El efecto Ribalda II en la admisión de prueba de videovigilancia en un despido disciplinario.

Pilar Rivas Vallejo
Catedrática de Derecho del Trabajo y de la Seguridad Social. Universidad de Barcelona

Resumen: *A partir de la doctrina europea y constitucional, el Tribunal Supremo considera que no es necesario informar a los trabajadores afectados por seguimiento a través de cámaras de videovigilancia de su finalidad disciplinaria si ya conocen su existencia previamente. Se reitera la doctrina sentada en sentencia de 7 de julio de 2016 y posteriores y se aplica a un supuesto de subcontratación del servicio de vigilancia.*

Palabras clave: *Videovigilancia. Consentimiento informado. Cesión de datos. Tratamiento de datos.*

Abstract: *On an European and constitutional doctrinal basis, the Supreme Court decides that the workers affected by monitoring through video surveillance cameras don't need to be informed of their disciplinary purpose if they already know of its existence previously. Application of doctrine established in judgement of July 7, 2016 to outsourced security service.*

Keywords: *The Ribalda's efect: admission of video surveillance evidence to support disciplinary dismissal.*

I. Introducción

La doctrina sentada en la STC 39/2016, como en la STDH de 17 de octubre de 2019 (*López Ribalda II*), implica considerar prueba válida para acreditar el incumplimiento laboral las imágenes obtenidas de cámaras de videovigilancia, si el trabajador afectado conocía su existencia, sin precisar información sobre la finalidad concreta de su instalación.

II. Identificación de la resolución judicial comentada

Tipo de resolución judicial: sentencia**.**

Órgano judicial: Tribunal Supremo, Sala Social.

Número de resolución judicial y fecha: sentencia núm. 817/2021, de 21 de julio.

Tipo y número recurso o procedimiento: RCUD núm. 4877/2018.

ECLI: ECLI:ES:TS:2021:3115

Fuente: CENDOJ.

Ponente: Excmo. Sr. D. Ignacio García-Perrote Escartín.

Votos Particulares: carece.

III. Problema suscitado. Hechos y antecedentes

1. La cuestión central: validez de imágenes captadas por cámaras de videovigilancia como prueba a efectos de acreditar un despido disciplinario

El problema que se suscita en la sentencia comentada es

la validez de imágenes obtenidas de cámaras de videovigilancia para acreditar el incumplimiento del trabajador objeto de la vigilancia cuando esta no se dispuso a tal fin, sino con fines de seguridad privada y pública por empresa principal que contrató la vigilancia de seguridad. A tenor de la doctrina constitucional y del TEDH, no es necesario precisar la finalidad de la presencia de la cámara (obvia si se vigila un recinto público por una empresa de seguridad) si el trabajador observado conoce su existencia y la captación y registro de imágenes, aunque de ellas se derive un posterior uso con fines laborales.

2. Los hechos

El demandante, vigilante de seguridad para la empresa de seguridad Securitas Seguridad España S.A. en el acceso principal de vehículos del recinto ferial K1 del cliente Ifema, fue objeto de despido disciplinario al amparo del art. 54.2.d) ET por trasgresión de la buena fe contractual, fraude, abuso de confianza y deslealtad, como consecuencia del incumplimiento de su deber de realizar de las requisas de vehículos (controles de seguridad aleatorios de vehículo en accesos al recinto y a los estacionamiento públicos) y su declaración como efectuadas en sus partes o registros diarios entregados a la empresa, es decir, por falsear tales partes e incumplir su prestación laboral durante el periodo de quince días del mes de febrero de 2017. El incumplimiento se contextualiza en la remisión por Ifema a la empleadora y de esta a sus trabajadores de instrucciones implantadas a partir del incremento del nivel de alerta de amenaza terrorista (desde enero de 2015, reforzado en abril de 2016, y acompañado de un curso al actor sobre el funcionamiento de la nueva operativa y de aviso de la Policía Nacional en diciembre de 2016 de la necesidad de mantener el nivel de alerta), y los hechos imputados se constatan a través del visionado de las imágenes registradas por las cámaras de seguridad del recinto en el periodo aludido, que demuestran idénticas conductas en varios trabajadores, lo que motiva también la rescisión de la contrata de seguridad con Securitas (la no renovación del contrato vigente a su término).

