Control empresarial de la actividad laboral mediante video vigilancia y colisión con los derechos fundamentales del trabajador Novedades del Proyecto de Ley Orgánica de protección de datos y derechos digitales

CARLOS GONZÁLEZ GONZÁLEZ

Magistrado de Juzgado de lo Social

Sumario

I. Introducción.-

Si en el control empresarial de los medios informáticos y tecnológicos la jurisprudencia había venido estableciendo criterios consolidados sobre los requisitos del acceso y las condiciones que permiten utilizar los datos obtenidos como prueba válida a los efectos de acreditar los incumplimientos laborales –ahora afectados por la doctrina "Barbulescu II"-, 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 TC que no siempre han sido bien recibidos por la doctrina científica y por los interlocutores sociales, dando lugar a pronunciamientos sorprendentes en muchos casos.

La dificultad para encontrar un criterio pacífico se explica en parte por que el TC y el TS habían construido la mayoría de sus criterios examinando la incidencia de la videovigilancia en los derechos fundamentales a la intimidad y a la propia imagen. Pero cuando se invoca la vulneración del derecho a la protección de datos en los casos de video vigilancia[1] el conflicto

[1] Como normativa básica sobre video vigilancia hay que citar **la LO 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos**, completada por el RD 596/1999, de 16 de Abril. Como referencia es conveniente destacar los principios de utilización de las videocámaras, que concreta el art. 6 de la Ley en los siguientes: 1. La utilización de videocámaras estará presidida por el **principio de proporcionalidad, en su doble versión de idoneidad y de intervención mínima;** 2. La idoneidad determina que **sólo podrá emplearse la videocámara cuando resulte adecuado, en una situación concreta, para el mantenimiento de la seguridad** ciudadana, de conformidad con lo dispuesto en esta Ley; 3. La **intervención mínima exige la ponderación, en cada caso, entre la finalidad pretendida y la posible afectación por la utilización de la videocámara al derecho al honor, a la propia imagen y a la intimidad de las personas**; 4. **La utilización de videocámaras exigirá la existencia de un razonable riesgo para la seguridad ciudadana, en el caso de las fijas, o de un peligro concreto, en el caso de las móviles;** 5. No se podrán utilizar videocámaras para tomar imágenes ni sonidos del interior de las viviendas, ni de sus vestíbulos, salvo consentimiento del titular o autorización judicial, ni de los lugares incluidos en el artículo 1 de esta Ley cuando se afecte de forma directa y grave a la intimidad de las personas, así como **tampoco para grabar conversaciones de naturaleza estrictamente privada**. **Las imágenes y sonidos obtenidos accidentalmente en estos casos deberán ser destruidas inmediatamente**, por quien tenga la responsabilidad de su custodia. En materia de investigación de delitos vid. las previsiones del Art. 588 quinquies, letra a, de la LECrim. **En el ámbito de la seguridad privada es de aplicación el Art. 42 de la Ley 5/2014, de 4 de abril, de Seguridad Privada, que concreta que los fines de esta medida** son los de «**evitar daños a las personas o bienes objeto**

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 que sea realmente eficaz el derecho de autodeterminación informativa inherente al derecho a la protección de datos.

Veamos con detenimiento la evolución de la doctrina del TC, distinguiendo la previa a las STC 29/2013 y 39/2016, de 3 de marzo, y la que resulta de estas últimas. Luego el impacto de la STEDH *"López Ribalda"* de 9 de enero de 2018 y la **prohibición de la videovigilancia encubierta.** Posteriormente, conviene insistir en el **deber informativo** como requisito imprescindible para la validez de las grabaciones audiovisuales y analizar la **incidencia en esta materia del Reglamento 2016/679** del Parlamento Europeo y del Consejo, del 27 de abril de 2016. También parece interesante examinar cómo es **la regulación de la videovigilancia en el proyecto de la ley orgánica de protección de datos y derechos digitales**, y hacer referencia a la videovigilancia en las relaciones laborales realizada a través de **detectives privados.** Por último, concluiremos con una referencia a otras **alternativas** que debiera tener en cuenta la empresa en esta materia.

II. La doctrina del TC hasta las SSTC 29/2013 y 39/2016

Es conveniente recordar la previa doctrina del TC sobre el uso empresarial de los instrumentos de video vigilancia para controlar cómo se desarrolla la actividad de los trabajadores[2].

---

de protección o impedir accesos no autorizados», y exige que los servicios se presten por vigilantes de seguridad o, en su caso, por guardas rurales. Aclara que los **servicios de videovigilancia consisten en el ejercicio de la vigilancia a través de sistemas de cámaras o videocámaras, fijas o móviles,** capaces de captar y grabar imágenes y sonidos, incluido cualquier medio técnico o sistema que permita los mismos tratamientos que éstas. Completa esta regulación la Instrucción 1/2006, de 8 de noviembre, de la AEPD, sobre tratamiento de datos personales con fines de vigilancia a través de cámaras o videocámaras. Y la guía de video vigilancia editada por la AEPD.

[2] Vid. GONZALEZ GONZALEZ, C: Control empresarial de la actividad laboral, video vigilancia y deber informativo. A propósito de la STC de 3 de marzo de 2016. Revista Aranzadi Doctrinal núm. 5/2016. BIB 2016/21165. Thomson Reuters, Pamplona, 2016.

Las **STC 98/2000**, de 10 de abril[3] y la **186/2000**, de 10 de julio[4], 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[5]. 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 de la colisión que pueda producirse entre los medios de control utilizados por la empleadora 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.

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 que incidan en el derecho fundamental sólo puede derivar bien del hecho de que la propia

---

[3] RTC 2000/98.

[4] RTC 2000/186.

[5] RTC 2013/29.

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 aquél.

iii. Necesidad de preservar el necesario 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. Y 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 y afectantes, en razonable aplicación del **principio de proporcionalidad**.

