



El derecho a la protección de datos personales ante la videovigilancia en el ámbito laboral: la progresiva devaluación en la jurisprudencia constitucional de la obligación de informar al trabajador

The right to the protection of personal data in the face of video surveillance in the workplace: the progressive devaluation in constitutional jurisprudence of the obligation to inform the worker

MIGUEL ÁNGEL CABELLOS ESPIÉRREZ

Catedrático de Derecho Constitucional

Universidad de Girona

E-mail: miguel.cabellos@udg.edu

ORCID: 0000-0002-3806-3512

DOI: <https://doi.org/10.47623/ivap-rvap.128.2024.1.01>

LABURPENA: Bideozaintza langileen ez-betetzeen aurkako kontrol-mekanismo gisa erabiltzeak eboluzio nabarmena izan du araudian eta jurisprudenzian. Eboluzio horretatik abiatuta, egiaztatu daiteke langileari jakinarazteko eginbeharrak gero eta devaluazio handiagoa izan duela, eta horrek goia jo du azken jurisprudenzia konstituzionalarekin. Izan ere, jurisprudenzia horrek, oraingo araudiaren interpretazioarekin, ia borondatezkoa egin du enpresariarentzat langileei informazioa ematea edo ez ematea modu zehatzean eta berariaz, enpresaren barruko bideozaintzaren eta horren helburuen inguruan. Aldi berean, aukera ematen zaio enpresariari bideozaintza-jardueraren emaitzez baliatzen jarraitzeko, lan-jarduera kontrolatze aldera, nahiz eta ez bete behar bezala langileei informazioa emateko eginbeharrak. Hori bateragarri izatea langileek datu-babesa izateko duten eskubideen funtsezko edukiarekin (Espainiako Konstituzioko 18.4. art.) eztabaidagarria da, eta horregatik, lan honek xede du KAREN egungo interpretazioak planteatutako arazoak aztertzea, bai eta horrek DPBEBLOaren xedapenei arautu nahi zuenarekin bat ez zetorren edukia nola eman zion ere, kaltegarria baita lan-esparruko datu-babesa den funtsezko eskubidea eraginkorra izateko.

HITZ GAKOAK: Datu-babesa. Bideozaintza. Langilearentzako informazioa. Proporzionaltasuna. Jurisprudenzia konstituzionala.

ABSTRACT: The use of video surveillance as a control mechanism for non-compliance by workers has been the subject of a very notable regulatory and jurisprudential evolution. From this evolution, it can be observed how the duty to



inform the worker has progressively depreciated, reaching its peak with the latest constitutional jurisprudence. With its interpretation of current regulations, the Constitutional Court has virtually made it voluntary for employers to inform, or not, in a minimally precise and explicit manner, the workers about the existence and purposes of video surveillance within the company. Meanwhile, employers are allowed to continue benefiting from the results of this video surveillance activity to monitor work activities, despite not having sufficiently fulfilled their obligations to inform the workers. Whether this is compatible with the essential content of the workers' right to data protection (Article 18.4 CE) is, at the very least, debatable. The purpose of this work is to analyze the problems posed by the current interpretation of the Constitutional Court and how it has given a content to the provisions of the Spanish Organic Law on Data Protection and Digital Rights (LOPDGDD) that does not seem to correspond to what the latter intended to regulate, with consequent harm to the effectiveness of a fundamental right such as the right to data protection in the workplace.

KEYWORDS: Data Protection. Video surveillance. Employee information. Proportionality. Constitutional jurisprudence.

RESUMEN: El uso de la videovigilancia como mecanismo de control frente a incumplimientos de los trabajadores ha sido objeto de una evolución normativa y jurisprudencial muy notable. A partir de dicha evolución puede constatarse cómo el deber de informar al trabajador ha ido sufriendo una progresiva devaluación, que ha alcanzado su punto máximo con la última jurisprudencia constitucional, que con su interpretación de la actual normativa ha acabado por hacer prácticamente voluntario para el empresario el hecho de informar o no de una manera mínimamente precisa y expresa a los trabajadores de la existencia y fines de la videovigilancia en el interior de la empresa, al tiempo que se le permite a aquel seguir beneficiándose de los resultados de esa actividad de videovigilancia para controlar la actividad laboral, pese a no haber cumplido suficientemente con sus obligaciones de información a los trabajadores. Que ello sea compatible con el contenido esencial del derecho de estos a la protección de datos (art. 18.4 CE) resulta, cuando menos, discutible, y el propósito de este trabajo es analizar por ello los problemas que plantea la interpretación actual del TC y cómo la misma ha dado a las previsiones de la LOPDGDD un contenido que no parece corresponderse con lo que esta parecía querer regular, con el consiguiente perjuicio para la eficacia de un derecho fundamental como es el de la protección de datos en el ámbito laboral.

PALABRAS CLAVE: Protección de datos. Videovigilancia. Información al trabajador. Proporcionalidad. Jurisprudencia constitucional.

Trabajo recibido el 20 de noviembre de 2023

Aceptado por el Consejo de Redacción el 19 de enero de 2024



Sumario: I. La evolución normativa y jurisprudencial en el ámbito de la videovigilancia laboral. —II. La devaluación del significado de la información en el ámbito laboral y sus efectos indeseados. ¿Puede la negligencia o la mala fe del empresario a la hora de aplicar la normativa sobre protección de datos ser utilizada en su propio beneficio? El caso de la STC 119/2022. —III. Entre la flagrancia y la mera sospecha. ¿Qué autoriza a acudir a las grabaciones realizadas? El concepto de acto ilícito. —IV. Conclusiones: un paso más en la devaluación del reconocimiento al derecho a la protección de datos en los casos de videovigilancia laboral. —V. Bibliografía.

I. La evolución normativa y jurisprudencial en el ámbito de la videovigilancia laboral

El uso de la videovigilancia como posible mecanismo de control frente a incumplimientos de los trabajadores (y con ello el tratamiento de los conflictos con los derechos de estos a que dicha medida pueda dar lugar) ha sido objeto de una evolución normativa y jurisprudencial muy notable. Ello se aprecia especialmente si atendemos al elemento de la información acerca de la recogida y tratamiento de datos del trabajador, información que forma parte del contenido esencial del derecho que a este le reconoce el art. 18.4 CE, por cuanto si tal derecho, según expusiera la STC 292/2000, «persigue garantizar a [la] persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado», es indudable que, para que tal control pueda ser real, resulta entre otras cosas imprescindible «el reconocimiento del derecho a ser informado de quién posee sus datos personales y con qué fin» (FFJJ 6 y 7).