El demandante firmó posteriormente (14 de marzo) autorización a la entidad ferial citada para la cesión de sus datos personales almacenados en el fichero de su responsabilidad, relativo a la videovigilancia a la empleadora, así como a esta, para incorporar dichas imágenes a su fichero de recurso humanos, en ambos casos con el fin de verificar el correcto cumplimiento de sus obligaciones laborales y bajo régimen de consentimiento informado. Y meses después del despido, acontecido el 21 de abril, en noviembre de 2017, solicitó su cancelación.

Tanto la sentencia de instancia (del Juzgado de lo Social núm. 40 de Madrid, de 12 de diciembre de 2017, autos 659/2017) como la que resuelve el recurso de suplicación por el Tribunal Superior de Justicia de Madrid (núm. 828/2018, de 28 de septiembre, rec. 275/2018) mantienen la improcedencia del despido. La base de esta decisión tiene carácter procesal, al inadmitirse la prueba de videovigilancia aportada por la empresa para justificar el despido, por aplicación de la sentencia del Tribunal Europeo de Derechos Humanos de 5 de septiembre de 2017 (Barbulescu II), ya que en ambos casos se entendió que la obtención de la prueba se había realizado con violación de los derechos fundamentales (en concreto, el derecho a la intimidad y vida personal reconocido en el art. 8 del CEDH) y, por tanto, no acreditándose la conducta imputada, el despido debía considerarse improcedente.

IV. Posición de las partes

La recurrente sostiene la validez de la captación de imágenes para probar el incumplimiento laboral que motivó el despido disciplinario, mientras que el demandante se ampara en la doctrina constitucional previa a la STC 39/2016, que exige que el trabajador tenga conocimiento cabal y exhaustivo, no solo de la existencia de cámaras de videovigilancia, sino también de su propósito, criterio que acogen tanto la sentencia de instancia como la de suplicación objeto del recurso.

V. Normativa aplicable al caso

Son de aplicación al caso el art.54.4 del convenio colectivo estatal de empresas de seguridad y el art. 54.2.d) ET.

VI. Doctrina básica

1. Basta el conocimiento genérico

La sentencia recurrida resuelve la cuestión planteada aplicando la doctrina de la STEDH de 9 de enero de 2018 (López Ribalda I), pues el sistema de videovigilancia que destapó el incumplimiento objeto del despido era conocido por el trabajador, pero su finalidad era la seguridad pública y no el control de la ejecución del trabajo, de lo que no fue informado expresa e inequívocamente. Pero, como pone de manifiesto la sentencia del Tribunal Supremo objeto de comentario, esta doctrina fue superada por la de la STEDH (Gran Sala) 17 octubre 2019 (López Ribalda II), que la deja sin efecto, y que se aplica en la sentencia de contraste, la STS 77/2017, 31 de enero de 2017, Pleno, rcud 3331/2015 (que rebajó las exigencias informativas en el sentido indicado por la STC 39/2016, 3 de marzo), que fue citada en la STS 21/2019, de 15 de enero, y que se aplica ya en la STS 212/2020, 5 de marzo de 2020 (rcud 256/2017). Y de igual modo avala la doctrina constitucional sentada en la STC 39/2016, de 3 de marzo, a tenor de la cual no es necesario concretar la finalidad exacta del control cuando el trabajador es conocedor de la instalación de tal sistema, basado en videovigilancia (a través del distintivo de la instrucción 1/2006 de la Agencia Española de Protección de Datos), doctrina que fue explicitada en la posterior Ley Orgánica Ley Orgánica 3/2018, de Protección de Datos, LOPD (art. 88.1).

