VALORACIÓN CRÍTICA SOBRE LA INTERPRETACIÓN DE LA REGULACIÓN SOBRE LOS SISTEMAS DE VIDEOVIGILANCIA DE SEGURIDAD EN EL TRABAJO TRAS LA SENTENCIA DEL TRIBUNAL CONSTITUCIONAL 119/2022, DE 29 DE SEPTIEMBRE

Juan Peña Moncho
Ayudante de Investigación
Instituto de Relaciones Laborales, Universitat Ramón Llull - ESADE

A El Foro,
Por su acogida y por mostrarme su conocimiento

Abstract

El Tribunal Constitucional publicó el 29 de septiembre de 2022 la sentencia núm. 119/2022, legitimando la redacción del segundo párrafo del artículo 89.1 LOPD. De esta forma, entiende que es válido el despido de un trabajador por vender ilegalmente productos de la empresa, teniendo como prueba del incumplimiento unas grabaciones videográficas. La existencia de dichas grabaciones tan solo había sido informada mediante el cartel informativo que exige el artículo 22.4 LOPD, sin que se comunicase al trabajador expresamente ni de la base jurídica ni de la finalidad del tratamiento. En este trabajo se aborda un comentario crítico en relación con dicho pronunciamiento.

The Constitutional Court published on September 29th, 2022, the decision nº 119/2022, confirming the wording of the second paragraph of article 89.1 LOPD. Therefore, the Tribunal asserts that is lawful an employee dismissal because he sold unlawfully goods from the company, using as proof of the infringement video records. The existence of such recording was only informed by the informational sign requested by article 22.4 LOPD, without communicating expressly the employee neither the legal basis nor the purposes for the processing. In this paper, a critical commentary on such decision is made.

Title: Critical commentary on the interpretation of the law on security video surveillance systems at work after the Constitutional Court decision nº 119/2022, of September 29th, 2022.

Palabras clave: cámaras, despido, derecho de información, artículo 89 LOPD.
Keywords: cameras, dismissal, right of information, article 89 LOPD.

IUSLabor 2/2023, ISSN 1699-2938, p. 131-149
DOI. 10.31009/IUSLabor.2023.i02.05

Fecha envío: 16.2.2023 | Fecha aceptación: 11.3.2023 | Fecha publicación: 22.6.2023

Sumario

1. Cuestión conflictiva y recorrido procesal

El Tribunal Constitucional emitió en la segunda mitad del 2022 una sentencia de gran relevancia en materia de videovigilancia y protección de datos, ya que hace una primera interpretación constitucional del segundo párrafo del artículo 89 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPD).

El supuesto de hecho que da pie a esta resolución trata de un empleado que trabaja para unos almacenes de material de hogar. Según se desprende de la carta de despido que se le entrega en junio de 2019, el trabajador vendió varios productos de la empresa valorados en 271´36€ más IVA sin hacer albarán y apropiándose de la cantidad de 250€ pagada en metálico por un cliente. Por ello, se le imputa en la carta de despido un incumplimiento muy grave de la buena fe contractual del artículo 54.2.d) del Estatuto de los Trabajadores (ET) por apropiación indebida "*consciente, deliberada y subrepticia*". Ante tal incumplimiento, la empresa decide sancionarle con el despido.

Según se describe en la carta de despido, la empresa tuvo la oportunidad de conocer estas circunstancias porque la tarde precedente al incumplimiento laboral, el responsable de la tienda vio una bolsa de una empresa de la competencia en el interior del mostrador donde trabajaba el empleado. Se acercó a comprobar su contenido y vio que era un termostato que comercializaba la empleadora. A la tarde siguiente, se comprobó que ni la bolsa ni el objeto estaban en ese lugar. Por ello, según consta en la carta de despido, el responsable de la tienda procedió a visionar las cámaras de vigilancia "*a fin de saber a quién podría pertenecer la bolsa; o quién se la podría haber olvidado*". De esta forma, se detectó la entrega y venta ilegal de los productos al cliente en la mañana del 7 de junio de 2019.

Tal y como consta en los hechos probados de la sentencia de instancia, la empresa contaba con un cartel informativo de videovigilancia en el exterior de su establecimiento. Asimismo, estas cámaras eran visibles en el interior del local. También se prevé en los hechos probados que en el año 2014 se procedió al despido de otro trabajador por hechos similares, haciéndose valer también las cámaras de videovigilancia.

El trabajador impugnó el despido en sede judicial solicitándose la improcedencia del mismo en atención a la ilegalidad de la prueba practicada. El Juzgado de lo Social nº 1 de Vitoria desestimó íntegramente la demanda, considerando como válida la prueba videográfica. Ante esta decisión, el empleado recurre en suplicación ante el Tribunal Superior de Justicia del País Vasco, que resuelve el asunto en su sentencia núm. 1211/2020 de 6 de octubre.