La determinación del modo concreto de facilitar esa información en el ámbito laboral se ha establecido de manera progresiva a lo largo del tiempo a partir de diversas normas y de una jurisprudencia que intentaba cubrir los flancos y dudas que el legislador o no había atendido aún o lo había hecho de manera parcial. A partir de esa evolución temporal constataremos cómo el deber de informar al trabajador ha ido sufriendo, tanto en el nivel normativo como en el jurisprudencial, una progresiva aminoración o devaluación, pero que ello, con la última jurisprudencia constitucional y su interpretación de la actual normativa, ha llegado al extremo de hacer prácticamente voluntario para el empresario el hecho de informar o no de una manera mínimamente precisa y expresa a los trabajadores de la existencia y fines de la videovigilancia en el interior de la empresa, al tiempo que se permite a dicho empresario seguir beneficián-



dose de los resultados de esa actividad de videovigilancia para controlar la actividad laboral pese a no haber cumplido suficientemente con sus obligaciones de información a los trabajadores. Que ello sea compatible con el contenido esencial del derecho a la protección de datos de estos resulta, cuando menos, discutible.

Antes de acudir al análisis de dichas cuestiones, sin embargo, resulta oportuno realizar una rápida mirada a la mencionada trayectoria normativa y jurisprudencial, como base necesaria para abordar después nuestro objeto central de análisis, la última jurisprudencia del TC en el ámbito que tratamos.

Comenzando por el plano normativo, desde un punto de vista general hemos de referirnos al art. 20.3 ET, relativo a los poderes de control del empresario¹, que en un primer momento, a falta de normativa más específica, sirvió para dar cobertura a toda clase de medidas de control empresarial con la exigencia añadida de que estas respetaran la dignidad del trabajador, a lo que fueron añadiéndose en esta primera etapa referencias en la normativa y la jurisprudencia a los derechos a la intimidad o a la propia imagen del art. 18.1 CE, pues el derecho a la protección de datos no entraría en juego hasta una etapa posterior². Aquel precepto de la norma laboral básica se vería con el tiempo complementado por la normativa dedicada a regular el tratamiento y protección de datos, primero desde una perspectiva más general y en los últimos años a través de regulaciones ya referidas específicamente a la videovigilancia laboral. Se ha ido remediando así paulatinamente en este sector lo que Goñi Sein ha denominado «un panorama de anomia e indiferencia del legislador hacia el papel de los derechos fundamentales en el ámbito de las facultades de control empresarial»³, que obligaba a los tribunales a ir aportando solu-

¹ Desde 1980 hasta la actualidad, en las sucesivas regulaciones del Estatuto de los Trabajadores, el precepto ha mantenido una redacción idéntica (salvo algún detalle léxico) y establece 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», aunque ello siempre «guardando la consideración debida a su dignidad».

² A modo de apoyo se citaban también el derecho de propiedad (art. 33 CE) y la libertad de empresa (art. 38 CE), pero era el precepto del ET el que realmente daba soporte a las actuaciones empresariales de vigilancia. Cuando posteriormente la normativa (y la propia jurisprudencia) atiendan también al derecho del art. 18.4 CE, la cita de los arts. 33 y 38 CE se mantendrá igualmente con una cierta función de dotar al art. 20.3 ET y al resto de preceptos legales concurrentes de un engarce constitucional que permita en cada caso realizar una ponderación con dicho art. 18.4 CE. Con todo, es de observar que poner ambos conjuntos normativos al mismo nivel es más que discutible, pues este último contiene un derecho fundamental que goza de la mayor protección por su ubicación en la Constitución, y frente a él se alzaría un precepto legal que pretendería ser expresión de los arts. 33 y 38 CE. *Vid.* en tal sentido el voto particular del magistrado Valdés Dal-Ré (al que se adhiere la magistrada Asua Batarrita) a la STC 39/2016.

³ *Vid.* GOÑI SEIN, J.L., «Vigilancia empresarial y protección de datos: Doctrina Jurisprudencial», en *Revista del Ministerio de Trabajo, Migraciones y Seguridad Social*, núm. 143, 2019, pág. 192.



ciones para cubrir esa laguna, lo que se hizo por parte del TS y del TC de manera no siempre armónica ni exenta de contradicciones⁴.

Así, debemos acudir en primer lugar a la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD) y sobre todo (por su mayor vigencia y aplicación en el tiempo) a la posterior Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), que derogó a la primera, y que de modo semejante a como lo hacía su predecesora establecía en su art. 5 la obligación de informar a aquellos cuyos datos personales se solicitaran de una serie de aspectos, e informarles de ellos «de modo expreso, preciso e inequívoco»⁵. Por su parte, el art. 6 fijaba la regla de que el tratamiento de los datos de carácter personal requeriría «el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa» y a continuación exceptuaba la necesidad de tal consentimiento, entre otros supuestos, «cuando [los datos] se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento». En tal caso, pues, no se requeriría consentimiento pero sí información al trabajador (en los términos del art. 5 antes mencionado).

El siguiente paso en la regulación de este ámbito vino dado por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGD), que viene a sustituir a su predecesora de 1999 y a adaptar nuestra normativa a las exigencias del Reglamento (UE) 2016/679, General de Protección de Datos (RGPD). Aparte de las consideraciones generales que la nueva ley hace en relación con los deberes generales de información a aquellas personas cuyos datos se recopilan (art. 11) o con el uso de la videovigilancia con carácter general (art. 22), lo relevante a nuestros efectos es que por primera vez se lleva a cabo en este ámbito una regulación específica de la videovigilancia en el ámbito laboral⁶, al tiempo que se aprovecha, mediante la Dis-

⁴ Goñi Sein señala que en la actuación de ambos tribunales «el TC ha marcado la pauta y el TS ha ido a rebufo, situándose en un área subalterna. Así, el panorama de la jurisprudencia más reciente del TS muestra los mismos vaivenes que los del TC en relación con la instalación de los sistemas de videovigilancia en el lugar de trabajo». Vid. GOÑI SEIN, J.L., «Vigilancia empresarial...», *ob. cit.*, pág. 201.

⁵ El art. 3 de la Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos de carácter personal con fines de vigilancia a través de sistemas de cámaras o videocámaras, desarrollaría una serie de elementos tendentes a brindar dicha información, entre ellos el distintivo de advertencia de videovigilancia dirigido al público en general y que sirviera a este para conocer la existencia de dicha videovigilancia en, por ejemplo, un local comercial.

⁶ Fuera del ámbito laboral se habían dictado antes algunas normas: así, se reguló su uso por parte de la policía en lugares de tránsito público con finalidades de preservación de la seguridad y prevención y control del delito a través de 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. También encontramos una breve regulación en el art. 42 de la Ley 5/2014, de 4 de abril, de Seguridad



posición final decimotercera de la ley, para introducir en el ET un nuevo artículo 20 bis sobre «derechos de los trabajadores a la intimidad en relación con el entorno digital y a la desconexión» (llama la atención la ausencia de referencia al derecho a la protección de datos), en el que a su vez se contiene una remisión a la LOPDGD. En esta, y por lo que aquí nos interesa, su art. 89 se dedica específicamente a proteger el derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo⁷. El uso de dichos mecanismos se permite para las finalidades del control de los trabajadores a que se refiere el art. 20.3 ET, y así nos lo dice expresamente el art. 89 LOPDGD al referirse al uso de las cámaras para «funciones de control de los trabajadores o los empleados públicos», al tiempo que se establecen límites (no poderse llevar a cabo la videovigilancia en espacios destinados al descanso o esparcimiento de los trabajadores, o en aquellos en que deba preservarse la intimidad de estos como aseos o vestuarios), pero sobre todo lo relevante es que la ley fija una regla y una excepción.

