Sentencia dictada por el Juzgado de lo Social Tres de Pamplona de fecha 18 de febrero de 2019 en el procedimiento de despido nº 875/2018.

Resumen de alguno de los fundamentos de derecho.

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

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

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

No parece, por otra parte, que puedan desvincularse los pronunciamientos de los casos "Barbulescu II" -STEDH de 5-09-2017, Bărbulescu contra Rumanía- **y "López Ribalda"** porque, aunque el primero se refiera al secreto de las comunicaciones

y a la intimidad en mensajes enviados por un trabajador a través del sistema *"Yahoo Messenger"* y el segundo a la video vigilancia encubierta, **en ambos casos se razona con fundamento en el mismo derecho, el consagrado en el artículo 8 de Convenio europeo de derechos humanos, a saber, el derecho a la vida privada**, **con su contenido complejo que comprende el derecho a la intimidad, al secreto de la correspondencia, a la inviolabilidad domiciliaria y a la protección de datos de los datos personales.**

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

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

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

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

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

b) **Prevalencia o primacía de la jurisprudencia comunitaria sobre la doctrina o jurisprudencia de los tribunales de los países miembros en la interpretación o aplicación de los preceptos y disposiciones del Derecho de la Unión Europea**, porque de conformidad con lo que establece el artículo 267 del TFUE la doctrina establecida por el TJUE, al resolver cuestiones prejudiciales, **es vinculante para el juez español. También para el Tribunal Supremo y ha de acatarla** (como recuerda la STS 23-03-2015, en rcud 2057/14 (RJ 2015, 1250), y declararon las STJCE 14-12-1982, asunto Waterkeyn; 5-03.1996, asuntos Brasserie du pêcheur y Factortame, C-46/93 y C-48/93). **Hoy consagra la vinculación del juez español a la jurisprudencia comunitaria el Art. 4 bis de la LOPJ.**

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

Pues bien, **el RGPD establece unos principios y unas exigencias aplicables para garantizar la tutela del derecho a la protección de los datos personales que no cabe desconocer en el enjuiciamiento de la validez de los distintos medios de control empresarial de la actividad de los trabajadores**. A la vista de la concepción amplísima de las nociones de *dato personal* y *tratamiento* que se contiene en el RGPD difícilmente puede considerarse **que la información a la que se accede en el control empresarial de los medios tecnológicos e informáticos que utilizan los trabajadores**

no constituya, cabalmente, un «*dato personal*» y que tal actividad sea, al mismo tiempo, «*tratamiento*». De la misma forma que la imagen -sistemas de videovigilancia- constituye un dato personal, también lo es la información a la que se accede cuando se controla la navegación por Internet, los ordenadores y los correos electrónicos La consecuencia jurídica no es otra que **extender al control empresarial de los medios tecnológicos las mismas exigencias que el Reglamento europeo -sin excepción alguna aplicable a las relaciones laborales-, impone al tratamiento de los datos personales**. Como sabemos, entre dichas exigencias se encuentra la **transparencia en el tratamiento y el deber informativo previo** a realizar la actividad.

El artículo 4 del RGPD define los **«datos personales»** como **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 se **debe cumplir a través de capas o niveles, el básico y el adicional. Además de la información por capas,** se establece una lista exhaustiva de la información que debe proporcionarse a los interesados (más amplia que la que reflejada en la LOPD de 1999) y que comprende: la información sobre el responsable

del tratamiento; **la finalidad del tratamiento**; la legitimación o título que legitima el tratamiento; los destinatarios de las cesiones o transferencias de los datos; los derechos de las personas; los datos del Delegado de Protección de Datos y la procedencia o fuente de los datos.