En el caso **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 trabajadores y 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. 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 ha quedado acreditado que la instalación del sistema de captación y grabación de sonidos sea indispensable para la seguridad y buen funcionamiento del casino**. Concluye 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 art. 20.3 LET y supone una intromisión ilegítima en el derecho a la intimidad** (art. 18.1 CE).

La segunda Sentencia a tener en cuenta -**STC 186/2000**[6]- 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 su 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 en sus manos. El resultado de la vigilancia realizada en diferentes fechas de abril y mayo de 1995 determinó el despido 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**.

[6] Sentencia dictada por la Sala Primera del TC, compuesta por don Pedro Cruz Villalón, Presidente, don Manuel Jiménez de Parga y Cabrera, don Pablo García Manzano, don Fernando Garrido Falla -ponente- y doña María Emilia Casas Baamonde.

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** y considera que en el caso se respetó por la empresa el derecho fundamental del trabajador y que las pruebas videográficas eran válidas.

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**[7].

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

[7] SSTC 57/1994, FJ 6, y 143/1994, FJ 6.

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**)[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[9],[10]y [11].

---

[8] 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.

[9] En el recurso de amparo el trabajador alegaba que la implantación del sistema de seguridad debía hacerse con publicidad y no con procedimientos ocultos, y exigía la previa comunicación al Comité de empresa y a los trabajadores (art. 64.1.3 d) ET). En cambio para la STC 186/2000 *«El hecho de que la instalación del circuito cerrado de televisión no fuera previamente puesta en conocimiento del Comité de empresa y de los trabajadores afectados (sin duda por el justificado temor de la empresa de que el conocimiento de la existencia del sistema de filmación frustraría la finalidad apetecida)* ***carece de trascendencia desde la perspectiva constitucional****, pues, fuese o no exigible el informe previo del Comité de empresa a la luz del art. 64.1.3 d) LET, estaríamos en todo caso ante una* ***cuestión de mera legalidad ordinaria****, ajena por completo al objeto del recurso de amparo».* Añade que además la cuestión fue resuelta de forma negativa por los órganos jurisdiccionales con criterio que no cabe tildar de arbitrario o irrazonable.

[10] Téngase presente que el art. 65.4 f) del ET prevé que el Comité de empresa tendrá derecho a emitir informe, con carácter previo a la ejecución por parte del empresario de las decisiones adoptadas por éste, sobre diversas cuestiones y, entre ellas, **la implantación y revisión de sistemas de organización y control del trabajo**. Y el Informe de la **Agencia Española de protección de Datos** 0006/2009, con referencia a la Instrucción 1/2006, de 8 de noviembre, de la AEPD sobre el tratamiento de datos personales con fines de videovigilancia a través de sistemas de cámaras o videocámaras, también **considera necesaria la previa información a los trabajadores**, aunque no constituya requisito la prestación de su consentimiento conforme a la excepción prevista para las relaciones laborales en el art. 6.2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. En el mismo sentido de exigir el deber informativo a la empresa en la revisión de las cuentas de correo electrónico facilitadas al trabajador puede consultarse

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**.

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

---

el Informe 0582/2009 de la AEPD, y sobre la colocación de un sistema de localización por GPS en la flota de vehículos de la empresa se pronuncia igual el Informe 193/2008 de la AEPD.

[11] 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.-; y en el mismo sentido las SSTS 26/09/2007 -RJ 2007, 7514-, 08/03/2011 -RJ 2011,932-). No obstante, en la **STS 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 exigía informar a los trabajadores de la existencia de control empresarial y los 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. Y en el mismo sentido la **STC 170/2013**, de 7 de octubre -RTC 2013,170- para supuesto de convenio colectivo que tipifica como infracción los usos extra laborales de las herramientas informáticas al considerar 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.

y a la propia imagen consagrados en el art. 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.

III. Videovigilancia y protección de datos en la doctrina de las STC 29/2013 y 39/2016.-

Como vemos en los caso 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[12], 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 como prueba** del comportamiento del trabajador las grabaciones. Hay que tener en cuenta, como hemos advertido con anterioridad, que el TC hasta entonces había establecido los principios en esta materia sobre la base de la colisión de las facultades de control con el derecho a la intimidad de los trabajadores, sin ninguna referencia al derecho de autodeterminación informativa que consagra art. 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[13] en donde se veía como el trabajador firmaba a unas determinadas horas, aunque entraba al establecimiento a otras horas[14]. Consta también en el relato de los hechos que el **Convenio Colectivo aplicable preveía** la posibilidad de **que el empresario efectuase control sobre los medios informáticos y audiovisuales.** El **Comité de Empresa había sido informado** sobre la

[12] Dictada por la Sala Primera del TC, compuesta por don Pascual Sala Sánchez, Presidente, don Manuel Aragón Reyes, doña Adela Asua Batarrita, don Andrés Ollero Tassara, don Fernando Valdés Dal-Ré -ponente-, y don Juan José González Rivas.

[13] Quedó acreditado que la Universidad de Sevilla La Universidad de Sevilla tenía concedida autorización administrativa de la Agencia Española de Protección de Datos para, entre otros fines, el control de acceso de las personas de la comunidad universitaria y del personal de empresas externas a sus campus y centros. En virtud de dicha autorización tenía instaladas varias cámaras de vídeo-grabación en los accesos al recinto del centro, con la debida señalización y advertencia públicas.

[14] 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.

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 la finalidad** 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 art. 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[15]. 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[16], 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 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**,

[15] **Declara la nulidad de las sanciones** porque habiéndose acordado con base en una lesión del art. 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.

[16] 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 art. 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»***.

dado que es complemento indispensable del derecho fundamental del art. 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[17].

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[18].

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

---

[17] Previamente destaca la STC 29/2013 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 art. 18.1 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.

[18] Para la STC 29/2013 tampoco podría situarse el fundamento en la 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 glosada 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) 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 art. 18.4 CE la utilización para llevarlo a cabo 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.
- 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.

Sin embargo, esta doctrina del TC va a ser modificada de forma sorpresiva 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[19]. La Sentencia cuenta con dos Votos particulares, formulados por los magistrados don Fernando Valdés Dal-Ré[20] y don Juan Antonio Xiol Ríos.