La regla es la necesidad de que el empresario informe «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» de usar cámaras con fines de control laboral⁸. No hay, pues, que obtener consentimiento de los trabajadores, pero sí que se les debe informar en los términos que acaban de indicarse.

La excepción (o si se quiere transformación del modo de informar por parte del empresario) es que «en el supuesto de que se haya captado la

Privada. Asimismo, se han dictado reglamentos de desarrollo en estos ámbitos, tanto en el plano estatal como autonómico.

⁷ También dentro del mismo ámbito de uso en el trabajo de mecanismos tecnológicos de vigilancia, el art. 87 se refiere al uso de dispositivos digitales y su posible control por el empresario, y el 90 al uso de dispositivos de geolocalización del trabajador. No nos referiremos a ellos aquí, pero sí que merece la pena reseñar las diferencias que hay en cada uno de los tres preceptos (87, 89 y 90) en cuanto a los deberes de información que en cada caso ha de cumplimentar el empresario: un deber más difuso en el caso de los dispositivos digitales (solo se dice que el empresario deberá «establecer criterios de utilización de los mismos»), muy estricto en cambio en el caso de la geolocalización, en que el empresario debe dar una información previa, completa y sin excepciones, y por último el caso de la videovigilancia constituiría un caso intermedio entre ambos: deber de información pero con atenuación en el caso de captación de acto ilícito flagrante, como se verá. *Vid.* sobre ello GARCÍA RUBIO, M.A., «Control tecnológico empresarial y nuevos problemas aplicativos tras la L.O. 3/2018. Una mirada desde el deber de información previa», *Labos*, vol. 3, núm. 1, 2022, págs. 27 ss. También ha de tenerse en cuenta que cuando la videovigilancia no solo capte imágenes sino también sonidos, el art. 89.3 LOPDGD endurece los requisitos para que su uso sea lícito. En el presente trabajo nos referiremos únicamente a la videovigilancia que capta imagen, pero no sonido (art. 89.1 LOPDGD).

⁸ Sobre el alcance de la información a los representantes de los trabajadores, *vid.* asimismo el art. 64.5 f) ET, que señala que: «el comité de empresa tendrá derecho a emitir informe, con carácter previo a la ejecución por parte del empresario de las decisiones adoptadas por este, sobre (...) la implantación y revisión de sistemas de organización y control del trabajo».



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». El art. 22 de la ley establece una regulación del modo como las personas físicas o jurídicas, ya sean públicas o privadas, podrán tratar las imágenes obtenidas mediante videovigilancia con finalidades de mantenimiento de la seguridad, y en su apartado 4 se señala que «el deber de información previsto en el artículo 12 del Reglamento (UE) 2016/679 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 consecuencia, en los casos de captación de la comisión flagrante de un acto ilícito por parte de una cámara que se hubiera colocado con fines de preservación de la seguridad en los términos del art. 22 LOPDGD (y que por tanto no estaba pensada para el control de la actividad laboral, porque en tal caso se hubiera tenido que cumplir con la regla de informar) será suficiente, por remisión del art. 89 al 22.4 LOPDGD, la existencia de un cartel informativo para considerar cumplimentado el deber de información del empresario hacia los trabajadores.

Por tanto, vemos cómo ha ido evolucionando la regulación del modo como podrán captarse imágenes en el ámbito laboral, y tratarse y utilizarse posteriormente en tanto que dato personal. Dicha evolución, y los matices que a lo largo de la misma han ido surgiendo, tendrán obviamente un reflejo directo en la jurisprudencia de cada época.

Pasando ahora al terreno jurisprudencial y refiriéndonos específicamente a la jurisprudencia constitucional, que será el objeto de este trabajo, las primeras sentencias relevantes se habían referido a los sistemas de vigilancia empresarial exclusivamente desde el punto de vista del derecho a la intimidad, sin entrar en absoluto en el mencionado derecho a la protección de datos. Tal ocurrió en la STC 98/2000, de 18 de mayo, en el caso de los sistemas de vigilancia auditiva instalados en el Casino de La Toja, o en la STC 186/2000, de 10 de julio, esta sí en torno a un sistema de videovigilancia cuyo uso dio lugar a un despido laboral, y en la que incluso el TC llega a afirmar que la ausencia de información previa a los trabajadores y al comité de empresa acerca de la instalación de dicho sistema «carece de trascendencia desde la perspectiva constitucional» desde el punto de vista del art. 18.1 CE, siendo en todo caso «una cuestión de mera legalidad ordinaria» (FJ 7)⁹. En ambas sentencias, por lo de-

⁹ Esta afirmación tan sorprendente intentará ser justificada por la posterior STC 29/2013, de 11 de febrero, diciendo que «una recta lectura de esa declaración revela que la dimensión ordinaria y no



más, el enfoque escogido es la revisión de si se han dado en la medida de vigilancia adoptada los elementos propios del test de proporcionalidad: que aquella sea necesaria, adecuada (por idónea), y proporcionada en sentido estricto.

La STC 292/2000, de 30 de noviembre, relativa al recurso de inconstitucionalidad interpuesto por el Defensor del Pueblo respecto de los arts. 21.1, 24.1 y 24.2 de la antes citada Ley Orgánica 15/1999, permitirá al TC salir de ese marco limitado al art. 18.1 CE en las sentencias subsiguientes, al hablar del contenido del derecho fundamental a la protección de datos y de su distinción con el derecho a la intimidad¹⁰, de los límites oponibles a aquel derecho y de la necesidad de establecerlos claramente mediante ley, entre otras cuestiones de interés.

Ya, por tanto, bajo la vigencia de la LOPD de 1999 y sobre la base de lo dispuesto en esta sentencia de 2000, la siguiente sentencia relevante del TC será la 29/2013, de 11 de febrero, relativa al caso de la grabación de imágenes en la Universidad de Sevilla. Es la primera sentencia que lleva a cabo su análisis desde la perspectiva del derecho a la protección de datos, y por ello la primera verdaderamente relevante a nuestros efectos. En ella, a los elementos propios del test de proporcionalidad se añadirá el de la información al trabajador como exigencia derivada del derecho contenido en el art. 18.4 CE. El TC indicará que, aunque el consentimiento del trabajador no sea necesario en ese caso porque así lo prevé la mencionada LOPD, se debe informar a aquél de la existencia de la videovigilancia, pues nada hay en dicha ley que exima de dicho deber en ningún caso; expresamente indica el TC, además, que el deber de aportar la necesaria información (que debe ser «previa y expresa, precisa,

constitucional de la cuestión no se predicaba del derecho de información como garantía nuclear del art. 18.1 CE, sino de las garantías complementarias del art. 18.1 CE que pudieran encontrar expresión en el art. 64.1.3 d) del texto refundido de la Ley del estatuto de los trabajadores (LET) y, por tanto, del alcance concreto de este precepto, relativo a los derechos de información del comité de empresa». Pero el propio Tribunal no deja de reconocer, de manera significativa, que «se comprende que el párrafo transcrito haya podido dar lugar a otras interpretaciones» (FJ 11).

