y culpable no exige que estemos en presencia de una conducta reiterada, pues basta con una ofensa aunque sea aislada que en el contexto en que se realizó ponga de manifiesto un incumplimiento grave, máxime cuando se trata de actos de violencia y agresión física, que constituyen sin duda justa causa para el despido disciplinario en supuestos como el aquí enjuiciado en que dos trabajadores se enzarzan y se agraden mutuamente, dentro del recinto del centro de trabajo, con golpes recíprocos y usando una fusta y un casco de una moto.

En definitiva, estando acreditados los hechos y correctamente tipificados conforme a las previsiones del Estatuto de los Trabajadores y del convenio colectivo de aplicación, y siendo además adecuados a la gravedad de la conducta desarrollada por el demandante y por el otro trabajador, no cabe sino **dictar sentencia declarando procedente el despido** (Art. 55 ET) y, con ello, desestimar la demanda.

CUARTO.- A tenor de lo dispuesto en el Art. 97.4 de la LRJS se deberá indicar a las partes si la Sentencia es firme o no, y en su caso los recursos que contra ella proceden, así como las circunstancias de su interposición. En cumplimiento de ello se advierte a las partes que la presente resolución no es firme y que contra ella puede interponerse RECURSO DE SUPLICACIÓN, con todos los requisitos que en el fallo se señalan, según se desprende del Art. 191 LRJS .

Vistos los arts. 9 , 117 y siguientes de la Constitución Española , así como los arts. 2 , 5 y concordantes de la Ley Orgánica del Poder Judicial y todos los que son de aplicación en estas actuaciones.

FALLO

Que desestimando la demanda sobre despido disciplinario improcedente deducida por D. Víctor frente a la empresa NUCAP EUROPE SL, debo declarar y declaro procedente el despido del demandante y, en consecuencia, debo absolver y absuelvo a la empresa demandada de las pretensiones frente a ella deducidas.

Contra esta sentencia cabe recurso de Suplicación ante la Sala de lo Social del Tribunal Superior de Justicia de Navarra, que se anunciará dentro de los CINCO DÍAS siguientes a su notificación, bastando para ello la manifestación de la parte, de su Abogado o de su representante en el momento de la notificación pudiendo hacerlo también estas personas por comparecencia o por escrito ante este Juzgado en el mismo plazo.

Al hacer el anuncio, se designará por escrito o por comparecencia, Letrado o Graduado Social colegiado que dirija el recurso, y si no lo hace, habrá que proceder al nombramiento de oficio, si se trata de trabajador o empresario con beneficio de Justicia Gratuita.

Así por esta mi sentencia, lo pronuncio, mando y firmo.

E/.