[19] Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras. En su art. 3 dispone que «Los responsables que cuenten con sistemas de videovigilancia deberán cumplir con el deber de información previsto en el artículo 5 de La Ley Orgánica 15/1999, de 13 de diciembre. A tal fin deberán: a) Colocar, en las zonas videovigiladas, al menos un distintivo informativo ubicado en lugar suficientemente visible, tanto en espacios abiertos como cerrados y b) Tener a disposición de los/las interesados/as impresos en los que se detalle la información prevista en el artículo 5.1 de la Ley Orgánica 15/1999». El contenido y el diseño del distintivo informativo se debe ajustar a lo previsto en el Anexo de la Instrucción, según el cual, el distintivo deberá incluir una referencia a la Ley Orgánica 15/1999, de protección de datos, una mención a la finalidad para la se tratan los datos ("Zona videovigilada") y una mención expresa a la identificación del responsable ante quien puedan ejercitarse los derechos a los que se refieren los arts. 15 y siguientes de la Ley Orgánica 15/1999.

[20] Al que se adhiere la Magistrada doña Adela Asua Batarrita.

Parece evidente que el Pleno del TC **ha cambiado la doctrina de la STC 29/2013**. Sin embargo, **resulta sorprendente** que no se mencione ese trascendente cambio, a pesar que la recurrente en amparo fundada gran parte de su recurso precisamente en el deber informativo al trabajador que resulta del art. 18.4 CE, tal y como había sido interpretado por la sentencia citada[21].

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.

[21] El VP del magistrado don Fernando Valdés Dal-Ré llama la atención sobre la **mutación constitucional** derivada de la STC de 3 de marzo de 2016 sobre el contenido esencial del derecho que reconoce el art. 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 art. 18.4 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».*

- **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.
- 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 art. 18.4 CE. 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 de 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 arts. 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 art. 18.4 CE.

Por su parte el Fiscal informó que no apreciaba la vulneración del art. 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 art. 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.

En todo caso 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[22].

iii. Aunque el **consentimiento del afectado** es el elemento definidor del sistema de protección de datos de carácter personal, **la propia LOPD 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[23].

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**. 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

[22] Sigue en esto de forma expresa a lo declarado por la STC 292/2000, de 30 de noviembre, FJ 7.

[23] El art. 6.1 LOPD prevé que «el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa». El propio art. 6 LOPD, en su apartado 2, enumera una serie de supuestos en los que resulta posible el tratar y ceder datos sin recabar el consentimiento del afectado; en concreto, «no será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias; **cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento**; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado».

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 art. 20.3 TRLET.

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 arts. 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 art. 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**[24].

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 allá de 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

[24] Cita aquí expresamente a las SSTC 186/2000, de 10 de julio, FJ 6, y 98/2000, de 10 de abril, FJ 8.

dinero); **idónea** para la finalidad pretendida por la empresa (verificar si algunos de los trabajadores cometía efectivamente las irregularidades sospechadas y en tal caso adoptar las medidas disciplinarias correspondientes); **necesaria** (ya que la grabación serviría de prueba de tales irregularidades); y **equilibrada** (pues la grabación de imágenes se limitó a la zona de la caja), por lo que debe descartarse que se haya producido lesión alguna del derecho a la intimidad personal consagrado en el art. 18.1 CE.

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[25] -que también exige con rigor el cumplimiento del deber de información previo a los trabajadores para admitir como prueba del comportamiento del trabajador las grabaciones-. 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 art. 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.

[25] RJ 2014, 3307. Resuelve la STS 13-5-2014 un supuesto de utilización de las cámaras de video-vigilancia instaladas como sistema disuasorio de hurtos de clientes, para sancionar a una trabajadora de supermercado que dejaba de escanear productos en la caja en beneficio de su pareja. El TS, recepciona la doctrina de la STC 29/2013, y considera vulnerado el derecho a la protección de datos de carácter personal (art. 18.4 CE) por la falta de información a los trabajadores sobre la utilidad de supervisión laboral asociada a las capturas de imágenes. Añade que no es óbice a la conclusión que obtiene el que existieran dispositivos anunciando la instalación y la captación de imágenes o la notificación de la creación de ficheros a la AEPD. Aclara, por último, que el caso es distinto al que resuelve desde la perspectiva del derecho a la intimidad la STC 186/2000 (instalación puntual y temporal de una cámara tras acreditadas razonables sospechas de incumplimientos contractuales que se emplea con la exclusiva finalidad de verificación de tales hechos).

En definitiva, la doctrina de la STC 39/2016 **devalúa el contenido esencial 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 TC 292/2000, de 30 de noviembre, y la STC 29/2013. Como hemos indicado en otras ocasiones[26], tal vez fuese oportuno 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[27].

IV. 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, 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.

La STEDH del caso **"*López Ribalda y otras v. España*"[28], de 9 de enero de 2018**[29], declara la vulneración del Art. 8 del CEDH por parte del

[26] Véase González González, C: *«Control empresarial de la actividad laboral y uso de las nuevas tecnologías»*. Revista Aranzadi Doctrinal núm. 11/2015. BIB 2015\17296.

[27] Como hace 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.

[28] TEDH 2008,1.

[29] En la STEDH de 9-01-2018, caso "López Ribalda", los hechos afectan a cinco demandantes que trabajaban como cajeros en una **cadena de supermercados familiar**. Ante la constatación en 2009 de **desajustes** entre las ventas que diariamente hacían y el inventario de un supermercado, **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

Estado español en la **utilización de sistemas de video vigilancia encubierta** conforme a estas conclusiones:

1. **La videovigilancia encubierta de un empleado/a 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 él/ella no puede evitar al estar obligado/a por el contrato de trabajo a desempeñar su trabajo en dicho lugar (véase *Köpke*).
2. 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.**
3. 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.**

---

cámaras, pero **no de las segundas** que controlaban directamente a los trabajadores que trabajaban en las cajas de los supermercados. Y tampoco informó a la RT. Detectado por el servicio de videovigilancia instalado 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 virtud del cual ellos se comprometieron a no recurrir el despido decidido por el empresario 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 se habían suscrito libre y voluntariamente. El TEDH acumula los asuntos y dicta la sentencia comentada.