¹⁰ Indica el Tribunal que: «el objeto de protección del derecho fundamental a la protección de datos no se reduce solo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales» y que «también el derecho fundamental a la protección de datos posee una segunda peculiaridad que lo distingue de otros, como el derecho a la intimidad personal y familiar del art. 18.1 CE (...) ya que a diferencia de este último, que confiere a la persona el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima de la persona y la prohibición de hacer uso de lo así conocido (...), el derecho a la protección de datos atribuye a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que no se contienen en el derecho fundamental a la intimidad, y que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales» (FJ 6). También es de interés la STC 254/1993, de 20 de julio, primera que traza el contorno del derecho fundamental del art. 18.4 CE, y que abriría una línea jurisprudencial que perfeccionaría la indicada sentencia 292/2000.



clara e inequívoca (...) de la finalidad de control») no queda excusado por el hecho de que hubiera distintivos colgados señalando la existencia de cámaras (FFJJ 7 y 8). Es significativo que el Tribunal concluyera que «lesiona el art. 18.4 CE la utilización [para llevar a cabo el control de la actividad laboral] de medios encubiertos que niegan al trabajador la información exigible» (FJ 7) y que «no contrarresta esa conclusión que existieran distintivos anunciando la instalación de cámaras y captación de imágenes en el recinto universitario, ni que se hubiera notificado la creación del fichero a la Agencia Española de Protección de Datos» pues, «privada la persona [el trabajador sancionado que recurría en amparo] de aquellas facultades de disposición y control sobre sus datos personales [al no haber sido debidamente informado], lo fue también de su derecho fundamental a la protección de datos» (FJ 8). El TC establece, pues, una conexión directa entre el derecho a ser informado (en aquellos casos en que no sea preciso el consentimiento) y el contenido esencial del derecho del art. 18.4 CE¹¹, que se vería vulnerado si no concurre aquella información, lo que excusa de realizar cualquier tipo de ponderación posterior entre los derechos de empresario y del trabajador para ver si la medida cumplía o no con los elementos del test de proporcionalidad. Si, por el contrario, se considerase admisible la falta de información o se entendiera cumplida esta a través de cualquier vía (por ejemplo la existencia de rótulos informativos dirigidos al público en general), entonces sí que habría que pasar a ponderar, pero como ya se ha dicho la sentencia no admite ninguna de esas posibilidades¹².

En claro contraste con esta posición decidida del TC en defensa del deber de informar a los trabajadores, la STC 39/2016, de 3 de marzo¹³,

¹¹ El TC se refiere en su FJ 7 a que es «elemento caracterizador de la definición constitucional del art. 18.4 CE, de su núcleo esencial, el derecho del afectado a ser informado de quién posee los datos personales y con qué fin».

¹² Pero sí que lo hace la tesis que, en cambio, se plasma en el voto particular del magistrado Ollero Tassara a la STC 29/2013, y que se convertirá en mayoritaria en 2016. También en sentido contrario a apreciar vulneración del art. 18.4 CE se pronunciaron Gude Fernández, para quien «el incumplimiento de esta obligación de información por parte de la Universidad, aunque debe castigarse administrativamente, como establece la LOPD, no ha de elevarse a la categoría de conducta vulneradora del artículo 18.4 de la CE sobre todo si tenemos en cuenta que la sanción que impone la ley es calificada como leve». Vid. GUDE FERNÁNDEZ, A., «La videovigilancia laboral y el derecho a la protección de datos de carácter personal», en *Revista de Derecho Político*, núm. 91, 2014, págs. 70-71, así como Desdentado Bonete y Muñoz Ruiz, para quienes si «cualquier infracción de la normativa de protección de datos, y en particular una infracción leve (...) es suficiente para determinar una lesión del derecho fundamental que consagra el art. 18.4 CE (...) se llegaría a una especie de sobredimensionamiento del derecho fundamental». Vid. DESDENTADO BONETE, A., MUÑOZ RUIZ, A.B., «Trabajo, videovigilancia y controles informáticos. Un recorrido por la jurisprudencia», en *Revista General de Derecho del Trabajo y de la Seguridad Social*, núm. 39, 2014, págs. 10-11.

¹³ Sobre ella vid. CABELLOS ESPIÉRREZ, M.A., «El derecho a ser informado como elemento esencial del derecho a la protección de datos. Una visión crítica de la jurisprudencia del Tribunal Cons-



viene a realizar un auténtico *overruling*¹⁴ y a sostener lo contrario que la anterior: siendo necesario según la normativa legal entonces aplicable no el consentimiento del trabajador pero sí la información a este de la existencia de la videovigilancia, considerará ahora el TC que la ausencia de dicho deber de informar «solo supondrá una vulneración del derecho fundamental a la protección de datos tras una ponderación de la proporcionalidad de la medida adoptada» (FJ 3) con lo que la diferencia con lo dicho en la sentencia previa es evidente: ha habido una disminución clara de la relevancia que la información tiene para que el trabajador pueda ejercer sus derechos, y se diluye la conexión de dicha información con el contenido esencial del derecho del art. 18.4 CE, conexión que veíamos que se daba en la sentencia de 2013¹⁵. Esa información, considera el TC, queda cumplida por el hecho de que «la empresa colocó el correspondiente distintivo en el escaparate de la tienda donde prestaba sus servicios la recurrente en amparo, por lo que esta podía conocer la existencia de las cámaras y la finalidad para la que habían sido instaladas» (FJ 4). Bastaría, pues, con colocar un distintivo (que cumpliera con las características establecidas en la Instrucción 1/2006 de la AEPD) para que el trabajador quede en todos los casos informado «sin que haya que especificar, más allá de la mera vigilancia, la finalidad exacta que se le ha asignado a ese control» (FJ 4)¹⁶, de manera que el requisito de la informa-

titucional y de su cambio de doctrina en la STC 39/2016», en *Revista Vasca de Administración Pública*, núm. 106, 2016, págs. 191-216.

¹⁴ Observa en su voto particular el magistrado Fernando Valdés Dal-Ré (al que se adhiere la magistrada Asua Batarrita) que la sentencia de 2016 se aparta de la de 2013 «sin hacer esfuerzo alguno por abrir un diálogo en divergencia [con esta], ofreciendo al menos explicaciones, aun cuando fueran de manera sumaria pero fundada [acerca del cambio de criterio] (...). El proceso de cambio doctrinal se ha llevado a cabo sin aportar la obligada argumentación jurídico-constitucional sobre las razones que conducen a abandonar una jurisprudencia cuyo objetivo, primero y esencial, fue el fijar los límites del contenido esencial del derecho fundamental que el art. 18.4 CE confiere a los trabajadores».