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

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

La anterior conclusión es relevante tenerla en cuenta al analizar el contenido de la reciente **Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales**, en la medida que ahora contiene una regulación expresa de las medidas de control empresarial que afectan al derecho fundamental a la intimidad de los trabajadores y al derecho a la protección de datos. Como la norma española **sólo puede complementar el reglamento europeo en aquello que este permite, y sin contradecir en ningún caso la regulación esencial del propio reglamento** –aplicable de forma directa y con eficaz primacía frente a las normas nacionales-, cabe concluir sin dificultad que **en ningún caso la ley española puede rebajar las exigencia del 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 o más específicas, 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 artículo 88 del RGPD dispone que los Estados miembros podrán, **a través de disposiciones legislativas o de convenios colectivos,** establecer **normas más específicas** para **garantizar** la protección de los derechos y libertades en relación con el **tratamiento de datos personales de los trabajadores en el 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 nacional específica **no deja una libertad regulatoria absoluta**, sino que dispone que dichas normas incluirán medidas adecuadas y específicas para **preservar** la **dignidad** humana de los interesados, así como sus intereses legítimos **y sus derechos fundamentales, prestando especial** atención a la **transparencia** del tratamiento, a la transferencia de los datos personales dentro de un grupo empresarial o una unión de empresas dedicadas a una actividad económica conjunta y a los **sistemas de supervisión en el lugar de trabajo.**

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

de protección de datos personales y garantía de los derechos digitales. Especialmente al regular la videovigilancia en las relaciones laborales.

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

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

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

Regula de forma expresa el **derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en 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. Tampoco proporciona la exposición de motivos explicación alguna sobre las razones por las que no se menciona el derecho que consagra el artículo 18.4 de la CE.

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

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

1. *«Los empleadores **podrán tratar las imágenes** obtenidas a través de sistemas de cámaras o videocámaras para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respectivamente, en el artículo*

20.3 del Estatuto de los Trabajadores y en la legislación de función pública, ***siempre que*** *estas funciones se ejerzan* ***dentro de su marco legal y con los límites inherentes al mismo****.*

Los empleadores ***habrán de informar con carácter previo****, y de forma* ***expresa, clara y concisa****, a los trabajadores o los empleados públicos y, en su caso, a sus representantes,* ***acerca 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, determinar los límites inherentes al ejercicio de las funciones de control empresarial, o qué significación y alcance tiene la referencia del legislador al deber de informar al trabajador "*acerca de esta medida"*. Pueden existir dudas sobre si es exigencia legal concretar la finalidad o finalidades para las que se establecen las medidas de control empresarial, y si incluye la finalidad sancionadora para el caso de que se graben incumplimientos laborales. Tampoco aclara la ley si la información previa va referida a una antelación general desde que se adopta la medida o a una antelación específica si la videovigilancia se concreta en uno o varios trabajadores, o si

quedan absolutamente prohibidas las grabaciones encubiertas. **Queda indeterminado o no definido el concepto de acto ilícito**, y no se expresan las razones que justificaron que de la redacción inicial del proyecto de ley del Gobierno –que se refería a la ***captación de un delito***- se haya pasado en la redacción final del precepto a la referencia a la captación por las cámaras de vigilancia de la comisión fragante de un ***acto ilícito*** a los efectos de exigir sólo para cumplir las exigencias de protección del derecho y la validez de la prueba que el empresario hubiera colocado el cartel informativo sobre zona videovigilada. Parece a primera vista que el hecho de que se entienda cumplido el deber informativo con el dispositivo *"zona videovigilada"* cuando se capta un acto ilícito significa que la prueba es válida y se puede sancionar al trabajador. Pero entonces, **¿para qué se exige la información *«previa, expresa, clara y concisa» acerca de la medida* de videovigilancia si en todo caso tendrá valor probatorio aunque se omitan tales exigencias informativas?**

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

Cabe dar una respuesta jurídica a estas cuestiones tomando como fundamento la doctrina del TEDH en las Sentencias «Barbulescu II» y «López Ribalda» y las exigencias derivadas del reglamento europeo de protección de datos. Es importante destacar que esta doctrina no puede entenderse de forma separada, considerando que la primera sólo es aplicable al control de las comunicaciones del trabajador -"Yahoo Messenger" en el caso- y la segunda sólo a la videovigilancia. En realidad **ambas se construyen sobre la base del derecho a la privacidad** que consagra el artículo 8 del Convenio de Roma, que comprende el derecho a la protección de los datos personales, de manera que aunque se deba introducir matizaciones según el medio de control utilizado por la empresa, sin embargo, **en los aspectos esenciales la doctrina del TEDH descansa sobre unos mismo mimbres conceptuales** vinculados al concepto amplio de privacidad, y por ello presenta un efecto de irradiación que no cabe desconocer. Tampoco puede sorprender esta estrecha relación si se tiene en cuenta que en el control de las comunicaciones, de los correos electrónicos, de la navegación por Internet o de los datos obtenidos de los ordenadores y demás medios tecnológicos en