4. 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 *Bărbulescu).***
5. **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.**
6. 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**.
7. 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 la finalidad 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".
8. 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.**
9. 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.**

10. **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 estuvo limitada 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.

11. 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 importante atender a la **vinculación que los Jueces y Tribunales españoles tienen respecto a la doctrina del Tribunal Europeo de Derechos Humanos.** El art. 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".**

La vinculación a la jurisprudencia del TEDH llega hasta el punto de que **cabe revisar una sentencia española firme** que haya vulnerado DF conforme a lo declarado por el TEDH. El actual **art. 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 **art. 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".**

V. El deber informativo requisito imprescindible para la validez de las grabaciones audiovisuales. Incidencia del Reglamento 2016/679 del Parlamento Europeo y del Consejo, del 27 de abril de 2016.-

En mi opinión, la STEDH comentada **es una llamada de atención respecto de la doctrina del TC y del TS sobre el limitado alcance del deber informativo en materia de video vigilancia**, imponiendo el **carácter absoluto del deber informativo** vinculado a la garantía propias del derecho

a la protección de datos en los términos previstos en el Art. 5 de la Ley 15/1999, y actualmente en los artículo 12 y 13 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.

Nuestros tribunales deberán volver al origen de su doctrina - que en nuestro caso vendría a ser la que recoge la STC 29/2013[30]- y exigir en el control empresarial un deber informativo previo, concreto y preciso, que incluya la finalidad del sistema implantado[31], sin degradarlo con menciones a las reglas prohibitivas generales que existan en las empresas o a la mera colación del cartel informativo[32]. Al menos

[30] Recordemos que la STC 186/2000 –caso de circuito cerrado de televisión que capta cómo el cajero de un economato de Ensidesa sustrae dinero de la caja, siendo despedido- declaró que 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**, **pero advirtiendo que así era al menos como exigencia derivada del contenido esencial de los derechos a la intimidad y a la propia imagen, únicos invocado en amparo.** En consecuencia, **no resolvió el recurso de amparo teniendo en cuenta las exigencias del derecho de protección de datos personales** (Art. 18.4), que fue a lo que atendió la STC 29/2013 al fijar al doctrina constitucional en materia de video vigilancia en las relaciones laborales.

[31] **La 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 lo previsto en la normativa en materia de protección de datos de carácter personal, y **especialmente a los principios de proporcionalidad, idoneidad e intervención mínima.**

[32] No está de más **llamar la atención sobre las importantes diferencias entre el alcance del deber informativo que se aprecia en la STC 29/2013 en el caso "Universidad de Sevilla", y la STC 39/2016 -de Pleno- en el caso "Bershka".** Por mucho que se afirme lo contrario de forma insistente, lo cierto es **que el deber informativo es mucho más exigente en la doctrina de la primera sentencia citada del TC que en la**

mientras nuestra legislación regule el derecho de autodeterminación informática con el alcance actual[33] y [34].

---

segunda, que dulcifica la exigencia, que queda cumplida con la colocación del cartel informativo correspondiente, sin necesidad de informar a los trabajadores sobre la concreta finalidad de la medida de video vigilancia implantada. **Declara la STC 29/2013 que es 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»*, 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».*** En cambio, la STC 39/2016 **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. **Entiende que 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 art. 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.**

[33] Desde esa perspectiva específica de la protección de datos resuelve el conflicto la **STC 29/2013**. 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. Consta también en el relato de los hechos que el **Convenio Colectivo aplicable preveía** la posibilidad **de que el empresario efectuase control** sobre los medios informáticos y audiovisuales. 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 la finalidad para la que podían ser recabados esos datos personales derivados de las grabaciones. Esta circunstancia es la que determinó que se considerase que la prueba del comportamiento del trabajador mediante el uso de las imágenes de las cámaras de seguridad era nula, afectando así a la propia calificación de nulidad de las sanciones impuestas por la Universidad de Sevilla.

No parece, por otra parte, que puedan desvincularse los pronunciamientos de los casos "Barbulescu II" y "López Ribalda" porque, aunque el primero se refiera al secreto de comunicaciones a través de "Yahoo Messenger" y el segundo a la video vigilancia encubierta, **en ambos casos se razona con fundamento en el mismo derecho consagrado en el art. 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 y a la protección de datos de los datos personales.**

La idea a tener en cuenta es que si la ley reconoce unos determinados derechos vinculados a la protección de datos de carácter personal, **necesariamente deberá respetarse el deber informativo previo que permita tener cabal conocimiento de quién tiene mis datos personales y para qué se utilizan**. Sólo así podrá el trabajador manifestar su consentimiento o solicitar la rectificación, cancelación o supresión de los datos.

Por otra parte, no cabe desconocer que la doctrina del TC y del TS 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. Como sabemos la norma europea es

---

[34] **Un caso curioso resuelve la STSJ Andalucía/Sevilla 22-3-2017** (AS 2017,1052) que excluye la vulneración del derecho a la intimidad del trabajador por considerar que el deber informativo debe ceder ante intereses prevalentes. **En concreto considera válida la colocación por la empresa de cámaras de videovigilancia en un cuarto de baño utilizado por las auxiliares para bañar a los residentes gravemente discapacitados, sin conocimiento ni consentimiento de residentes, ni de los familiares de éstos, ni de los trabajadores del centro , y ante la sospecha de malos tratos a éstos, considerando que la medida era razonable y proporcionada.** La cámara grabó constante o ininterrumpidamente durante un período de tiempo no determinado. En dichas grabaciones la empresa apreció que el demandante se encontraba en el cuarto de baño con una auxiliar y un residente **al que reiteradamente estimuló tocándole** con su mano en el brazo, incidiendo su dedo en el abdomen, en alguna ocasión dirigiendo el dedo hacia la zona de los ojos, y en varias ocasiones pellizcándole o retorciéndole el meñique hasta lograr que el propio residente comenzara a bajarse los pantalones y ropa interior.

de directa aplicación (art. 288 TFUE). Al ser un Reglamento de la Unión Europea es predicable de él dos concretos efectos jurídicos:

- **Aplicación directa**, tanto en las relaciones verticales como en las horizontales, constituyendo una norma jurídica perfectamente invocable ante los Tribunales de Justicia.
- **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.