¹⁵ Por tanto, la ausencia de información precisa y clara al trabajador puede aparejar, nos dice el Tribunal, «sanciones legales» pero no conllevará siempre la vulneración del art. 18.4 CE (de lo que deducimos que puede constituir una cuestión de mera legalidad ordinaria). Para saber si ha habido tal vulneración deberá «ponderarse así el derecho a la protección de datos y las eventuales limitaciones al mismo justificadas en el cumplimiento de las obligaciones laborales y las correlativas facultades empresariales de vigilancia y control reconocidas en el art. 20.3 del texto refundido de la Ley del estatuto de los trabajadores, en conexión con los arts. 33 y 38 CE» (FJ 4).

¹⁶ Tras ello, el TC examinará la constitucionalidad de la medida empresarial (la grabación en video de la zona de cajas ante la existencia de descuadres contables y la sospecha de que pudiera estarse realizando algún acto ilícito) desde el punto de vista del principio de proporcionalidad aplicando los tres criterios conocidos de la necesidad, la idoneidad y la proporcionalidad en sentido estricto, pero todo ello partiendo del presupuesto de que el deber de informar ya había quedado cumplido. Critica esta lógica de ponderación el voto particular de Valdés Dal-Ré y Asua Batarrita a la sentencia, por cuanto se pondera, como se dijo, un derecho fundamental (el del art. 18.4 CE) con un pretendido derecho constitucional al control empresarial construido a partir de la suma del art. 20.3 ET y los arts. 33 y 38 CE, y se descuida con ello la protección al contenido esencial del art. 18.4 CE. También



ción queda cumplido y puede ya pasarse a examinar si la medida adoptada resultaba necesaria, adecuada y proporcionada en sentido estricto: como ha señalado Molina Navarrete, con esta sentencia lo que se hace es «privar de autonomía propia a la garantía informativa previa, para confundirla de pleno en el juicio de proporcionalidad»¹⁷. Se aprecia, pues, una devaluación del contenido y características de la información a aportar al trabajador: ya no es que su ausencia pueda no ser constitutiva de vulneración del art. 18.4 CE¹⁸, sino que un mero distintivo serviría para dar por cumplido el deber de informar¹⁹. La solución del distintivo, como ya se vio, pasaría después (pero solo para un caso concreto —actos ilícitos— y no con carácter general como en esta sentencia) al plano normativo con la Ley Orgánica de 2018, bajo la que se dictará la STC 119/2022, de 29 de septiembre de 2022, última hasta ahora de esta serie de pronunciamientos del TC y a la que nos referiremos más específicamente en los siguientes apartados²⁰.

crítico con la desatención al contenido esencial se muestra en su voto a idéntica sentencia el magistrado Xiol Ríos.

¹⁷ Vid. MOLINA NAVARRETE, C., «¿Son legítimos los usos laborales de cámaras ocultas?: no, pero sí; sí, pero no», en *La Ley Privacidad*, núm. 3, 2020, pág. 3. El autor señala que el TEDH, en su sentencia *Barbulescu II* y *López Ribalda I* optó por la solución contraria y dio autonomía al principio de transparencia, pero que el *López Ribalda II* optó sorprendentemente por la solución contraria.

¹⁸ Como señala Rojo Torrecilla, «la tesis de la sentencia (...) eleva a los altares de la argumentación jurídica constitucional la protección del poder de dirección del empleador, reconocido legalmente en el art. 20.3 de la LET y que debe ponerse «en conexión con los arts. 33 y 38 CE», siendo así que de un plumazo el contenido esencial del derecho se sitúa en igualdad de condiciones que el poder de dirección del empleador. (...) La tesis del TC, extraordinariamente importante por la reformulación del poder de dirección del empleador en clave constitucional y muy poco respetuosa a mi parecer con el modelo que debe inspirar las relaciones de trabajo en el marco de un estado social y democrático de Derecho, (...) lleva (...) a colocar en igualdad de condiciones, a efectos de su ponderación, el contenido esencial de un derecho como el de protección de datos y por otro el poder de dirección, legal repito una vez [más], del empleador». Vid. ROJO TORRECILLA, E., «Después de las Jornadas Catalanas de Derecho Social. ¿Constitucionalización del poder de dirección empresarial en la relación de trabajo? Nota crítica a la sentencia del Tribunal Constitucional de 3 de marzo de 2016 (sobre instalación de cámaras de videovigilancia) (II)», en su blog «El nuevo y cambiante mundo del trabajo. Una mirada abierta y crítica a las nuevas realidades laborales», 21 de marzo de 2016.

¹⁹ En palabras de Goñi Sein, con dicha sentencia, «la falta de una información específica sobre la finalidad de control de la actividad laboral y su posible uso con fines disciplinarios, ya no comporta la invalidez de la prueba, ni excluye la validez del procedimiento sancionador, siempre que el empleado haya tenido conocimiento de la existencia de las cámaras. El deber de información ha terminado por poseer en nuestro país una relevancia meramente formal». Vid. GOÑI SEIN, J.L., «Vigilancia empresarial...», *ob. cit.*, pág. 202.

²⁰ Henríquez Tillería distingue hasta 2019 tres periodos en la jurisprudencia constitucional en el tema que estudiamos: un primer «periodo del principio de proporcionalidad» (SSTC 98/2000 y 186/2000); un «periodo de exigencia informativa estricta» (STC 29/2013) y un tercer «periodo de flexibilidad informativa» (STC 39/2016). Obviamente la STC 119/2022 se sigue inscribiendo en este tercer periodo y profundiza en él. Vid. HENRÍQUEZ TILLERÍA, S., «Protección de datos, videovigilancia laboral y doctrina de la sentencia López Ribalda II: un peligroso camino hacia la degradación de la obligación de información», en *IUSLabor*, núm. 3, 2019.



La jurisprudencia del TC se ha visto acompañada también de una jurisprudencia relevante del TEDH, especialmente en los últimos años. Es sobre todo, y sin perjuicio de la existencia de sentencias anteriores²¹, el caso de la STEDH de 5 de septiembre de 2017 (asunto *Barbulescu c. Rumanía, Gran Sala*), no referida a un caso de videovigilancia sino de control de los mensajes del trabajador en *Yahoo Messenger*, y que sirvió al TEDH, profundizando en el caso previamente resuelto por la Sala sobre idéntico asunto mediante sentencia de 12 de enero de 2016, para examinar los límites del control empresarial y su incidencia en la intimidad del trabajador, así como para fijar un test que permitiera abordar estos casos mediante el examen de una serie de elementos que vienen a recoger, entre otros, los propios del test de proporcionalidad y le añaden la información al trabajador y la previsión en el sistema estatal de un recurso judicial a disposición de este (§121). Por ello, si en la sentencia *Barbulescu I* de 2016 se había desestimado la existencia de vulneración del derecho a la protección de la vida privada que enuncia el art. 8 CEDH, en la *Barbulescu II* de 2017, en aplicación del mencionado test y de los diversos elementos que integra, se llega a la conclusión opuesta y a declarar por tanto dicha vulneración²².