Este Tribunal Superior de Justicia del País Vasco considera que, para proceder a una videograbación legítima, por norma general, el artículo 89.1 LOPD exige que las empresas informen con carácter previo y "*de forma expresa, clara y sencilla a los trabajadores de esta medida*". No obstante, añade que, según dicho precepto, "*(q)ueda a salvo de esta información el supuesto en el que se haya captado la comisión flagrante de un acto ilícito por los trabajadores, en cuyo caso se entiende cumplido el deber de informar cuando existiesen dispositivos colocados de forma que informen suficientemente de la existencia del aparato de cámara, informándose de la identidad del responsable y la posibilidad de ejercitar los derechos sobre ello*". En este sentido, entiende que, pese a que en este supuesto de hecho se podría considerar que aplica la excepción del cartel informativo, por el hecho de que en el año 2014 ya se utilizó por parte de la empresa la videovigilancia para despedir a otro trabajador "*es difícilmente comprensible que en el transcurso de cinco años no haya procedido a regular la situación del control por cámaras, informando adecuadamente a los trabajadores según le exige la normativa.*"

De esta forma, al no cumplir con la obligación de informar a los trabajadores de esta medida, "*lo que está realizando* (la empresa) *con esta omisión es una interpretación unilateral de la facultad excepcional, atribuyéndose medios y facultades que el Ordenamiento Jurídico solo ha previsto de forma excepcional, y que en modo alguno sirven para omitir los deberes que frente a los derechos fundamentales competen a la empresa*". Por ello, considera que la prueba que da pie al despido vulneró el derecho a la intimidad del trabajador, debiéndose calificarse el despido del mismo como improcedente.

Frente a la resolución del Tribunal Superior de Justicia del País Vasco se alzó la empresa, presentando recurso de casación para la unificación de doctrina frente al Tribunal Supremo. No obstante, este Tribunal inadmitió el recurso por considerar que no concurría la contradicción de supuestos exigida para resolver sobre el asunto.

Ante esta inadmisión, la empresa presenta recurso de amparo ante el Tribunal Constitucional alegando que la sentencia del Tribunal Superior de Justicia del País Vasco le ha provocado una vulneración del derecho a la tutela judicial efectiva (artículo 24 CE) por dos motivos: (i) por considerar que la inadmisión indebida de la prueba habría convertido en ineficaz la prueba testifical del gerente de la empresa cuando declaró que el trabajador había reconocido los hechos en su presencia; (ii) por considerar que la inadmisión de la grabación era indebida, impidiéndole utilizar los medios de prueba pertinentes y el derecho a un proceso con todas las garantías.

2. Sentencia 119/2022 del Tribunal Constitucional desde el punto de vista de la protección de datos

2.1. Argumento mayoritario de la sentencia

En atención a los hechos anteriormente descritos el Tribunal Constitucional admite el recurso de amparo presentado por la empresa por el segundo de los motivos alegados por la misma. Esto es, por la indebida declaración de nulidad de las grabaciones videográficas. De esta forma, se concede el amparo solicitado por la empresa.

En esencia, el Tribunal Constitucional admite que el objeto del pleito versa sobre la licitud o no de la prueba videográfica, resultando esta "*determinante para apreciar, en su caso, la vulneración del resto de los derechos invocados. A su vez, la nulidad de esa prueba se basaba en una supuesta vulneración de dos derechos: (i) el derecho a la intimidad (art. 18.1 CE), por realizar una grabación continuada en una zona de trabajo, y (ii) el derecho a la protección de datos (art. 18.4 CE), por incumplimiento de los deberes de información derivados del tratamiento inherente a la grabación y utilización de las imágenes captadas por el sistema de seguridad de la empresa*.". Por tanto, la argumentación del Tribunal Constitucional para resolver sobre este recurso se centra en el uso de las cámaras de videovigilancia desde el punto de vista de la protección de datos y, más concretamente, en relación con el apartado 1 del artículo 89 LOPD.

En este sentido, el Tribunal Constitucional, cuando aborda el asunto desde la perspectiva del derecho a la protección de datos, recuerda cuál es el marco general de protección del mencionado derecho, recogido en el artículo 18.4 de la Constitución Española (CE). En este sentido, remitiéndose a su STC 39/2016 de 3 de marzo, expone que el "*contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales (…) se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero (…). Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder de oponerse a esa posesión y usos*". De esta forma, resume el Tribunal Constitucional que "*los elementos que definen el derecho a la*

protección de datos son el consentimiento y la información para, en su caso, ejercer el derecho de oposición".

No obstante, con remisión a la misma sentencia 39/2016, el Tribunal Constitucional se ratifica en que en las relaciones laborales el consentimiento "*se entiende implícito en la propia aceptación del contrato que implica reconocimiento del poder de dirección del empresario*". Y, pese a ello o por ello, persiste el deber de información. Por tanto, "*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 (…)*."

De esta forma, para resolver el presente caso concreto, el Tribunal Constitucional entiende que para verificar la constitucionalidad del uso de videocámaras con fines disciplinarios en el ámbito laboral se debe, en primer lugar, analizar si la empresa ha cumplido con la normativa vigente en la materia, respetándose los principios de consentimiento e información, y, en segundo lugar, en caso de no haberse respetado tales principios, habrá que hacerse una tarea de ponderación o juicio de proporcionalidad para valorar la justificación de la medida.

En este sentido, el Tribunal Constitucional entiende que la regulación vigente sobre la materia se circunscribe a la interpretación y aplicación conjunta de los artículos 22 y 89 LOPD, así como del artículo 20 ET. Este último precepto, dispone que el "*empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad*". Asimismo, el artículo 20 bis ET determina que toda intromisión en el derecho a la protección de datos debe hacerse respetando lo dispuesto en la LOPD vigente.

En este sentido, el precepto específico que regula la videovigilancia laboral es el artículo 89 LOPD, remitiéndose también al mismo el artículo 22 LOPD, que regula la videovigilancia en términos generales. Según el artículo 89.1 LOPD,

> "*(l)os 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.*"

Al hilo de lo anterior, conviene indicar que el artículo 22.4 LOPD prevé en su primer párrafo que el deber de información "*se entenderá cumplido mediante 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 Reglamento (UE) 2016/679*".