Pues bien, el RGPD establece unos principios y unas exigencias en el derecho a la protección de 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 **cabe considerar que la información a la que se accede en el control empresarial de los medios tecnológicos e informáticos constituye, cabalmente, un "*dato personal*" y tal actividad es, 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**. Y como sabemos entre tales exigencias se encuentran la **transparencia en el tratamiento y el deber informativo previo** a realizar tal actividad.

El art. 4 del RGPD define los **«datos personales»** como **toda información 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 ahora 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) 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 **sin que se prevea excepción alguna aplicable en 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 la misma como consecuencia obligada de lo que impone el RGPD al regular el deber informativo.**

La anterior conclusión es relevante tenerla en cuenta al analizar el proyecto de la ley orgánica de protección de datos personales y 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 deber informativo 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 circunscrita al establecimiento de garantías adicionales, nunca a 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 art. 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 ámbito laboral**, en particular a efectos de contratación de personal, ejecución del contrato laboral, incluido el cumplimiento de las obligaciones establecidas por la ley o por el convenio colectivo, gestión, planificación y organización del trabajo, igualdad y diversidad en el lugar de trabajo, salud y seguridad en el trabajo, protección de los bienes de empleados o clientes, así como 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 específica **no deja una libertad absoluta** regulatoria,

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 s**istemas 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 del proyecto actualmente en tramitación en el Congreso, especialmente al regular la videovigilancia en las relaciones laborales.

e) La regulación de la video vigilancia en el proyecto de la ley orgánica de protección de datos y derechos digitales

Teniendo en cuenta los límites señalados cabe analizar las previsiones del proyecto de la ley de protección de datos. Por primera vez se regula el control de la actividad de los trabajadores cuando colisiona con el derecho a la intimidad y el derecho 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 el lugar 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.**

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 esta ley orgánica (art. 22.8 del proyecto).**

Dada la novedad de esta regulación, no está de más transcribir cómo queda redactado el art. 89 del proyecto de ley:

*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 de esta medida****.*

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

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 destacamos las siguientes:

1. ¿Cuáles son los límites inherentes al ejercicio de las funciones de control empresarial?
2. ¿Informar "*acerca de esta medida"* qué significación y alcance tiene?
3. ¿Debe concretarse la finalidad o finalidades por la que se establece la medida de control? ¿Incluyendo la finalidad sancionadora si se graban incumplimientos laborales?

4. ¿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?
5. ¿Si es necesario la información previa quedan absolutamente prohibidas las grabaciones encubiertas?
6. ¿Qué debe entenderse como acto ilícito?
7. ¿Qué razón determinó que de la redacción inicial –***captación de un delito***- se haya pasado a la referencia al **acto ilícito**?
8. 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?
9. Si la respuesta anterior es afirmativa, ¿para qué se exige la información "previa, clara, precisa y concisa" acerca de la medida de videovigilancia si en todo caso tendrá valor probatorio aunque se omitan tales exigencias informativas?
10. ¿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?
11. ¿Esta regulación respeta las exigencias del deber informativo que impone el Reglamento europeo de protección de datos personales?
12. Si no se ajusta a la regulación del RGPD ¿qué debe hacer el juez español?
13. ¿Es obligatorio que el juez plantee una cuestión prejudicial o puede simplemente inaplicar la norma nacional y extraer las consecuencias jurídicas que resultan de las exigencias y garantías de dicho reglamento?

Voy a aventurar 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 auque se pueden y deben introducirse matizaciones según el medio de control utilizado por la empresa, sin embargo, **en los aspectos nucleares la doctrina del TEDH descansa sobre unos mismo mimbres conceptuales** vinculados al concepto amplio de privacidad y tiene 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, en la navegación por internet o en los datos obtenidos de los ordenadores o medios tecnológicos en general, **se acceda a información que constituyen datos personales** conforme a la definición del art. 4 del Reglamento europeo de protección de datos, y con ello son aplicables sus garantías y exigencias. Entre ellas, por lo que interesa en esta materia, el cumplimiento del deber informativo. Precisamente por ello, además de la doctrina del TEDH, necesariamente habrá que tener en cuenta las disposiciones de dicho 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 razona que se vulneraba el art. 8 del Convenio de Roma porque la grabación encubierta supone desconocer el derecho que incumbe al trabajador a ser informado antes del tratamiento de sus datos conforme a lo previsto en la LOPD española (otorgando relevancia a la regulación del derecho a la vida privada que haya configurado la propia 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**.

Tampoco hay que perder de vista que tanto el derecho a la privacidad como el derecho a la protección de datos personales tiene consagración en

los **art. 7 y 8 de la Carta europea de derechos fundamentales**[35], cuyo **valor jurídico es el propio del derecho originario** de la Unión Europea, y cuyos preceptos deben ser aplicados e interpretados, cabalmente, conforme a la doctrina del TEDH.

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** (art. 52.1 de la Carta). En segundo lugar, que en la medida en que la Carta contenga 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 preguntas anteriores, siguiendo el mismo orden:

1. Los **límites inherentes al control empresarial** a través de este medio son, lisa y llanamente, el **necesario respeto de los derechos fundamentales** del trabajador y significadamente los

[35] El art. 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**». Y el art. 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).

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 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 sancionar incumplimientos laborales. La norma no excepciona ningún supuesto que legitime la intervención sin cumplir la exigencia informativa.

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 exoneran 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.

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 a la referencia al **acto ilícito**. La redacción actual es consecuencia de una enmienda del PP, pero por desgracia en la justificación de la enmienda no se ofrecen argumentos que sirvan al intérprete para orientarle para dar una respuesta más segura.