general, **se acceda a información que constituye dato personal** conforme a la definición del artículo 4 del Reglamento europeo de protección de datos, y con ello deben ser aplicables sus garantías y exigencias. Entre ellas, por lo que ahora interesa destacar, el cumplimiento del deber informativo. Precisamente por ello, **además de la doctrina del TEDH, necesariamente habrá que tener en cuenta las disposiciones del reglamento y el conjunto de principios y exigencias que establece dada su eficacia directa y la primacía sobre las normas de los Estados miembros**.

Se hace mención a la anterior cuestión porque si hasta ahora el TEDH en la sentencia López Ribalda razonó la vulneración del artículo 8 del Convenio de Roma porque la grabación encubierta suponía desconocer el derecho que incumbe al trabajador a ser informado antes del tratamiento de sus datos conforme a lo previsto en la LOPD española de 1999 (otorgando relevancia a la regulación del derecho a la vida privada tal y como se hubiera configurado en la legislación nacional), **actualmente la normativa directamente aplicable no es otra que el reglamento europeo** -desde el 25 de mayo de 2018-, **sin que la norma española pueda contradecir sus mandatos esenciales, entre los que se encuentra, sin duda alguna, el preceptivo deber informativo y las exigencias de transparencia del tratamiento**, **no exceptuadas para las relaciones laborales cuando el empleador utiliza medidas de control de la actividad laboral**.

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

Tampoco hay que perder de vista que tanto el derecho a la privacidad como el derecho a la protección de datos personales tienen consagración en los **artículos 7 y 8**

de la Carta europea de derechos fundamentales, cuyo **valor jurídico es el propio del derecho originario** de la Unión Europea, y sus preceptos deben ser aplicados e interpretados conforme a la doctrina del TEDH.

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

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

Hay dos aspectos especialmente relevantes que deben tenerse en cuenta en la aplicación e interpretación de los derechos que reconoce la Carta. En primer lugar, que **cualquier limitación** del ejercicio de los derechos y libertades que reconoce **deberá ser establecida por la ley** y respetar el **contenido esencial** de dichos derechos y libertades. Además, dentro del respeto del principio de proporcionalidad, **sólo podrán introducirse limitaciones cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás** (garantía de reserva de ley, respecto del contenido esencial y necesidad de la limitación que consagra el artículo 52.1 de la Carta). En segundo lugar, que en la medida en que la Carta consagra derechos

que correspondan a derechos garantizados por el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, **su sentido y alcance serán iguales a los que les confiere dicho Convenio** (Art. 52.3 de la Carta). Y lógicamente ese alcance lo determina el **Tribunal Europeo de Derechos Humanos**.

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

1. Los **límites inherentes al control empresarial** a través de la videovigilancia son, lisa y llanamente, el **necesario respeto de los derechos fundamentales** del trabajador y significadamente los derechos a la intimidad, a la imagen y a la protección de datos personales. Ese respeto conlleva que debe aplicarse la doctrina conocida sobre incidencia de las funciones de vigilancia empresarial en los derechos fundamentales, que **sólo pueden ser objeto de limitaciones en la medida estrictamente necesaria para satisfacer un derecho o un interés legítimo del empleador.** Por lo mismo, la medida de control **sólo es válida si supera el juicio de proporcionalidad** (idoneidad, necesidad y proporcionalidad).
2. Informar **acerca del alcance de la medida** no puede entenderse sino como expresa **información de la finalidad** del sistema instalado.
3. Por eso, **sí que debe concretarse por el empleador que incluye la finalidad sancionadora** si se captan incumplimientos laborales de los trabajadores.
4. En la medida que este modo de controlar la actividad de los trabajadores incide especialmente en su derecho a la protección de datos -la imagen es un dato personal-, cabe entender que **el momento en que debe suministrarse la información sobre la finalidad es precisamente cuando se instalan las cámaras**, y también cada vez que se contrate a un trabajador. Lógicamente**, si la empresa no tenía instalado este sistema, y lo dispone a raíz de sospechas de irregularidades** de algún o algunos trabajadores, **es ese momento cuando deberá informarles** que se instalan las cámaras y que su finalidad incluye el sancionar los incumplimientos laborales. La norma europea no excepciona ningún supuesto que legitime la

intervención sin cumplir la exigencia informativa y la doctrina del TEDH tampoco.