En definitiva, concluye la resolución comentada, la sentencia recurrida no se adecúa a la STC 39/2016, 3 de marzo, y, ”aunque en determinadas circunstancias, la STEDH (Gran Sala) de 17 octubre de 2019 (López Ribalda II) admite que la empresa no advierta al trabajador de la existencia ni del emplazamiento de determinadas cámaras de videovigilancia, sin que ello conduzca a la nulidad de la prueba de videovigilancia que sustenta y acredita la sanción al trabajador”, en el caso analizado el demandante sí tenía conocimiento de su existencia y emplazamiento, por lo que el matiz está en que desconocía que las imágenes en ellas captadas pudieran tener una ulterior utilidad práctica, consistente en su empleo para verificar incumplimientos. Pues, en definitiva, apunta la sentencia, el control empresarial amparado por el art. 20.3 ET cubre el tratamiento de datos sin necesidad de autorización, que, por tanto, se entiende implícita en la celebración del contrato de trabajo“; y ello por el "desequilibrio claro" que puede existir entre el interesado y el responsable del tratamiento al que hace referencia el considerando 43 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016” (RGPD), si bien en el presente caso existió autorización expresa para el tratamiento de los datos.

2. Admisión de la prueba: triple juicio de necesidad, adecuación y proporcionalidad

De acuerdo con la doctrina de la STC 39/2016, recogida en la STS 77/2017, de 31 de enero y posteriores, basta con poner en conocimiento de los trabajadores la existencia de la videovigilancia sin necesidad de concretar su finalidad, lo cual es notorio en el caso analizado, dada la actividad desempeñada por el demandante, donde constituye elemento central de su actividad el uso de cámaras de videovigilancia, como se prevé en la Ley 5/2014, de 4 de abril, de Seguridad Privada (LSP), que las exige con carácter preceptivo en determinados recintos o instalaciones

con riesgo evidente, excluidas en caso de acceso a aparcamientos, pero no en la situación examinada, el acceso a un recinto ferial abierto al público. Como argumenta la resolución comentada, “concurrían también intereses públicos de gran importancia derivados del incremento de la amenaza terrorista, intereses que se podían ver seriamente comprometidos por un deficiente control de seguridad en el acceso al recinto ferial”.

Del cumplimiento con los requisitos reseñados (el conocimiento de la existencia de cámaras de videovigilancia -se entiende enfocadas al ámbito de la prestación del trabajo del demandante-) se deriva la validez del uso posterior de las imágenes que se pudieran captar para verificar un posible incumplimiento contractual de este. Por ello, concluye la sentencia, “la prueba de la reproducción de lo grabado por las cámaras de videovigilancia era, así, una medida justificada, idónea, necesaria y proporcionada al fin perseguido, por lo que satisfacía las exigencias de proporcionalidad que imponen la jurisprudencia constitucional y del TEDH”, y, por consiguiente, “debió de [sic] admitirse porque se adecuaba a la doctrina de la STC 39/2016, 3 de marzo de 2016, y de la STS 77/2017, 31 de enero de 2017 (Pleno, rcud 3331/2015), respetaba las exigencias jurisprudenciales de proporcionalidad y era necesaria para poder acreditar la veracidad de los hechos imputados al trabajador”. Tal admisión altera los términos del debate sustantivo ante el tribunal que se devuelven los autos, que deberá valorar la conducta imputada a tenor, también, de la prueba videográfica, pues, como reza el auto del Tribunal Supremo de 18 de septiembre de 2018 (rcud. 1092/2018), "la prueba consistente en reproducción de imágenes y sonidos (videovigilancia) es lícita, siempre que el trabajador conozca la instalación de las cámaras y su ubicación por motivos de seguridad”, habiendo matizado en las SSTS de 7 de julio de 2016 (rcud. 3233/2014) y posteriores que tal información se entiende cumplida sin necesidad de concretar el propósito de la videograbación.

VII. Parte dispositiva

La resolución estima el recurso de casación para la unificación de doctrina, casa y anula la sentencia recurrida y, estimando el recurso de suplicación, revoca la sentencia del juzgado de lo social y anula las actuaciones practicadas desde el acto del juicio para que se celebre uno nuevo en el que se admita y practique la prueba denegada, y donde se dilucide de nuevo si, a tenor de tal prueba, el despido puede considerarse procedente.