En atención a esta regulación el Tribunal Constitucional concluye que, en términos generales, la implantación de cámaras de videovigilancia no requerirá el consentimiento de los trabajadores, pero sí de darles información previa y expresa sobre su existencia y finalidad, respetándose la intimidad de los lugares destinados al descanso o esparcimiento o que tengan carácter reservado. Excepcionalmente, el uso de cámaras para verificar o acreditar la comisión flagrante de un acto ilícito no exigirá el previo deber de información en los términos generales, sino que será suficiente con el distintivo informativo del artículo 22.4 LOPD.

Aplicada esta posición jurisprudencial al caso concreto, el Tribunal Constitucional entiende que la empresa procedió a la visualización de las cámaras de seguridad porque se detectó una conducta que calificó de "irregular". Después de dicha visualización se verificó la comisión de un acto ilícito. Sin perjuicio de que no consta que se informase a los trabajadores de la instalación de un sistema de videovigilancia, las cámaras estaban en un lugar visible, habiendo el cartel distintivo exigido por el artículo 22.4 LOPD.

El Tribunal Constitucional entiende que la razón de la excepción del segundo párrafo del artículo 89.1 LOPD, remitiéndose al distintivo del artículo 22.4 LOPD, es razonable, dado que "*no tendría sentido que la instalación de un sistema de seguridad en la empresa pudiera ser útil para verificar la comisión de infracciones por parte de terceros y, sin embargo, no pudiera utilizarse para la detección y sanción de conductas ilícitas cometidas en el seno de la propia empresa. Si cualquier persona es consciente de que el sistema de videovigilancia puede utilizarse en su contra, cualquier trabajador ha de ser consciente de lo mismo.*" Simplificadamente, el Tribunal Constitucional viene a decir que, si pueden iniciarse medidas legales contra una persona ajena a la empresa que cometa un

acto ilícito en las instalaciones de la misma habiendo un cartel informativo de que hay una videograbación, con la misma razón se debe poder sancionar a un trabajador.

Asimismo, el Tribunal Constitucional le da un sentido totalmente distinto al Tribunal Superior de Justicia del País Vasco al hecho de que en el año 2014 la misma empresa despidiese a otro trabajador por hechos similares a los del supuesto presente y utilizándose también cámaras de videovigilancia para imponer la sanción. Mientras que para el Tribunal Superior de Justicia del País Vasco supone un incumplimiento de la obligación de informar de forma previa y expresa a los trabajadores impuesta por el primer párrafo del artículo 89.1 LOPD, para el Tribunal Constitucional implica que el trabajador despedido estaba plenamente informado de las consecuencias que podían derivarse de sus actos, esto es, de que podía ser despedido, teniendo en cuenta que prestaba servicios para la empresa desde el año 2007. De esta forma, rebatiendo al Tribunal de Justicia del País Vasco, entiende que "*de ese dato no se puede deducir la invalidez de la utilización de esas imágenes en los casos de conducta ilícita flagrante, porque la mayor o menor flagrancia de la conducta no depende de la existencia o no de un hecho acreditado con anterioridad a través de esa medida*".

En definitiva, el Tribunal Constitucional entiende que la actuación de la empresa se ha circunscrito a los cánones legales exigidos por la normativa vigente en materia de protección de datos personales, dado que: (i) existía el cartel informativo en un lugar visible y cumpliendo con las previsiones del artículo 22.4 LOPD; y, (ii) las cámaras se usaron para comprobar un hecho en concreto, "*que resultó flagrante, y sobre la base de una sospecha indiciaria concreta, como era la irregularidad manifiesta de guardar un producto de la empresa dentro de una bolsa con el logotipo de una empresa de la competencia, en un lugar no habilitado a tal efecto, del que desapareció al día siguiente*." Es decir, en este caso, no resultó necesario realizar el triple juicio de proporcionalidad, dado que la conducta de la empresa fue totalmente respetuosa con la legalidad vigente al incluir el cartel distintivo exigido por el segundo párrafo del artículo 89.1 LOPD en relación con el artículo 22.4 LOPD, habiéndose detectado la comisión flagrante de un acto ilícito.

2.2. Voto particular

Sin perjuicio del sentir mayoritario, se emite un voto particular contra este por parte de 5 magistrados del Tribunal Constitucional en el que se discrepa de la fundamentación jurídica y el fallo de la sentencia. Básicamente, expone dos motivos. El primero, que se ha otorgado al derecho de prueba del artículo 24.1 CE un alcance que no tiene. El segundo, y en el que se centra este comentario de sentencia, que no debe permitirse en

este caso una excepción a la obligación de informar ante un tratamiento de datos personales mediante sistemas de videovigilancia.

Se expone en el voto particular que ante un sistema de videovigilancia hay una posición muy distinta entre los trabajadores y la clientela o público general, dado que no se monitoriza en el mismo grado la imagen de unos y de otros. Por ello, entiende que, siendo el derecho a la información parte esencial del núcleo del derecho a la protección de datos, se debe informar a los trabajadores no solo de que se está captando su imagen, sino también sobre la finalidad a la que va a estar dirigido dicho tratamiento.

Para el voto particular, la nueva regulación contenida en el artículo 89.1 LOPD, que no había sido valorada por ninguna se las sentencias anteriores del Tribunal Constitucional y del Tribunal Europeo de Derechos Humanos, supone un cambio de paradigma, ya que desautoriza "*la posibilidad del cumplimiento ordinario del deber de información a los trabajadores mediante la mera información genérica dada al público*".