En segundo lugar, son igualmente relevantes las sentencias del caso *López Ribalda*, estas ya sí en un caso de videovigilancia en el ámbito laboral: la STEDH de 9 de enero de 2018 (*López Ribalda y otros c. España, asuntos 1874/13 y 8567/13, Sala*), y la STEDH de 17 de octubre de 2019 (ídem, *Gran Sala*): la sentencia *López Ribalda I* consideró que la videovigilancia mediante cámaras ocultas realizada sin previa información a los trabajadores había vulnerado su derecho del art. 8 CEDH, mientras que la *López Ribalda II* concluyó un año después lo contrario, al atenuar la relevancia de dicha información como veremos más adelante.

Esta breve exposición del itinerario normativo y jurisprudencial del tema tratado nos permite tener ya el contexto necesario para abordar los principales aspectos de interés que, tras la última jurisprudencia constitucional, se plantean en el asunto que tratamos, pues tales aspectos traen causa lógicamente de ese itinerario previo.

²¹ Como por ejemplo *Köpke c. Alemania*, asunto 420/07, de 5 de octubre de 2010.

²² Como señala García Rubio, la sentencia *Barbulescu II* aún a través de estos criterios dos elementos: el tradicional examen del principio de proporcionalidad y el elemento de la información previa dada por la empresa al trabajador, siendo este segundo componente del canon el elemento novedoso que aporta la sentencia. Vid. GARCÍA RUBIO, M.A., «Control tecnológico...», *ob. cit.*, págs. 24-26. También sobre la concurrencia de ambos elementos en la jurisprudencia del TEDH y del TC Vid. LAHERA FORTEZA, J., «Videovigilancia laboral y grabación de sonidos en el lugar de trabajo», en *Revista del Ministerio de Trabajo y Economía Social*, núm. 148, 2021, págs. 261 y ss.



II. La devaluación del significado de la información en el ámbito laboral y sus efectos indeseados. ¿Puede la negligencia o la mala fe del empresario a la hora de aplicar la normativa sobre protección de datos ser utilizada en su propio beneficio? El caso de la STC 119/2022

Como ya se indicó antes, la LOPDGD de 2018 regula específicamente en su art. 89.1 el deber de información desde un esquema de regla y excepción. La regla es la información previa y de forma expresa, clara y concisa por parte del empresario a los trabajadores acerca de la videovigilancia²³, y la excepción, aplicable en caso de captación de la comisión flagrante de un acto ilícito, sería la suficiencia de la existencia de un distintivo informativo de la videovigilancia²⁴. Queda clara, por tanto, la voluntad de la ley de poner en un primer plano a modo de regla general el deber de informar, cosa lógica pues, no requiriéndose el consentimiento del trabajador, es la información al mismo lo único que va a posibilitar que este pueda ejercer sus derechos.

Así como la regla está pensando en toda clase de cámaras colocadas de manera estable y que tienen (entre otras, porque pueden también cumplir funciones de seguridad) la finalidad de controlar a los trabajadores²⁵, la excepción se aplica a cámaras colocadas frente al público en general con finalidad de preservación de la seguridad pero que han captado casualmente un acto ilícito del trabajador (doctrina del hallazgo casual). Queda la duda de si puede integrarse también o no en dicho régimen de excepción el supuesto de la cámara oculta que se coloca *ad hoc* al tenerse sospechas de que un trabajador esté realizando una actividad ilícita, modalidad esta de videovigilancia encubierta que no encuentra regulación expresa en la nueva ley²⁶.

²³ Incluyendo, como señala García Rubio, «la referencia a la finalidad del tratamiento, (...) que implica indicar que la videovigilancia está dirigida al control laboral, con los posibles efectos sancionadores que pueden derivar». Vid. GARCÍA RUBIO, M.A., «Control tecnológico...», *ob. cit.*, pág. 34. Vid. asimismo sobre las características de la información el art. 12 RGPD (Reglamento UE 2016/679).

²⁴ Distintivo o rótulo regulado en el art. 3 de la Instrucción 1/2006 de la AEPD, cuyo anexo indica que deberá contener una referencia a la ley reguladora, a la finalidad de tratar los datos y la mención a quién es el responsable ante el que pueden ejercitarse los derechos propios de la protección de datos.

²⁵ En sentido favorable a esta interpretación *vid.* ALTÉS TÁRREGA, J.A., «La videovigilancia encubierta en la nueva regulación sobre derechos digitales laborales y la incidencia de la STEDH López Ribalda (II)», en *Revista General de Derecho del Trabajo y de la Seguridad Social*, núm. 55, 2020, págs 334-335. En contra, sosteniendo que no cabe videovigilancia con finalidad de control laboral, sino solo de seguridad en general, de modo que el control laboral solo sería posible por vía indirecta (hallazgo casual de un acto ilícito registrado en las grabaciones de seguridad), *vid.* BAZ RODRÍGUEZ, J., «La Ley Orgánica 3/2018 como marco embrionario de garantía de los derechos digitales laborales. Claves para un análisis sistemático», en *Trabajo y Derecho*, núm. 54, 2019, págs. 9-11. Sin embargo, el propio tenor literal del art. 89.1 LOPDGD aboga en favor de la videovigilancia con fines de control laboral.

²⁶ En opinión de Lahera Forteza, para el caso de la cámara oculta puesta tras la existencia de sospechas, caso no regulado expresamente en la ley, la solución oscilaría, a su juicio, entre tres posi-



Se corrige con ello en la LOPDGDD, redimensionándola, la solución que había dado por buena la STC 39/2016, que apartándose netamente de la 29/2013 acogió la opción del distintivo como medio de dar información al trabajador con carácter general. Decimos que se corrige y redimensiona porque en la LOPDGDD, para dar por buena la opción del distintivo, se exige que haya habido captación de la comisión flagrante de un acto ilícito por parte del sistema de grabación, requisito este que no se mencionaba en la sentencia de 2016, que aceptaba sin limitaciones la solución del distintivo como sustitutivo de la información expresa, y que por ello iba mucho más allá de lo que iría la ley aprobada dos años después. La LOPDGDD, a diferencia de la sentencia de 2016, parte de la información previa, clara y expresa como regla inicial, y también encaja esta solución legal de 2018 con la atenuación del valor del deber de informar que se había plasmado en la STEDH López Ribalda contra España (Gran Sala) de 17 de octubre de 2019 (López Ribalda II), que no va tan lejos como la sentencia del TC de 2016, pero que, tras tomar en consideración una serie de elementos (la legitimidad de la instalación del sistema de videovigilancia a partir de la sospecha por parte del empresario de la comisión de actos ilícitos, el alcance —geográfico, temporal— de la vigilancia, su necesidad y sus consecuencias) concluyó que la infracción del deber de informar sería «solo uno de los elementos a tener en cuenta» junto con el resto de criterios ya mencionados a la hora de ponderar la licitud o no de la medida. La consecuencia de que no se hubiera cumplido con ese deber de informar sería, para el TEDH, que el resto de elementos ponderativos adquirirían «una particular relevancia» (§131) y ello significará que «solo un requisito primordial relativo a la protección de intereses públicos o privados importantes podría justificar la falta de información previa» (§133).