8. En la mente del legislador parece que cabe entender que cuando 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 si el proyecto de ley ve la luz **no estará 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**. Este 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 de la unión europea originario (Carta) y el derecho derivado con 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.

Para finalizar esta cuestión cabe señalar que indudablemente era mucho más clara la **propuesta del grupo socialista** 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**».

VI. La especialidad de la vigilancia de los detectives privados en el ámbito de las relaciones laborales.-

Las grabaciones pueden ser realizadas también por **detectives privados**, **debiendo sujetarse a principios y exigencias parecidas a las expuestas.**

La Ley 5/2014, de Seguridad Privada, regula los **servicios de investigación privada**, que consisten en la realización de las averiguaciones que resulten necesarias para la **obtención y aportación**, por cuenta de terceros legitimados, **de información y pruebas sobre conductas o hechos privados** relacionados con los siguientes aspectos:

a) Los relativos **al ámbito** económico, **laboral**, mercantil, financiero y, en general, a la vida personal, familiar o social, exceptuada la que se desarrolle en los domicilios o lugares reservados;

b) La obtención de información tendente a garantizar el normal desarrollo de las actividades que tengan lugar en ferias, hoteles, exposiciones, espectáculos, certámenes, convenciones, grandes superficies comerciales, locales públicos de gran concurrencia o ámbitos análogos;

c) La realización de averiguaciones y la obtención de información y pruebas relativas a delitos sólo perseguibles a instancia de parte por encargo de los sujetos legitimados en el proceso penal (Art. 48.1).

En todo caso queda prohibido investigar la vida íntima de las personas que transcurra en sus domicilios u otros lugares reservados[36], **ni podrán utilizarse en este tipo de servicios medios personales, materiales o técnicos de tal forma que atenten contra el derecho al honor, a la intimidad personal o familiar o a la propia imagen o al secreto de las comunicaciones o a la protección de datos** (Art. 48.3).

En orden a las exigencias de los medios empleados en las labores de investigación, dispone la Ley que los servicios de investigación privada se

[36] Es interesante la STS -Penal- 20-4-2016 (RJ 2016,1691), que considera se vulnera el derecho a la inviolabilidad del domicilio con la observación por los agentes de policía del interior de la vivienda, situada en el décimo piso, desde un inmueble próximo, valiéndose para ello de unos prismáticos, dando lugar a la absolución de los condenados por tráfico de drogas porque no existía prueba de cargo válida. Tras señalar que el Art. 588 *quater a)* de la LECrim somete a autorización judicial la utilización de dispositivos electrónicos orientados a la grabación de imágenes o de las comunicaciones orales directas entre ciudadanos que estén siendo investigados, ya se encuentren aquéllos en un recinto domiciliario, ya en un lugar público, señala «que es cierto que no se contempla de forma específica el empleo de prismáticos. Éstos no permiten la grabación de imágenes. Sin embargo, la intromisión en la intimidad domiciliaria puede encerrar similar intensidad cuando se aportan al proceso penal las imágenes grabadas o cuando uno o varios agentes testifican narrando lo que pudieron observar, valiéndose de anteojos, en el comedor del domicilio vigilado. En el presente caso, además, se da la circunstancia de que no concurría ninguno de los supuestos de legitimación de la injerencia a que se refiere el art. 18.2 de la CE. No medió autorización judicial. Tampoco existió consentimiento del morador, expreso o implícito, ni por actos concluyentes. Y ello pese al esfuerzo argumental de los Jueces de instancia para derivar esa autorización del hecho de no haber corrido las cortinas del salón principal de la vivienda (…). Ya hemos dicho que la protección constitucional frente a la incursión en un domicilio debe abarcar, ahora más que nunca, tanto la entrada física del intruso como la intromisión virtual. La revolución tecnológica ofrece sofisticados instrumentos de intrusión que obligan a una interpretación funcional del art. 18.2 de la CE. La existencia de *drones*, cuya tripulación a distancia permite una ilimitada capacidad de intromisión en recintos domiciliarios abiertos es sólo uno de los múltiples ejemplos imaginables».

ejecutarán con respeto a los **principios de razonabilidad, necesidad, idoneidad y proporcionalidad** (Art. 48.6 de la Ley 5/2014)[37].

Hasta ahora se han admitido con cierta normalidad las investigaciones de los detectives privados y la utilización de medios de grabación de imágenes y sonido, incluido en el ámbito de las relaciones laborales y para finalidades de control de las actividades de los trabajadores que pudieran implicar incumplimientos de las obligaciones laborales.

Ahora bien la propia ley exige respetar en la utilización de los medios de investigación los derechos fundamentales, incluyendo el derecho a la intimidad y el de protección de datos personales. Y desde esta exigencia no puede perderse de vista que el detective tiene la condición de responsable del tratamiento de datos personales y, por ello mismo, queda sujeto a las obligaciones que establece el RGPD. Lo que adquiere una especial transcendencia al determinar cómo debe cumplir el deber informativo respeto del interesado -aquí el trabajador investigado-, teniendo en cuenta que dicho deber comprende la expresa información de la finalidad del tratamiento de los datos personales.