Para el Tribunal Constitucional, la aplicación de la excepción del segundo párrafo del artículo 89.1 LOPD no solo depende de la existencia un incumplimiento flagrante, sino que además se exige que "*se den cumplidas razones por parte del empleador respecto de su incumplimiento* (del deber de informar)". A su juicio, entender esta previsión normativa en el sentido en que lo hace el voto mayoritario pone "*en un mismo nivel valorativo la regla general y la excepción*". Y, por ello, debió desestimarse el recurso de amparo presentado.

3. Marco general de regulación del deber de información en la videovigilancia

Tal y como se reconoce en la propia sentencia del Tribunal Constitucional, la imagen de una persona es a todas luces un dato de carácter personal que está protegido, por tanto, por el artículo 18.4 CE. En este sentido, todo tratamiento de datos personales debe respetar el marco general diseñado por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (RGPD).

Como también asume el propio Tribunal Constitucional en la sentencia comentada, la normativa de protección de datos parte de la premisa de que en las relaciones laborales el consentimiento, como base jurídica para fundamentar un tratamiento de datos personales (artículos 6.1.a) y 9.2.a) RGPD), tiene una validez limitada al producirse un desequilibrio

de poder evidente entre la figura de la empresa y el trabajador que lo condicionará en la mayoría de casos en favor de la empresa[1].

Pese a ello, subsiste en el RGPD la obligación de respetar el resto de principios del RGPD. Entre ellos, el principio de transparencia (artículo 5.1.a) RGPD), que, desarrollado por el artículo 12.1 RGPD, obliga a todo responsable del tratamiento[2] a tomar "*las medidas oportunas para facilitar al interesado toda información indicada en los artículos 13 y 14 (…) en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo (…)*". En esencia, dichos preceptos obligan a informar al interesado -la persona cuyos datos son objeto de tratamiento- antes de que se inicie un tratamiento de datos personales de, entre otros aspectos, la identidad del responsable, sus datos de contacto, la finalidad del tratamiento, su base jurídica, y el plazo de conservación de los mismos. Por tanto, antes de que se inicie un tratamiento de datos personales relacionado con la videograbación en un centro de trabajo, el RGPD exige que la empresa informe individualmente a cada uno de los trabajadores de que va a ser grabado, por qué va a ser grabado, para qué va a ser grabado y durante cuánto tiempo. El objetivo de este derecho específico de informar es permitir que la persona pueda ejercitar los derechos relacionados con la protección de datos personales[3].

Sin embargo, la LOPD introdujo una regulación específica en materia de videovigilancia, tanto para el público en general (artículo 22 LOPD) como para las relaciones laborales (artículo 89 LOPD). De esta forma, como detalla Federico NAVARRO NIETO, gracias a la construcción legal y jurisprudencial en el ordenamiento jurídico-laboral español se recogen actualmente tres categorías o tipos de videovigilancia en el trabajo: cámaras de control laboral, cámaras de seguridad, y cámaras ocultas[4].

En primer lugar, existe la videograbación con fines específicos de control laboral. Es decir, grabaciones destinadas a ejercer un control permanente de la prestación de servicios de los trabajadores. Como consecuencia de la instalación de las cámaras de videovigilancia, el apartado 1 del artículo 89 LOPD recoge ciertas garantías específicas.

---

[1] Comité Europeo de Protección de Datos, "Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679", 2020, p. 8-9.

[2] El término responsable es definido por el artículo 4.7) RGPD como "*la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento*". En las relaciones laborales, lo lógico es que la figura de responsable recaiga en la empresa.

[3] DURO CARRIÓN, Susana, "El deber de información en el artículo 87 y 89 LOPDGDD. La quiebra de la expectativa de privacidad vinculada al derecho a la intimidad y otros derechos fundamentales en liza en la relación laboral", *Revista de Derecho Laboral*, nº 3, 2021, p. 78.

[4] NIETO NAVARRO, Federico, "La videovigilancia empresarial frente a ilícitos laborales. Comentario a la STC 119/2022, de 29 de septiembre", *Diario La Ley*, nº 10177, 2022 (versión digital).

La primera, que el control laboral del artículo 20.3 del Estatuto de los Trabajadores (ET) se ejerza dentro del marco legal de dicho precepto y con los límites inherentes al mismo. Es decir, respetándose la dignidad de la persona y su derecho a la intimidad, haciéndose un uso proporcional de la videovigilancia. Ello hace que no parezca admisible, en general, la instalación de cámaras de videovigilancia de forma genérica y permanente como forma de control laboral[5].

La segunda, que se informe sobre esta medida de control laboral tanto a los trabajadores individualmente considerados como a su representación laboral, en caso de haberla, siempre con carácter previo a su implementación y de forma expresa, clara y concisa. A mí modo de entender, esto supone la obligación de informar a los trabajadores y a su representación cumpliendo con las exigencias del artículo 12.1 RGPD. Es decir, para ejercer una función de control laboral mediante cámaras de videovigilancia el artículo 89.1 ET dispone las mismas exigencias que el artículo 12.1 RGPD. Por tanto, antes de iniciarse la grabación de imágenes se deberá informar a la persona trabajadora de la existencia de estas grabaciones y la finalidad de las mismas, entre otros aspectos.

Asimismo, el ordenamiento jurídico-laboral español prevé una tercera garantía para estos casos en el artículo 64.5.f) ET. Según este precepto, antes de implementar una medida de control laboral (como la videovigilancia) la empresa debe informar a la representación de la plantilla al respecto y solicitar que emita un informe al respecto. Es decir, además de recibir la información, la representación social tiene la posibilidad de emitir un informe al respecto.