VIII. Pasajes decisivos

La resolución sintetiza a modo de título en su fundamento de derecho tercero el fallo de la Sala, literalmente: “la prueba de videovigilancia aportada por la empresa para justificar el despido del trabajador debió admitirse, conforme a la doctrina de la STEDH (Gran Sala) 17 octubre 2019 (López Ribalda II), de la STC 39/2016, 3 marzo 2016 y de la sentencia de contraste, la STS 77/2017, 31 de enero de 2017 (Pleno, rcud 3331/2015)”. Y “debió de [sic] admitirse porque se adecuaba a la doctrina de la STC 39/2016, 3 de marzo de 2016, y de la STS 77/2017, 31 de enero de 2017 (Pleno, rcud 3331/2015), respetaba las exigencias jurisprudenciales de proporcionalidad y era necesaria para poder acreditar la veracidad de los hechos imputados al trabajador” (fundamento de derecho tercero, apartado quinto). (…) “el hecho de que, como igualmente ocurría en el supuesto enjuiciado por el TEDH, la prueba no fuera nula desde la perspectiva de la impugnación judicial de la sanción disciplinaria impuesta al trabajador, no impide que la empresa pueda ser responsable en el ámbito de la legislación de protección de datos” (mismo FD tercero.5).

IX. Comentario

1. Lo que analiza y lo que sólo apunta la sentencia

La sentencia comentada basa su argumentación en la aplicación de la doctrina sentada en la STC 39/2016 como en la llamada sentencia *López Ribalda II* del TEDH (ya citada), que se resume en que no resulta relevante la comunicación del propósito de la videovigilancia, sino su conocimiento por parte de los trabajadores objeto de tal

control videográfico, por lo que reitera la doctrina ya sentada en las SSTS de 7 de julio de 2016 (rcud. 3233/2014), de 31 de enero de 2017 (rcud. 3331/2015), de 1 y de 2 de febrero de 2017 (rcud. 3262/2015 y 554/2016) y de 15 de enero de 2019 (rcud. 341/2017), por aplicación de la doctrina constitucional nacida de la STC 39/2016, y que revisaba la doctrina mantenida en su anterior sentencia de 13 de mayo de 2014 (rcud. 1685/2013), en la que también la instalación de videocámaras obedecía a un propósito ajeno al control de la actividad laboral (control de robos por terceros en cadena de supermercados), en la que se entendió vulnerado el art. 18.4 CE por desviar su uso para fines disciplinarios, pese al conocimiento, por obvio y visible, de la existencia de videocámaras. La citada doctrina no toma en consideración, como sí lo hace la doctrina norteamericana, la necesidad de negociar con la representación legal del personal la instalación y uso de las videocámaras (cfr. sentencia del Tribunal de Apelaciones del Circuito del Distrito de Columbia de los Estados Unidos de Brewers & Maltsters, Local Union # 6, et al. contra Anheuser-Busch, Inc., 5 de julio de 2005, US App. LEXIS 13292 -DC Cir., 2005-), pero, a diferencia de esta (amparada en la sección 10 (c) de la Ley Nacional de Relaciones Laborales), no concede validez *absoluta* a las pruebas videográficas para acreditar conductas tributarias de despido disciplinario, dada la primacía, en el ámbito europeo, de la protección de los datos personales como parte del derecho a la intimidad en el ámbito del trabajo, frente al interés empresarial.

La sentencia europea que inspira la resolución comentada desautoriza la vigilancia encubierta basada en sospecha de incumplimientos laborales, pero admite que la sospecha razonable de la comisión de una falta grave podría constituir la justificación pertinente para amparar tal práctica y que debe ponderarse también la posibilidad de reclamar ante la autoridad nacional de control de protección de datos. De su doctrina la sentencia analizada infiere que tal admisión es posible en supuestos de vigilancia expresa y comunicada, aun cuando el objeto de la información no precise con exactitud la finalidad de tal seguimiento. A título ejemplificativo comparado, en el asunto *Doolin v The Data Protection Commissioner [2020] IEHC 90*, de 21 de febrero de 2020, donde también se interrelaciona la seguridad pública con las finalidades disciplinarias, el Tribunal Superior de Irlanda (tribunal competente en asuntos civiles) opta por una interpretación divergente, entendiendo que, si el material videográfico obtenido de cámaras de videovigilancia se iba a utilizar con fines disciplinarios, tal uso habría de haberse informado al trabajador implicado.