El título que legitima la intervención del detective ni siquiera es la ley, como ocurre con nuestra LOPD de 1999, ya que ahora el RGPD se refiere a la legitimación del responsable cuando el tratamiento sea necesario para

[37] La actuación del detective privado da lugar a la elaboración de informes de investigación. Impone la ley que dichos informes deberán conservarse archivados, al menos, durante tres años, sin perjuicio de lo dispuesto en el artículo 16.3 de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. **Además las imágenes y los sonidos grabados durante las investigaciones se destruirán tres años después de su finalización, salvo que estén relacionadas con un procedimiento judicial, una investigación policial o un procedimiento sancionador**. En todo caso, **el tratamiento de dichas imágenes y sonidos deberá observar lo establecido en la normativa sobre protección de datos de carácter personal**, especialmente sobre el bloqueo de datos previsto en la misma (Art. 49.4 de la Ley 5/2014, de Seguridad Privada). Por último, dispone la normativa reguladora que las investigaciones privadas tendrán carácter reservado y los datos obtenidos a través de las mismas solo se podrán poner a disposición del cliente o, en su caso, de los órganos judiciales y policiales, en este último supuesto únicamente para una investigación policial o para un procedimiento sancionador (Art. 49.5).

cumplir una obligación legal, que evidentemente aquí no existe en la medida que ninguna ley impone al detective la obligación de utilizar medios de video vigilancia. Por eso el título habrá que fundarlo en su caso en la existencia de un interés legítimo (art. del RGPD). Pero al margen del título legitimador, a nadie se le escapa que si el detective como responsable debe informar al trabajador previamente o al mismo tiempo que obtiene el dato personal de la finalidad de la captación de su imagen la videovigilancia resultará totalmente ineficaz.

Debe tenerse en cuenta también que en realidad nada impone que la investigación de hechos y conductas privadas tengan que documentarse con fotografías o vídeos que capten la imagen del trabajador. El detective podrá realizar sus funciones de seguimiento e investigación y declarar en el juicio sobre los hechos y conductas que haya observado. De hecho la naturaleza de esta prueba de detectives es la testifical, no la documental ni pericial según la doctrina judicial. En este sentido, el que nos hayamos acostumbrado a admitir como prueba las grabaciones que haya realizado un detective no quiere decir que no quepa replantearse su eficacia desde la perspectiva de las garantías y exigencias derivadas de los derechos fundamentales en juego.

Los arts. 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 a las relaciones laborales ni al detective privado, por lo que si 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 videovigilancia, difícilmente no será aplicable la misma exigencia al detective.

Aclarar que a estos efectos no nos sirve atender a los plazos que cuenta el responsable del tratamiento para cumplir el deber informativo con el interesado, distinguiendo a estos efectos la LOPD 15/1999 según los datos se hayan solicitado del propio interesado (“deberán ser informados previamente de (…) la finalidad”) o no proceden del interesado (“cuando no hayan sido recabados del interesado, éste deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o su

representante, dentro de los tres meses siguientes al momento del registro de los datos"). No parece que estos plazos sirvan para salvar las contradicciones destacadas porque en definitiva esta regulación ya estaba presente cuando el TEDH impuso el deber informativo previo de la finalidad de la videovigilancia en la sentencia López Ribalda.

Bien pudiera pensarse que le TEDH no tuvo en cuenta estas distinciones de la ley española, y sin más razonamiento aplicó a la video vigilancia de la empresa la exigencia del deber informativo previo –incluida la finalidad del tratamiento-, sin caer en la cuenta que ese sistema no implica obtener el dato personal del propio interesado, y con ello al menos habría un plazo de tres meses para cumplir con la obligación.

Sea como sea, actualmente **el RGPD distingue** en los artículos 13 y 14 **estos supuestos:**

a) Información que deberá facilitarse cuando los datos personales se obtengan del interesado.

En este caso informará el responsable al interesado en el momento en que se obtengan los datos. Incluyendo la finalidad del tratamiento.

b) Información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado.

Para este supuesto la información al interesado de la finalidad del tratamiento debe realizarse "dentro de un plazo razonable, una vez obtenidos los datos personales, **y a más tardar dentro de un mes,** habida cuenta de las circunstancias específicas en las que se traten dichos datos.

Pero añade que **si está previsto comunicarlos los datos a otro destinatario**, debe cumplirse el deber informativo a más tardar en el momento en que los datos personales sean comunicados por primera vez (en nuestro caso sería en el momento en que se entreguen a la empresa que contrató los servicios del detective).

Si consideramos aplicable esta regulación a la intervención del detective –con cierta dificultad hay que reconocer, al menos si nos atenemos a la doctrina del TEDH que no parte de estas disquisiciones para imponer el deber informativo con carácter previo a la obtención de las imágenes-, cabría tener por salvada la dificultad señalada. Ahora bien, la validez de la prueba de videovigilancia siempre quedará condicionada a que se cumpla el

deber informativo de la finalidad y demás circunstancias en los plazos previstos en el art. 14 del RGPD.

Por otra parte, cuanto se lleva dicho queda circunscrito, única y exclusivamente, a supuestos de sistemas de vigilancia fuera del lugar de trabajo. Porque en el centro o lugar de trabajo, conforme a la doctrina del TEDH, y si se aprueba conforme a las previsiones del proyecto de la ley orgánica de protección de datos, el empresario sólo puede establecer estas medidas de control de la actividad laboral cumpliendo el deber informativo previo sobre el alcance y naturaleza de los medios empleados. Y parece lógico concluir que estas exigencias son de obligado respeto al margen de que el sistema de video vigilancia lo disponga el empresario o lo encargue a un investigador privado. Pro lo tanto, aunque sea éste el que disponga los medios técnicos subsiste la obligación de informar con carácter previo de todas las circunstancias que impone la norma. Lo que excluye, en definitiva la validez de las grabaciones ocultas o encubiertas, que es tanto como decir las no informadas. Otro entendimiento permitiría burlar con suma facilidad las garantías que constituyen contenido esencial del derecho a la protección de datos. Y, sobre todo, no se aprecian razones para considerar que lo que no puede realizar o incumplir el empresario en el lugar de trabajo sí quede admitido cuando interviene un detective privado.

Avala esta conclusión una última razón relacionada con la regulación del proyecto de la ley orgánica de protección de datos. En efecto, si llega a aprobarse, hay que tener en cuenta que en su art. 22 dispone que el tratamiento de datos por parte de los detectives privados se rige por la Ley de Seguridad Privada (art. 22.7), y a continuación 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 esta ley orgánica. Con lo que parece que quiere significar que en el lugar de trabajo (que es lo que regula el art. 89 del proyecto) sólo cabe establecer estos sistemas de vigilancia conforme a las propias exigencias y requisitos que la norma establece.