bilidades: (a) considerar inaceptable esta modalidad de videovigilancia en todos los casos; (b) considerarla admisible si supera en el caso concreto un test de proporcionalidad como el usado por el TEDH, o (c) aplicar por analogía la solución del distintivo del art. 89 (aparte de la necesidad de superar el test). El autor se decanta por la segunda opción (superación del test), aunque limitando el uso de estas cámaras ocultas a la detección de actos delictivos de cuya comisión se haya tenido sospecha. *Vid.* LAHERA FORTEZA, J., «Videovigilancia...», *ob. cit.*, págs. 272 y ss. Con todo, con ello se debilita aún más el deber de información y estimo preferible aplicar además, aunque los supuestos sean distintos (el hallazgo aquí no es casual) el régimen de la excepción que prevé el art. 89 de la ley, lo que tampoco resulta muy gravoso para la empresa, a la que poco le costaría incluso ir más allá de la colocación de un distintivo y notificar a los trabajadores, por ejemplo al firmarse el contrato con cada uno de estos, que en el futuro podrían colocarse cámaras ocultas con finalidades también de control laboral. *Vid.* también, sobre los pros y los contras de aplicar a estos casos el régimen del hallazgo casual ALTÉS TÁRREGA, J.A., «La videovigilancia...», *ob. cit.*, págs. 357 y ss. En la jurisprudencia ordinaria resulta de interés por su claridad la STSJ de Galicia de 15 de febrero de 2021 (rec. 4586/2020), que excluye la posibilidad de admitir una grabación obtenida tras instalar cámaras luego de tener sospechas si no se colocó debidamente el distintivo, no bastando, además, uno colocado a la entrada de la empresa, alejado del lugar donde se iba a grabar, ya que no existía «una continuidad entre todos los espacios a los cuales se puede acceder desde la visualización del dispositivo informativo» (FJ 3).



Dicho deber de información se configura, pues, como un deber no imprescindible, sino sustituible en ciertos casos por la concurrencia de otros elementos²⁷. La solución legal de 2018 de admitir en el supuesto indicado (comisión de un acto ilícito flagrante) una información de carácter genérico, no dirigida específicamente a los trabajadores sino al público en general y plasmada en la existencia de un rótulo, sería coherente con esa concepción atenuada del deber de informar aplicable en determinadas circunstancias, circunstancias que la sentencia del TEDH cifra en la protección de los mencionados intereses públicos o privados importantes y que la LOPDGDD de 2018 por su parte identifica con el supuesto de captación de la comisión flagrante de actos ilícitos que perjudican lógicamente tales intereses: lo que hace la ley, pues, es dar por válido un supuesto de concurrencia de otros intereses relevantes que permitan atenuar el deber de información, pero al mismo tiempo debiera concluirse que ha excluido cualesquiera otros supuestos distintos²⁸, y que ha configurado dicho supuesto como única excepción a la regla de informar de manera expresa, clara y concisa, matiz importante por lo que luego se dirá²⁹.

²⁷ Como señala Hernández Tillería, «la sentencia de la Gran Sala realiza un tratamiento bastante particular o difuso de la obligación de informar la implementación de sistemas de videovigilancia. Flexibiliza la contravención de este deber legal, al crear una explícita exención de responsabilidad frente a su incumplimiento, siempre que se den ciertas condiciones fácticas, vinculadas al cumplimiento del principio de proporcionalidad —con mayores exigencias y una ponderación más severa—. Esto acarrea una importante carga de incertidumbre jurídica, por tratarse de una ponderación *ex post* de la proporcionalidad de la medida», *Vid. HERNÁNDEZ TILLERÍA, S., «Protección de datos...», ob. cit., pág. 73.*

²⁸ En este sentido, el voto particular de los magistrados Xiol Ríos, Conde-Pumpido Tourón, Balaguer Callejón, Sáez Valcárcel y Montalbán Huertas a la STC 119/2022 hace notar que «el nuevo marco normativo establecido por el art. 89.1 de la Ley Orgánica 3/2018, también incide en la jurisprudencia constitucional establecida en la STC 39/2016, desautorizando la posibilidad del cumplimiento ordinario del deber de información a los trabajadores mediante la mera información genérica dada al público», por cuanto dicho cumplimiento a través del rótulo o cartel ya solo será posible en el concreto caso que indica la ley, y no en cualquiera.

²⁹ Algún sector doctrinal ha considerado, no obstante, que esa decisión de la ley en los casos de acto ilícito «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, ni tampoco las exigencias del deber informativo que impone el Reglamento Europeo de Protección de Datos Personales. En tal caso, el juez español debe extraer las consecuencias del incumplimiento de las exigencias y garantías citadas y determinará la nulidad de la prueba obtenida por vulnerar un derecho fundamental», proponiendo también que el juez inaplique el art. 89 LOPDGDD por incompatible con el RGPD de la UE. *Vid. ECHEVARRÍA DE RADA, M.T., «Protección de datos y Videovigilancia en el ámbito laboral», en Actualidad Civil, núm. 9, 2019, pág. 18. También, más extensamente, GONZÁLEZ GONZÁLEZ, C., «Control empresarial de la actividad laboral mediante la videovigilancia y colisión con los derechos fundamentales del trabajador. Novedades de la Ley Orgánica 3/2018», en Revista Aranzadi Doctrinal, núm. 4, 2019, págs. 103-142. Igualmente muestra dudas sobre la compatibilidad del art. 89.1 LOPDGDD con el RGPD MOLINA NAVARRETE, C., «¿Son legítimos...», *ob. cit.*, pág. 5. Con todo, a la vista del RGPD, de lo que dispone la LOPDGDD y de la propia jurisprudencia del TEDH (sobre todo con la López Ribalda II) dicha opinión puede resultar un tanto excesiva, y no ha tenido reflejo tampoco en la jurisprudencia, más allá de una concreta sentencia del Juzgado de lo Social núm. 3 de Pamplona de 18 de febrero de 2019, ni en la mayor parte de la doctrina que ha tratado el tema.*



En tal supuesto, pues, el legislador ha realizado una ponderación entre los derechos e intereses en juego y ha optado por la posibilidad de atenuar sustancialmente el deber de información a los trabajadores, que deja de tener las características que en principio debiera reunir para poder ser satisfecho a través de la presencia del mencionado cartel dirigido al público³⁰. Con todo, parece que las excepciones como la del art. 89.1 han de tomarse como tales, y no pueden erigirse en sustitutivas de la regla o dar pie a que el empresario, por propia voluntad y no habiendo obrado, en lo referido al deber de informar, conforme a las exigencias de la buena fe³¹, acabe liberándose de la regla y beneficiándose de manera permanente de la excepción, como sucede en el caso resuelto por la STC 119/2022 y en la solución a la que en ella llega el TC.