En segundo lugar, existen las cámaras de videovigilancia relacionadas con la seguridad de las instalaciones, las personas y los bienes. Las condiciones y garantías para el uso legal de estas cámaras están condicionados, según el segundo párrafo del apartado 1 del artículo 89 LOPD, a que el trabajador cometa un flagrante "acto ilícito" y a que exista "*el dispositivo al que se refiere el artículo 22.4 de esta ley orgánica*" respectivamente. Es decir, en este caso la garantía prevista es que la empresa disponga en sus instalaciones del dispositivo al que se refiere la Instrucción 1/2006, de 8 de noviembre de la Agencia Española de Protección de Datos. Como puede apreciarse, en estos casos el contenido de la obligación de información se reduce, probablemente para evitar que se consideren ilícitas -y, por tanto, inválidas- unas grabaciones que detectan la comisión de un acto ilícito por vulnerar un derecho fundamental[6].

[5] GARCÍA MURCIA, Joaquín, y RODRÍGUEZ CARDO, Iván Antonio, "La protección de datos personales en el ámbito de trabajo: una aproximación desde el nuevo marco normativo", *Revista Española de Derecho del Trabajo*, nº 216, 2019 (versión digital)

[6] VALLE MUÑOZ, Francisco Andrés, "Las cámaras de videovigilancia en la empresa como prueba en el proceso laboral", *IUSLabor*, nº 3, 2021, p. 41.

De esta forma, un visionado de imágenes que no respetase el deber genérico de informar a los trabajadores, sino que este se limitase al dispositivo informativo de la Instrucción 1/2006, solo sería legal en el ámbito laboral si existe una sospecha razonable de que se ha cometido un "acto ilícito". Si bien, como apunta Raquel SERRANO OLIVARES[7], esta referencia deja latente la duda sobre si se refiere a ilícitos laborales o penales, estoy de acuerdo con la opinión de que se refiere a supuestos relacionados con la transgresión de la buena fe contractual, la deslealtad y el abuso de confianza, pero no con incumplimientos relacionados con el horario de trabajo[8]. De hecho, el Tribunal Supremo se posiciona en este sentido en múltiples sentencias cuando afirma que el uso de estas cámaras "*excluye otro tipo de control laboral que sea ajeno a la seguridad, esto es el de la efectividad en el trabajo, las ausencias del puesto de trabajo, las conversaciones con compañeros, etc.*"[9].

Por último, en atención a la STEDH, Gran Sala, de 17.10.2019 (asunto López Ribalda II), se entiende que, pese a que no hay una ley que lo regule, es posible instalar una videovigilancia oculta *ad hoc* (no permanente) para ejercer un control laboral en supuestos específicos y realizando un test de proporcionalidad que lo legitime. Con anterioridad a la LOPD actual los órganos judiciales tendían generalmente a considerar legal este tipo de prácticas, eximiéndose de la obligación de informar previamente al trabajador, en los casos en que el cumplimiento de esta obligación frustraría la finalidad pretendida por la medida, siendo suficiente en estos casos el cumplimiento de los criterios de idoneidad, necesidad y proporcionalidad en sentido estricto[10].

En este sentido, tras la entrada en vigor de esta ley orgánica en el 2018, el pronunciamiento más importante que se ha producido hasta el momento al respecto ha sido la sentencia del Tribunal Supremo nº 692/2022, de 22 de julio, que ha legitimado el despido de una empleada del hogar a partir de una videograbación con cámara oculta por robar una cantidad cercana a los 30.000€. Así, parece ser que la nueva normativa no ha alterado en exceso el criterio anterior a la misma para estos casos, aunque en ese supuesto de hecho concurren circunstancias especiales como la existencia de una relación laboral especial de trabajo en domicilio y la situación de vulnerabilidad de la empleadora.

---

[7] SERRANO OLIVARES, Raquel, "Los derechos digitales en el ámbito laboral: Comentario de urgencia a la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales", *IUSLabor*, nº 3, 2018, p. 223.

[8] NIETO NAVARRO, Federico, "La videovigilancia empresarial frente a ilícitos laborales", *op cit.*, (versión digital).

[9] Entre otras, STS nº 503/2022 de 1 de junio (rec. nº 1993/2020); STS nº 1003/2021 de 13 de octubre (rec. nº 3715/2018); y, STS nº 86/2017 de 1 de febrero (rec. nº 3262/2015).

[10] RODRÍGUEZ ESCANCIANO, Susana, "Videovigilancia empresarial: límites a la luz de la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales", *Diario La Ley*, nº 9328, 2019 (versión digital).

4. Valoración crítica de la sentencia

Teniendo en cuenta todo este marco jurídico, en el presente caso el Tribunal Constitucional resuelve sobre un supuesto de hecho enmarcado en el ámbito de la videovigilancia de seguridad. Esto es, en el segundo párrafo del artículo 89.1 LOPD.

Con anterioridad a este pronunciamiento, se dudaba de si este precepto exigía dar la información previa, expresa, clara y concisa que exige el primer párrafo del artículo 89.1 LOPD o, en cambio, llevar a cabo controles sorpresivos sin cumplir con la exigencia de información anterior, limitándose a la mera "pegatina"[11].

A esta duda se le añadía, además, que el Tribunal Constitucional nunca mantuvo una posición estricta a lo largo de sus varios pronunciamientos sobre videocámaras en las relaciones laborales[12]. Cierto es que cada uno de estos asuntos tenía sus particularidades. Como también es cierto a este respecto que no había una norma general tan trascendente como el Reglamento General de Protección de Datos ni tampoco una norma específica como el artículo 89 LOPD.