VII. Otras alternativas que debiera tener en cuenta la empresa.-

Teniendo en cuenta las circunstancias expuestas, parece evidente que **las empresas tendrán que replantearse las estrategias de control de la**

actividad laboral a través de los medios tecnológicos e informáticos, incluyendo los sistemas de videovigilancia.

Es necesario, por supuesto, la elaboración de protocolos específicos sobra la implementación de los instrumentos de control empresarial de la actividad laboral de los trabajadores, revisar las políticas de uso respecto de los que ya instalados, y proporcionar siempre una **exhaustiva información a los trabajadores en los términos exigidos por la sentencia Barbulescu II y "López Ribalda"[38].**

Lo anterior impone un examen concreto del juicio de proporcionalidad. **Sólo informando previamente a los trabajadores, de forma completa y clara, del control empresarial, incluyendo los medios empleados y la finalidad de la vigilancia, a la par que superando el juicio de**

[38] **Un caso curioso resuelve la reciente STSJ Castilla 25/2018 de 12 Ene. 2018,** Rec. 1416/2017, **declarando Improcedente despido de un vigilante de seguridad que fumaba, veía material pornográfico y se masturbaba en la caseta, porque, aunque no era necesario que se le hubiera avisado previamente que se iba a instalar una cámara de video vigilancia en la caseta, cuando ya existen carteles en el centro de trabajo indicando que es zona videovigilada, sin embargo, la medida no era necesaria ni proporcionada.** Razona que conforme a la STC 39/2016 «el hecho de que el actor no fuera informado previamente de forma alguna por la empresa de su intención de instalar una cámara de video vigilancia en la caseta en la que prestaba sus servicios, ante la sospecha de que estaba cometiendo irregularidades laborales, **existiendo avisos y advertencias de la presencia de cámaras de video vigilancia en el interior del recinto empresarial, pero no en el interior de la caseta, no vulneraría, en principio, el derecho del trabajador a la protección de datos».** Pero destaca que, aunque la medida estaba justificada, **no era necesaria para acreditar que el trabajador fumaba**, que fue la razón inicial por la que se instaló. **La empresa podía probar este hecho con las declaraciones de otros trabajadores y del gerente**, así como también por la desinfección que tuvo que hacer en otra ocasión anterior para higienizar la caseta. Por lo demás, declara que el despido es improcedente y no nulo porque el empresario utilizó este medio para comprobar una actitud impropia del trabajador. Sostiene que «lo que no se ha admitido es el medio de prueba contaminado (...) pero no se ha concluido que la decisión extintiva, en sí mismo considerada, pretendiera la vulneración de un derecho fundamental o libertad pública del trabajador, que llevara aparejada la calificación de nulidad del mismo (Art. 55.5 ET)», citando como precedentes las STSJ Castilla-La Mancha (Sec.1ª) 10 junio 2014 -AS 2014/1619 -; en igual sentido STSJ Castilla-La Mancha (Sec. 2ª) 28 noviembre 2014 - AS 2015/484-).

proporcionalidad, la prueba obtenida por la empresa será considerada válida[39].

Por otra parte, es importante destacar que **la tendencia del derecho de la UE y a nivel internacional en materia de protección de datos y control empresarial es poner la atención, más que en aplicar el régimen sancionador, en la implementación de medidas preventivas de carácter técnico que impidan a los trabajadores usos no autorizados de los medios tecnológicos e informáticos para fines extralaborales** (como suprimir páginas web o de navegación, los accesos a puertos USB y similares).

Por último, debe llamarse la atención sobre el hecho de que muchas de las dificultades expuestas se evitarían si los convenios previesen expresamente como infracciones laborales graves o muy graves de los

[39] También puede servir de parámetro para enjuiciar la validez de los sistemas de vigilancia encubiertos en el ámbito laboral atender a la **doctrina del TC contraria a la posibilidad de utilizar en reportajes cámaras ocultas, y ello a pesar de estar en juego la libertad informativa.** Si la doctrina constitucional prohíbe este medio de investigación periodística, **parece que con mayor razón debemos considerar excepcional medidas de control empresarial de la actividad laboral mediante cámaras ocultas en el que no está en juego un derecho fundamental, sino sólo la libertad de empresa** (Art. 38 CE). En este sentido **la STC 12/2012 de 30 enero** acota el alcance del recurso, señalando que lo que se cuestiona no es el contenido estricto de la información obtenida, sino cómo se ha recogido y registrado mediante videograbación subrepticia, y el lugar donde se ha llevado a cabo, el reducto reservado de una consulta profesional. Todo ello con referencia a un supuesto de reportaje periodístico realizado a través de «cámara oculta», obteniendo el periodista que se hace pasar por cliente imágenes y las declaraciones del esteticista en su consulta profesional. Partiendo de que la relación se desarrolla en un ámbito estrictamente privado, concluye el TC que la captación está basada en un ardid o engaño y no hay consentimiento expreso, válido y eficaz del afectado, por lo que se utiliza una técnica periodística ilegítima, vulnerándose la ética periodística en cuanto a la solvencia y objetividad del contenido informativo, siendo la captación realizada muy intrusiva y el método utilizado innecesario e inadecuado para el objetivo de la averiguación**. Lo mismo se reitera en la STC 74/2012** (para un supuesto de obtención de imágenes en consulta de parapsicología por parte de dos periodistas que se hacen pasar por clientes con la finalidad de hacer pública y denunciar la existencia de prácticas supuestamente fraudulentas: método utilizado innecesario e inadecuado para el objetivo de la averiguación).

trabajadores el acceso o la utilización con fines extralaborales de los medios tecnológicos o informativos puestos a su disposición por la empresa. En estos casos podría ejercitarse la facultad disciplinaria acreditando la conducta del trabajador con los medios técnicos que permiten verificar esos incumplimientos en los accesos y usos de los medios tecnológicos e informáticos (alertas y similares medidas de carácter técnico), sin necesidad de llegar a realizar conductas de control empresarial intrusivas en los derechos fundamentales de los trabajadores.