Se omite el análisis de otras cuestiones, por no ser objeto del recurso, reducido a analizar si la prueba de imágenes obtenidas de tal modo resulta válida para acreditar el incumplimiento y por tanto la procedencia del despido, como la forma en que se obtuvo el consentimiento de los trabajadores, o su aplicabilidad al ámbito afectado por la decisión (el de la seguridad privada, donde entran en juego otra serie de consideraciones, de orden público y privado), aunque se apunta a la hipotética vigilancia del trabajo en la empresa principal por parte de la contratista, pero se realizarán algunas consideraciones al respecto seguidamente.

2. Videovigilancia en trabajos de seguridad privada

Un posible error de partida podría viciar la argumentación relativa al uso doble de la videovigilancia tanto por razones de seguridad pública como de orden disciplinario. La sentencia comentada, como la impugnada, reiteran que el demandante “no había sido informado de que la finalidad de dicho sistema, además de para la seguridad del acceso al recinto de Ifema, era para controlar la actividad laboral”, lo que parece partir de la presunción de que el sistema de videovigilancia fue concebido con ese doble propósito, lo cual no ha sido constatado, pues en principio la seguridad pública es la que justifica supervisar cómo se lleva a término el control de accesos. Lógicamente esto compromete a trabajadores en la ejecución de su prestación laboral (así lo entendió la STEDH de 9 de enero de 2018, en el primer asunto López Ribalda, así como la STC29/2013), pero no es esta la finalidad perseguida, sino constatar que se cumplen los parámetros de seguridad exigibles por las razones anteriormente expuestas, relacionadas con el nivel de alerta terrorista presente en aquella fecha. La propia dinámica de un sistema de seguridad implica que las imágenes captadas van a

incluir a las personas que prestan tal servicio, por lo que, como se indica, es un hecho notorio, pero además intrínseco a la propia ejecución de tal servicio, de acuerdo con el art. 22 de la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana, la Ley Orgánica 7/2021, de 26 de mayo, y, en particular, el art. 42.4 LSP, a tenor del cual "las grabaciones realizadas por los sistemas de videovigilancia no podrán destinarse a un uso distinto del de su finalidad". Pese a ello, la sentencia recurrida, que sí alude expresamente a este extremo, entiende que en casos como el analizado la vigilancia de la actividad laboral no es el fin principal buscado, pero indirectamente tiene lugar *como consecuencia* del fin legítimo de control y seguridad. Por consiguiente, que no se trata de un doble propósito, sino de un propósito principal y otro derivado, que constituye consecuencia inevitable del primero, al incluirse entre las imágenes captadas aquellas que afectan a trabajadores en el desempeño de su trabajo. Y es desde esta afectación secundaria desde la que igualmente deben respetarse las salvaguardas indispensables para el respeto de sus derechos fundamentales, consistentes en la información previa, objetivo de la operación, periodo de conservación, derechos de acceso y rectificación, procesado de datos y consulta con la representación de los trabajadores (no se especifica de qué empresa), e incluso con la autoridad supervisora, la AEPD. La resolución casada equipara la captación y tratamiento con la cesión de datos a la empleadora, en este caso con fines exclusivamente disciplinarios.

Lo que está en juego no es esa supervisión, sino que, con efectos laborales, esto es, de control y disciplinarios, esas imágenes fueran objeto de tratamiento y/o de cesión a la empleadora, contra lo previsto en el art. 42.4 LSP, porque en este caso ya no está en lid la seguridad pública o privada, sino el control de la actividad laboral. Ergo lo que podría ser objeto de debate es *esa cesión de imágenes*, que, en el caso enjuiciado, requirió consentimiento informado, concretado en sendas autorizaciones firmadas por el demandante. Son estas las que deben analizarse.