En cualquier caso, tras la publicación de esta sentencia, queda claro que el Tribunal Constitucional entiende, como la Agencia Española de Protección de Datos[13], que siempre que haya un flagrante acto ilícito -sin aclarar si se trata de actos ilícitos laborales o penales- el deber de información que exige el principio de transparencia del derecho a la protección de datos queda saldado con el dispositivo informativo del artículo 22.4 RGPD.

No obstante, ya adelanto que no comparto la opinión mayoritaria del Tribunal Constitucional, tanto desde el punto de vista de la interpretación del deber de información en materia de protección de datos como desde el punto de vista de la solución aplicada al caso concreto en aplicación de su propia doctrina.
En relación con la primera de las discrepancias, en mi humilde opinión, carece del mínimo sentido que se propugne que la razón de ser del derecho a la protección de datos es "*la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso*

[11] GARCÍA MURCIA, Joaquín, y RODRÍGUEZ CARDO, Iván Antonio, "La protección de datos personales en el ámbito de trabajo", *op. cit.* (versión digital).
[12] En la STC 29/2013, de 30 de noviembre, el Tribunal Constitucional entendió que vulnera el derecho a la protección de datos el uso no informado de cámaras de videovigilancia para legitimar el despido de un trabajador por llegar tarde reiteradamente a su puesto de trabajo. Mientras, en la STC 39/2016, de 3 de marzo, entendió legítimo el uso de videocámaras ocultas para justificar el despido de una trabajadora que consiguió extraer dinero del cajero de la empresa.
[13] Agencia Española de Protección de Datos, "La protección de datos en las relaciones laborales", 2021, p. 52.

los está sometiendo"[14], pero se considere ajustada a dicho derecho una normativa que, bajo una aparente justificación en la seguridad de los medios, instalaciones y personas, exige un deber de información mínimo e insatisfactorio en relación con los trabajadores. En concreto, esta información mínima consistiría en informar con un cartel visible sobre la existencia del tratamiento, la identidad del responsable, y la posibilidad de ejercitar los derechos de protección de datos (artículos 15 a 22 RGPD). Es decir, no se exige informar sobre la finalidad a la que se van a destinar esos datos personales, ni tampoco sobre la base jurídica que legitima el tratamiento.

Hay que destacar que, según afirma el propio Tribunal Constitucional en la sentencia objeto de este comentario, el consentimiento y el deber de información forman parte del contenido esencial del derecho a la protección de datos y que, en el marco de las relaciones laborales, el primero carece de relevancia. De esta forma, ante la ausencia del primero, el segundo debería devenir más trascendente todavía en el entorno laboral.

En este sentido, pese a que el Tribunal Constitucional defiende en su sentencia que su doctrina es compatible con la STEDH, Sala 2ª, de 5.9.2017 (Barbulescu II) y con la STEDH, Gran Sala, de 17.10.2019 (asunto López Ribalda II), entiendo que legitimar el uso de videocámaras de seguridad con fines disciplinarios en el marco de una relación laboral sin que se informe al respecto puede contravenir la doctrina de la sentencia Barbulescu II. Recuérdese que, pese a que referido al secreto de las comunicaciones y no al tratamiento de la imagen de una persona, el Tribunal Europeo de Derechos Humanos consideró que el despido de este trabajador vulneró su derecho a la privacidad porque este "*no parecía haber sido informado con anticipación del alcance y la naturaleza de las actividades de monitorización de su empresario*". Teniendo en cuenta que, en ese caso, la empresa había enviado un texto al trabajador, que lo firmó, informándole de que se monitorizaría el uso de internet de los trabajadores pudiendo tomar medidas disciplinarias si no se daba un uso apropiado a sus dispositivos informáticos, pero sin indicarle que la monitorización alcanzaría a sus cuentas personales.

Por consiguiente, entiendo que no respeta el núcleo esencial del derecho a la protección de datos una normativa que ampara el uso de la videovigilancia por motivos de seguridad sin que se ponga a disposición de los trabajadores información sobre el uso al que se puede destinar sus datos personales, ni sobre la base jurídica que legitima el tratamiento. Es decir, que no se informe sobre el fundamento legal que sostiene una invasión de la privacidad de la persona, ni sobre para qué se va a usar la información tratada.

[14] STC 292/2000, de 30 de noviembre, FJ 6.

Más, teniendo en cuenta que, una videovigilancia continuada puede tener consecuencias perversas también para el derecho a la intimidad de los trabajadores (artículo 18.1 CE). Al amparo de esta excusa, pueden ser objeto de un tratamiento de datos personales excesivamente invasivo, por constante en intensidad -durante toda su jornada laboral- y continuado en su duración -a lo largo de todo el tiempo que permanezca contratado por la empresa-. Todo ello, sin respetar la garantía de información.

En consecuencia, una interpretación como la del Tribunal Constitucional pone en riesgo el principio de minimización de datos personales, que exige que se traten únicamente los datos "*adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados*" (artículo 5.1.c) RGPD), ya que se está permitiendo que se obtenga una gran cantidad de imágenes de los trabajadores de forma indiscriminada para utilizarlos con fines laborales que previamente no han sido claramente determinados.

Asimismo, la inobservancia del deber de información también pone en entredicho el principio de limitación de la finalidad, que exige que los datos sean "*recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines*" (artículo 5.1.b) RGPD). En este sentido, sin informar al respecto, se está permitiendo que la videovigilancia por motivos de seguridad, un tratamiento de datos personales basado en el interés legítimo de una empresa para proteger sus medios, instalaciones y personas (artículo 6.1.f) RGPD), se utilice con fines de cumplimiento del contrato de trabajo (artículo 6.1.b) RGPD), que es una base jurídica distinta a la prevista inicialmente. Es decir, podría existir incluso una incompatibilidad entre ambos tratamientos.