5. Efectivamente, dado que existe un deber de informar previamente al trabajador de la instalación de las cámaras de vigilancia, ya no serán posibles y **quedan absolutamente prohibidas las grabaciones encubiertas u ocultas, que es tanto como decir no informadas**. Las **sospechas de irregularidades** graves en el desempeño de la actividad laboral **no legitiman una excepción** del deber de informar de la grabación que afecta al puesto objeto de sospecha, **ni exonera de cumplir las exigencias del RGPD.** La empresa siempre dispone de un medio de defensa de sus intereses, como es el anuncio de la grabación de las imágenes y de la finalidad, que ofrece ya una protección sobre su patrimonio por la función disuasoria que razonablemente debe producir.
6. Por **acto ilícito** sólo cabe entender lo que la propia expresión indica: **cualquier acto que contraría el ordenamiento es un acto ilícito.** Es ilícito el acto que constituye delito. También lo es el que constituya una infracción administrativa. Y, por último, los incumplimientos de las obligaciones laborales quedan incluidos en esa noción.
7. No podemos conocer la razón que determinó que de la redacción inicial –***captación de un delito***- se haya pasado en el informe de la ponencia del proyecto de la ley orgánica y en el texto definitivo a hacer mención al *"**acto ilícito"***. La redacción actual es consecuencia de una enmienda que, por desgracia, en su justificación no ofreció argumentos que sirvan al intérprete para orientarle y poder dar una respuesta más segura sobre el alcance de la expresión.
8. En la mente del legislador español parece estar presente el criterio de que en el supuesto de que las cámaras de vigilancia captan actos ilícitos fragantes la prueba obtenida es válida, aunque no se haya cumplido con las exigencias del deber informativo y sólo figure el dispositivo ***"zona videovigilada".*** Ello supondría que el trabajador a quien se refiera la grabación y que realizó el acto ilícito podrá ser sancionado. **Supone volver a la doctrina restrictiva de la STC 39/2016, claramente superada por la STEDH "*López Ribalda*".**

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

10. Lo que si podemos concluir es que **excluir la exigencia informativa de la finalidad de la videovigilancia,** que forma parte del contenido esencial del derecho fundamental a la protección de datos personales, supone que la LO 3/2018 **no está respetando el derecho a la privacidad y a la protección de datos personales conforme a la doctrina del TEDH**.

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

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

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

plantear la cuestión prejudicial, lo que constituye una obligación si contra la sentencia del tribunal no cabe recurso.

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

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

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

CE la utilización para llevarlo a cabo de medios encubiertos que niegan al trabajador la información exigible» (STC 29/2013).

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

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

C) Aplicación de las exigencias anteriores al caso enjuiciado

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

utilizaba, **incluyendo la posibilidad de sancionar si captan actos ilícitos o incumplimientos laborales**.

Hay que destacar que los hechos que han dado lugar al despido disciplinario del trabajador son anteriores a la entrada en vigor de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Y, **desde esta perspectiva temporal, ni siquiera la nueva regulación es aplicable al caso enjuiciado a pesar de la alegación realizada en el acto del juicio por la empresa demandada**. Y **tampoco se estima aplicable la doctrina que cita** de la STC 39/2016 porque **en los términos razonados lo cierto es que el deber informativo sobre el alcance de las medidas de videovigilancia, incluyendo la finalidad sancionadora, es una exigencia que se impone en todo caso, más allá de la mera colocación del cartel informativo, conforme a la jurisprudencia del Tribunal Europeo de Derechos Humanos y el propio Reglamento General de Protección de Datos** a que se ha hecho referencia, que obligan a su aplicación y a interpretar la propia normativa nacional en los términos que exige el TEDH y que se derivan del Reglamento Europeo, dotado de eficacia directa y primacía frente a la norma nacional que contradiga su contenido, teniendo en cuenta que **en dicho reglamento no se establece excepción alguna al deber de transparencia e informativo en materia de protección de datos aplicable a las relaciones laborales**.