La cesión de tales imágenes, sometida a la LOPD, se inscribe en el control de la ejecución del trabajo, pero se verifica con posterioridad a la conducta supervisada a través de tales imágenes, por tanto, anteriores a la cesión del derecho sobre ellas (extremo relevante para la sentencia objeto de casación). El sistema de videovigilancia no se concibió para el control de su prestación laboral, sino que se da tal uso posterior a las imágenes ya captadas, una vez conocido el presunto incumplimiento grave. Efectivamente podría haberse concebido el sistema con este segundo propósito y en tal caso debería haberse informado cumplidamente de ello a los trabajadores implicados. Este es el argumento de base analizado: que no se les informó de esta segunda finalidad. Aunque, si el sistema de videovigilancia no fue concebido con tal propósito, podría sostenerse, con la recurrente, que no cabía tal información previa, pero lo cierto es que, dada la implicación laboral de la videovigilancia, sí debería preverse un eventual uso extraordinario de las imágenes captadas con esta finalidad, que en este caso se introdujo *a posteriori* y a través de la firma de conformidad del trabajador, si bien concedida para examinar imágenes *anteriores* no sujetas a tal consentimiento informado (y la consiguiente precaución derivada de saberse videovigilado). En realidad, lo que justifica este examen posterior es justamente una de las excepciones doctrinales para amparar este tipo de controles: la verificación de un incumplimiento grave. Pero, de igual modo, esta circunstancia extraordinaria en el contexto analizado debió incluirse en el régimen jurídico aplicable a la subcontratación y explicitarse en supuestos que impliquen a trabajadores de servicios sujetos a videovigilancia de seguridad.

3. Videovigilancia de trabajadores en casos de subcontratación

La resolución examinada apunta a la relación entre empresa principal y contratistas en el tratamiento de datos de los trabajadores. Y, a tal efecto, razona que "el hecho que el sistema de videovigilancia fuera de Ifema y no de Securitas puede ser relevante, sin duda, desde la óptica del cumplimiento de la legislación de protección datos por parte de ambas entidades, pero no debe llevar necesariamente a impedir que Securitas aporte en un juicio laboral unas grabaciones que pueden ser necesarias

para satisfacer la carga de la prueba que sobre ella recae". Y, existiendo ya cámara de videovigilancia en la empresa cliente, argumenta la resolución, "podría ser desproporcionado, desde la perspectiva de los derechos fundamentales de los trabajadores, y hasta impracticable, que Securitas instalara un adicional y paralelo sistema de videovigilancia".

La sentencia recurrida equipara la captación y tratamiento de imágenes con la cesión de datos a un tercero que no es el responsable del tratamiento, la empleadora, en realidad la verdadera clave del problema, ya que en todo momento parece interpretarse, tanto por el Tribunal Superior de Justicia de Madrid como por el Tribunal Supremo, que ambas empresas ocupan una posición idéntica en el tratamiento de los datos frente a los trabajadores. Y lo cierto es que la segunda, la empleadora contratista, es la única cuya intervención responde única y exclusivamente a finalidades disciplinarias, y que sólo la primera es la responsable del tratamiento de datos. Por otra parte, la resolución casada indica que el tratamiento de los datos debiera ser objeto de consulta con la representación legal del personal, pero, en un caso como el presente, no detalla si esta debiera ser la de la empleadora o la de la empresa principal.

La sentencia del Tribunal Supremo introduce también la hipótesis de la videovigilancia directa por la empleadora en las propias instalaciones de la empresa principal, a partir de la instalación directa en ellas de cámaras de videovigilancia, situación de probable régimen de coordinación que no resuelve, pero califica de "impracticable". Con independencia de las razones prácticas aludidas, ello no impediría, por el contrario, proveer a los trabajadores con dispositivos inteligentes que suplieran tal función a través de otras alternativas de seguimiento adecuado al tipo de trabajo y de control que se quisiera ejercer. Y en tal caso habría de plantear la admisibilidad de tal invasión del espacio controlado por la empresa principal, cuestión central en el debate actual sobre el uso de dispositivos inteligentes en entornos laborales, lo que conduciría al examen de los parámetros constitucionales y legales que lo ampararían…o que conducirían a su rechazo. Ya se constató cómo la misma sala, en sentencia de 8 de febrero (núm. 163/2021), consideraba oportuno el seguimiento por geolocalización mientras se realizase con dispositivos titularidad de la empresa si resulta ser práctica habitual del sector (en el caso analizado, el seguimiento del reparto de los pedidos por empresa de comida a domicilio). Sería interesante conocer qué solución se daría a uso dentro de las instalaciones de terceros, incluida la empresa principal, que en esta resolución queda abierta.