No obstante, es cierto que, en temas de seguridad o ante incumplimiento laborales de mayor trascendencia, tiene sentido que la exigencia de información a los trabajadores sea más laxa. Y, por ello, cabe una interpretación lógico-sistemática del segundo párrafo del artículo 89.1 LOPD en combinación con el artículo 22.4 LOPD que podría ser más flexible con el deber de información, pero también más garantista con el derecho a la protección de datos de los trabajadores.

Si se lee detenidamente, el artículo 22.4 LOPD -al que se remite el artículo 89.1 LOPD- establece en su segundo párrafo que "*(e)n todo caso, el responsable del tratamiento deberá mantener a disposición de los afectados la información a la que se refiere el citado reglamento.*" Por tanto, según la interpretación que hago de este redactado, aun en los casos en los que un visitante a un establecimiento sea informado mediante el cartel informativo de que está siendo objeto de una videograbación, la entidad que gestione el local debe disponer de una garantía adicional: permitir que estas personas accedan

instantáneamente a la información exigida por el artículo 12 RGPD en relación con los artículos 13 y 14 RGPD, si así lo solicitan.

Esta obligación puede cumplirse fácilmente en las relaciones laborales, sin necesidad de notificar o proporcionar individualmente a los trabajadores esta información. Por ejemplo, publicando esta información a través de la intranet o la web de la empresa, pudiendo ser descargada en cualquier momento. También si se expone en el tablón de anuncios de la empresa, exigido por el artículo 81 ET. E, incluso, podría defenderse que dicha información estaba disponible para los trabajadores si se hubiese informado fehacientemente a la representación social de la existencia de videocámaras de seguridad con fines disciplinarios, dado que el artículo 64.7.e) ET exige que la representación unitaria informe al colectivo al que representa de, entre otras cuestiones, los sistemas de control del trabajo.

No obstante, el Tribunal Constitucional se ha acogido a una interpretación literal del segundo párrafo del artículo 89.1 LOPD, que tan solo exige que conste "*al menos el dispositivo al que se refiere el artículo 22.4 de esta ley orgánica*", pero no la puesta a disposición de la información prevista en su segundo párrafo. Es decir, haciendo una exégesis estricta de dicha norma, se entiende que el segundo párrafo del artículo 89.1 LOPD da por cumplido el deber de información del artículo 12 RGPD con la existencia de la famosa "pegatina". De esta forma, según la interpretación del Tribunal Constitucional, no es exigible la garantía adicional del artículo 22.4 LOPD. Esto es, que esté disponible para los trabajadores la información sobre el uso al que se destinan las imágenes capturadas por una videocámara de seguridad. Una exigencia que entiendo que sí que se deriva del artículo 22.4 LOPD para el personal no laboral afectado por este tipo de tratamientos. Así, considero que la interpretación que hace el Tribunal Constitucional del segundo párrafo del artículo 89.1 LOPD en relación con el artículo 22.4 LOPD es, incluso, menos proteccionista con los trabajadores que con cualquier visitante de un establecimiento sometido a videovigilancia, quienes no están vinculados contractualmente de forma permanente y continua con la empresa.

Por consiguiente, estoy de acuerdo con el voto particular en que esta sentencia abre la puerta a convertir la excepción del segundo párrafo del artículo 89.1 LOPD en la regla, ya que puede permitir que las empresas que ignoren la obligación de informar a los trabajadores cuando traten datos personales mediante videocámaras, prevista en el primer párrafo del artículo 89.1 LOPD, utilicen dichos datos ante cualquier incumplimiento laboral vinculado con la "seguridad" (merezca también sanción penal o no), siempre y cuando las cámaras capten que dicho incumplimiento es "flagrante". Es decir, la posición

del Tribunal Constitucional podría contribuir a desincentivar el cumplimiento del deber de información ante el uso de cámaras de videovigilancia por parte de las empresas[15]

En cambio, no concuerdo con el voto particular con el hecho de que el párrafo segundo del artículo 89.1 LOPD exige que la empresa tenga una justificación reforzada para el incumplimiento del deber de informar ante situaciones de "flagrante acto ilícito". Ello no se deriva de dicho precepto que, en su literalidad, es bastante claro. Otra cosa distinta es que dicha literalidad respete el derecho a la protección de datos, que en mi humilde opinión, si no es haciendo una interpretación lógico-sistemática, entiendo que no.

En lo que respecta a la segunda de las objeciones con la sentencia comentada, ya se ha indicado que, según el Tribunal Constitucional, se recurrió al visionado de las cámaras de seguridad "*sobre la base de una sospecha indiciaria concreta, como era la irregularidad manifiesta de guardar un producto de la empresa dentro de una bolsa con el logotipo de una empresa de la competencia, en un lugar no habilitado a tal efecto, del que desapareció al día siguiente*". Es decir, el Tribunal Constitucional entiende que se produjo el visionado de las cámaras porque se sospechaba que se hubiese cometido un acto ilícito.

Sin embargo, ello no se corresponde con el relato hecho por la empresa en la carta de despido que le entrega al trabajador, y que vincula y limita su defensa judicial en virtud del artículo 105.2 de la Ley Reguladora de la Jurisdicción Social. En este sentido, según consta literalmente en la carta de sanción, el motivo del visionado de las cámaras de seguridad era "*saber a quién podría pertenecer la bolsa; o quién se la podría haber olvidado*". Es decir, según se declara en la carta de despido, la empresa procedió al visionado de las cámaras con una motivación de ejercer un control laboral estricto, ya que declara expresamente que querían conocer la titularidad de la bolsa. Por tanto, en este momento la empresa no tenía una sospecha de que se estuviese produciendo un "flagrante acto ilícito", sino que ejerció funciones de control laboral produciéndose un "*hallazgo casual*", tal y como lo define el Tribunal Supremo en su auto de inadmisión del recurso de casación para la unificación de doctrina.