4. La vulneración relativa a la protección de datos

La sentencia comentada razona que "la admisión de la prueba denegada no es incompatible con la posible denuncia a la Agencia Española de Protección de Datos por las infracciones que se hubieran podido cometer desde la óptica de la mencionada normativa de protección de datos". Tal afirmación se basa en el registro de las imágenes del demandante por parte de la empresa principal y en su cesión posterior a la empleadora, en ambos casos objeto de consentimiento informado por el trabajador (amparado por el art. 4 RGPD y el art. 6 LOPD), seguramente porque su consentimiento en el contexto de una relación de trabajo puede condicionar su validez, en tanto que su prestación debe realizarse en plena libertad y de manera específica para cada una de las finalidades previstas para el tratamiento de los datos (condición esta última que se acredita cumplida en el presente caso), previa información al trabajador.

Esta necesidad de reforzar las garantías de los trabajadores, en virtud de la relación de desequilibrio que les une a sus empleadoras, exige, pues, respetar escrupulosamente los principios de necesidad y de proporcionalidad, tal y como recoge la

Guía «La protección de datos en las relaciones laborales» de la Agencia Española de Protección de Datos -AEPD- (2021), que indica literalmente que "en el ámbito de las relaciones laborales, la base jurídica principal es la ejecución del contrato de

trabajo, porque el consentimiento del afectado no es válido cuando se proporciona en un contexto de «desequilibro claro entre el interesado y el responsable del tratamiento», la posición de desequilibrio entre la empresa y la persona trabajadora exige extremar las cautelas y, en particular, el respeto a los principios de proporcionalidad y de limitación de la finalidad". Así como restringir la prestación del consentimiento informado con arreglo a tales parámetros y a finalidades exclusivamente laborales (art. 9 LOPD), que excluye su validez cuando el fin del tratamiento sea identificar otros parámetros personales (categorías especiales de datos) y, por tanto, no el mero cumplimiento de sus obligaciones laborales (art. 6.3 LOPD: “no podrá supeditarse la ejecución del contrato a que el afectado consienta el tratamiento de los datos personales para finalidades que no guarden relación con el mantenimiento, desarrollo o control de la relación contractual”). De igual modo, y contra la jurisprudencia constitucional y europea, exige que el contenido del consentimiento *se refiera explícitamente a todas y cada una de las posibles finalidades del tratamiento*, bajo la premisa de que este sea necesario y proporcional, y, finalmente, que la prestación del consentimiento no condicione la ejecución del contrato.

En el caso analizado, se cumplen los parámetros exigidos por el citado precepto en el sentido interpretado: conocer tanto la identidad del responsable del tratamiento como los fines de este, así como el criterio de necesidad y proporcionalidad, pues el consentimiento, emitido antes de proceder al tratamiento de los datos y no con carácter genérico ni condicionante de la prestación laboral, se presta en el contexto de una verificación del cumplimiento de los deberes derivados del contrato de trabajo y ante la situación extraordinaria que conforman los indicios de su incumplimiento.

Obviamente, las anteriores consideraciones se refieren a la cesión de las imágenes captadas del trabajador al amparo del art. 22 LOPD, pues su propia captación estaría a su vez vinculada a las razones de orden público que justifican la instalación de cámaras en los accesos a un recinto público y la intensificación de la vigilancia por razones de seguridad pública (al amparo de autorización pública, ex art. 41.2 c y d de la LSP), en este caso reforzada por la alarma policial ya referida en relación con un alto nivel de amenaza terrorista, que la sentencia recurrida niega que conste acreditada (al contrario, mantiene que el control fue prolongado e indiscriminado, sin causa ni proporcionalidad, por no haberse acreditado los indicios de irregularidades que motivaron el examen de las imágenes). En este segundo escenario, el art. 22.4 LOPD da cobertura al deber informativo exigible, entendiendo equiparable a este “la colocación de un dispositivo informativo en lugar suficientemente visible, identificando, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos en los artículos 15 a 22 del [RGPD]”, lo cual no puede entenderse suficiente en relación con la videovigilancia de trabajadores, que igualmente debería ser informada expresamente por los empleadores, aunque la prestación laboral contratada en este caso podría eximir del cumplimiento de este deber reforzado, si se atiende a que esta se inscribe en la LSP y en las funciones inherentes a la profesión de vigilante de seguridad, a la que remite el art. 22.7 (“lo regulado en el presente artículo se entiende sin perjuicio de lo previsto en la [LSP] y sus disposiciones de desarrollo”).

Por otra parte, de acuerdo con la norma aplicable, las imágenes debieron suprimirse transcurrido el plazo máximo de un mes desde su captación (art. 22.3), lo que no aconteció en este caso, pues al término de tal plazo la empresa principal se acogió a la excepción prevista en el art. 22.3: “cuando hubieran de ser conservados para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones” (se prevé en tal caso un plazo máximo de setenta y dos horas para su puesta a disposición de la autoridad competente), entregando en fecha de 16 de marzo las registradas en los días posteriores al 5 de febrero y hasta el 15 de ese mes, periodo al que se refieren los hipotéticos incumplimientos laborales. Pues, a tenor del art. 42.5 de la LSP, “la monitorización, grabación, tratamiento y registro de imágenes y sonidos por parte de los sistemas de videovigilancia estará sometida 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" (lo cual debe ponerse en relación con la Ley Orgánica 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, por la necesaria coordinación de tal vigilancia derivada del carácter público del recinto, ya que se trata de un consorcio en cuya constitución participan entidades públicas, como la Comunidad y el Ayuntamiento de Madrid, https://www.ifema.es/que-es). Condiciones que, en definitiva, concurren en un recinto de alta densidad de actividad, y a la que acceden más de 700.000 vehículos anuales (Ifema: https://www.youtube.com/watch?v=vOKt_1Ebu00&list=PLZqD2rY3sLykqqChbIV8-xsL_OqZm6FP7&index=15).

X. Apunte final

Es llamativo que, en el año 2018, es decir, después de la rescisión del contrato de prestación del servicio de videovigilancia con la empresa Securitas, Ifema obtuviera un premio a su sistema de seguridad en accesos y videovigilancia (https://diariofinanciero.com/ifema-premiada-por-su-sistema-de-seguridad-en-accesos-y-videovigilancia/) precisamente por sustituir dicha contrata por la asunción del servicio (Unidad de Control de Seguridad y Salud) y su automatización, recientemente mediante un sistema inteligente de Wizzie Data Platform (WDP) de Wizzie Analytics (https://intereconomia.com/noticia/ifema-madrid-intensifica-en-fitur-su-seguridad-con-un-sistema-inteligente-que-ayudara-a-recuperar-las-ferias-presenciales-20210522-2302/). También la empleadora Securitas emplea algoritmos para detectar "patrones anómalos de conducta" (https://www.securitas.es/soluciones_de_seguridad/servicios-digitales/artificial-intelligence-ai/), que pudieran resultar susceptibles de aplicación a sus propios trabajadores.

La empresa principal de este caso utiliza ya módulos de la plataforma para el geoposicionamiento, detección de patrones estanciales y de comportamiento de los asistentes, pero muy probablemente, aunque no se cuenta en los reportajes y noticias alusivas, también a los trabajadores que prestan los diversos servicios que aquella presta. Quizás podamos ver en el futuro en qué medida afecta este sistema basado en inteligencia artificial a los trabajadores de la empresa principal, o posibles contratas, como en el caso analizado, en relación con el tratamiento de datos personales (art. 22 del RGPD). La STEDH *López Ribalda II* no podrá alumbrar ya una respuesta clara a tal problema. Pero lo que sí es claro es que una evaluación de impacto de riesgos evitaría incurrir en vulneración de derechos fundamentales, sin perjuicio de la posibilidad y necesidad de negociar la introducción de estos sistemas de seguimiento y control de la actividad laboral.