De hecho, en la misma carta de despido se afirma que, una vez visualizada la grabación, "*procedió a la revisión de los albaranes a fin de determinar si existía alguno generado por usted conteniendo dichos productos.*" Es decir, la empresa confirma en la carta de despido que hizo el camino inverso al que marca la doctrina del Tribunal Constitucional.

[15] BELTRÁN DE HEREDIA RUIZ, Ignasi, "Cámaras de vigilancia, intimidad y protección de datos: prueba lícita y despido procedente (STC 119/2022)", *Una mirada crítica a las relaciones laborales* (blog), 22.10.2022 (disponible en: https://ignasibeltran.com/2022/10/25/camaras-de-vigilancia-intimidad-y-proteccion-de-datos-prueba-licita-y-despido-procedente-stc-119-2022/; consulta, 20.1.2023).

Sin tener sospechas relevantes, decide visualizar las cámaras de seguridad para verificar la titularidad de la bolsa. Las cámaras demuestran que, a priori, ha habido una venta ilegal en el centro de trabajo. Posteriormente, para confirmarlo, la empresa sigue investigando si se ha registrado esa venta o si se ha hecho un presupuesto de la misma en los registros informáticos. De esta forma, comprueban que sí que se hizo un presupuesto por parte del trabajador, que luego fue ocultado por el mismo, para tener una aproximación del valor de los productos vendidos para así repercutirlo ilegalmente en su cliente. Es decir, el visionado de las cámaras de seguridad tampoco demuestra que el acto ilícito sea flagrante, dado que necesitan confirmarlo después con otras actuaciones indagadoras.

En este sentido, para poder proceder a una visualización legal de las cámaras de seguridad siguiendo la doctrina del Tribunal Constitucional, una vez se hubiese confirmado que el termostato ya no estaba encima de la mesa de atención al cliente, se debería de haber comprobado si se registró la venta y/o se hizo un presupuesto al respecto. Y después, tras descubrir que había un presupuesto oculto realizado con dicho termostato, se debería de haber procedido a visualizar las cámaras de seguridad, ya que a partir de dicho momento las sospechas de una apropiación indebida serían mucho más razonables.

De esta forma, la actuación de la empresa se enmarca a mi juicio en el primer párrafo del artículo 89.1 LOPD y, no habiendo cumplido con el deber genérico de información que le exige dicho precepto en relación con el artículo 12.1 RGPD, el Tribunal Constitucional, aplicando su propia doctrina, debió de entender que la visualización vulneró dichos preceptos y, por tanto, el derecho a la protección de datos (artículo 18.4 CE).

En definitiva, sea por la interpretación que se hace del derecho a la protección de datos en relación con la videovigilancia en el ámbito laboral *ex* artículos 89.1 y 22.4 LOPD, sea por la aplicación de su propia doctrina al caso en concreto, comparto con el voto particular de esta sentencia que "*la jurisprudencia constitucional no ha respondido en este caso a la altura de las circunstancias históricas en que se encuentra el desarrollo del derecho a la protección de datos de carácter personal frente al desafío de la vertiginosa evolución de las tecnologías del control personal, dejando desatendida la tutela del derecho a la protección de datos de carácter personal en un ámbito de especial sensibilidad como es el de las relaciones de trabajo.*"

5. Bibliografía

Agencia Española de Protección de Datos, "La protección de datos en las relaciones laborales", 2021.

BELTRÁN DE HEREDIA RUIZ, Ignasi, "Cámaras de vigilancia, intimidad y protección de datos: prueba lícita y despido procedente (STC 119/2022)", *Una mirada crítica a las relaciones laborales* (blog), 22.10.2022 (disponible en: https://ignasibeltran.com/2022/10/25/camaras-de-vigilancia-intimidad-y-proteccion-de-datos-prueba-licita-y-despido-procedente-stc-119-2022/; consulta, 20.1.2023).

Comité Europeo de Protección de Datos, "Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679", 2020.

DURO CARRIÓN, Susana, "El deber de información en el artículo 87 y 89 LOPDGDD. La quiebra de la expectativa de privacidad vinculada al derecho a la intimidad y otros derechos fundamentales en liza en la relación laboral", *Revista de Derecho Laboral*, nº 3, 2021, p. 91-2017.

GARCÍA MURCIA, Joaquín, y RODRÍGUEZ CARDO, Iván Antonio, "La protección de datos personales en el ámbito de trabajo: una aproximación desde el nuevo marco normativo", *Revista Española de Derecho del Trabajo*, nº 216, 2019 (versión digital).

NIETO NAVARRO, Federico, "La videovigilancia empresarial frente a ilícitos laborales. Comentario a la STC 119/2022, de 29 de septiembre", *Diario La Ley*, nº 10177, 2022 (versión digital).

RODRÍGUEZ ESCANCIANO, Susana, "Videovigilancia empresarial: límites a la luz de la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales", *Diario La Ley*, nº 9328, 2019 (versión digital).

SERRANO OLIVARES, Raquel, "Los derechos digitales en el ámbito laboral: Comentario de urgencia a la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales", *IUSLabor*, nº 3, 2018, p. 216-229.

VALLE MUÑOZ, Francisco Andrés, "Las cámaras de videovigilancia en la empresa como prueba en el proceso laboral", *IUSLabor*, nº 3, 2021, p. 31-59.