En el caso examinado por la STC 119/2022 se dan dos circunstancias de interés: la primera, que la empresa había colocado en lugar visible un distintivo relativo al sistema de videovigilancia conforme establece la normativa sobre protección de datos; la segunda, que en 2014 se había despedido a un empleado a resultas de haberse comprobado en las grabaciones del sistema de videovigilancia que había cometido una conducta ilegal. Ambas circunstancias abonarían la tesis de que los trabajadores no podían ser desconocedores de que la empresa realizaba en sus instalaciones grabaciones de imágenes. Pero es un conocimiento derivado de los mencionados hechos, y no de que en ningún momento la empresa hubiera informado de manera específica a los trabajadores acerca de su actividad de videovigilancia: no se cumplió la regla de tener que informar de manera previa y de forma expresa, clara y concisa sobre dicha actividad, y ello pese a que, por ejemplo, entre el despido de 2014 y la comisión de los hechos que dieron lugar en 2019 al despido de que trae causa la sentencia de 2022, la empresa tuvo la apreciable cantidad de cinco años para llevar a cabo correctamente dicha información. Si no lo hizo, pues, fue por negligencia, cuando no por mala fe.

La pregunta que cabe plantearse es si, constatándose de manera tan obvia que ha existido como mínimo negligencia por parte de la empresa en el cumplimiento de sus deberes durante un muy prolongado plazo de

³⁰ Como señala Lahera Forteza, «el art. 89 LOPD, norma específica frente al art. 22 LOPD es, en consecuencia, resultado de una ponderación jurídica, ya mostrada por el TC y TS, entre los arts. 38 y 33 CE, y su manifestación legal en el art. 20 ET —poder contractual de control de la empresa— y los arts.18.1 y 4 CE, y su manifestación legal en el art. 4.2.e ET». *Vid.* LAHERA FORTEZA, J., «Videovigilancia...», *ob. cit.*, pág. 267. Otra cosa es, lógicamente, determinar como ya se dijo anteriormente si los dos platos de la balanza están en pie de igualdad o si estamos ponderando entre grupos de normas de distinto peso.

³¹ Sobre las obligaciones que del principio de buena fe debieran derivarse para el empresario en relación con el deber de informar a los trabajadores *vid.* RODRÍGUEZ ESCANCIANO, S., *Poder de control empresarial, sistemas tecnológicos y derechos fundamentales de los trabajadores*, Tirant lo Blanch, Valencia, 2015, págs. 137-141.



tiempo, ello debiera beneficiarla de alguna forma. Es una pregunta, por lo demás, que ha estado presente durante el enjuiciamiento del caso en la vía ordinaria: en primera instancia el Juzgado de lo Social optó por no dar relevancia a esa negligencia y dar por bueno el hecho de que los trabajadores tuvieran (o pudieran tener) *de facto* la información por las circunstancias antes mencionadas (el distintivo, el despido de cinco años antes) aplicando, pues, sin más la vía de la excepción legalmente prevista; no habría por tanto vulneración de derechos y la grabación sería admisible como prueba lícita. Por el contrario, la sentencia del TSJ del País Vasco resolviendo el recurso de suplicación partió de presupuestos más estrictos y más atentos con la efectividad de los derechos en juego: aun existiendo un distintivo que, en este caso, pudiera servir para activar la excepción a la regla de informar de manera previa, clara, precisa y expresa, la existencia del despido cinco años antes a partir de una videograbación y el hecho de que ni siquiera entonces, ni durante esos cinco años, la empresa hubiera procedido a subsanar su incumplimiento del deber de informar, llevan a que la Sala de lo Social del mencionado TSJ entienda que lo que la empresa está haciendo 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», lo que lleva al TSJ a considerar ilícita la prueba por cuanto el uso de esas imágenes habría vulnerado el «derecho a la intimidad del trabajador», si bien hubiera sido más correcto a mi juicio que se hubiera referido el TSJ al derecho a la protección de datos, como señala el TC en su FJ 6b al glosar la conclusión a que llega la sentencia del TSJ³².

El TC se alinearán con la tesis del Juzgado de lo Social, a partir de la consideración de dos elementos. En primer lugar, para el TC, el hecho de que el trabajador, que estaba en la empresa desde 2007, conociera los hechos que condujeron al despido de 2014 es algo que no excluye «la responsabilidad de la empresa en el incumplimiento de su deber de información» (FJ 6b). Pero en segundo lugar, sin embargo, dicha no exclusión queda en la práctica en nada, pues de la misma «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 misma medida» (FJ 6b). Por tanto, que el empresario no hubiera informado correctamente durante años pudiendo (y debiendo) hacerlo se da como irrelevante en la práctica.

³² Sobre las cuestiones de índole procesal relativas a la presentación de la grabación de video como prueba en el litigio laboral *vid.* en detalle VALLE MUÑOZ, F. A., «Las cámaras de videovigilancia en la empresa como medio de prueba en el proceso laboral», *IUSLabor* 3, 2021, págs. 31-59.



Que se abra la puerta de este modo a la utilización de la excepción que el art. 89.1 añade a la regla supone, como señala el voto particular, situar «a ambas en un mismo nivel axiológico y desvirtúa con ello el esfuerzo legislativo por dotar de un régimen de garantía a este tipo de medidas» (apartado 16). Y desconoce el TC, con ello, que la voluntad del legislador es que la información a los trabajadores sobre la existencia de una videovigilancia que pueda ser usada con fines de control laboral sea, como regla, específica para ellos, y no la misma información que pueda darse al público en general; esto último solo debe ser posible como excepción, en un caso concreto, y sin que lógicamente esa excepción pueda, a elección del empresario, convertirse en regla. Lo contrario sería, en palabras también del voto con las que coincidimos, ignorar la «garantía material del derecho fundamental, que no consiente una dejación o desatención continuada en su estricto cumplimiento por parte del empleador cuyos posibles abusos tiene por objeto contener» (apartado 16), dejación continuada que, de darse, debería tener consecuencias en orden a no admitirse la prueba así obtenida.

Por lo demás, poco parece cohonestarse con el deber de buena fe que ha de presidir la relación contractual laboral que el empresario pueda, sin consecuencia alguna para él, desatender un deber legal³³, lo que en la práctica hará que el elemento de la información como componente del derecho fundamental del art. 18.4 CE quede reducido a un plano meramente simbólico, hasta casi desaparecer, y se sustituya la atención al respeto del contenido esencial del derecho por un juicio de ponderación en el que será difícil no encontrar alguna argumentación que apoye la decisión empresarial, bastando para ello con que existan meras sospechas acerca de que se pueda haber captado la comisión de un acto ilícito y pudiéndose a partir de ahí darse por satisfechos con facilidad los criterios del test de proporcionalidad³⁴, de manera que se considere que el incumplimiento

³³ En el voto particular del magistrado Valdés Dal-Ré a la STC 39/2016 aquél manifestaba sus dudas sobre «la verdadera finalidad a la que atiende la doctrina sentada [en dicha STC de 2016] que enuncio en términos interrogativos: ¿se pretende asegurar un control legítimo por el empresario de la actividad laboral, con respeto a las garantías legales y a los derechos fundamentales o, por el contrario y más bien, se busca habilitar controles sorpresivos, que permitan identificar in fraganti a un trabajador que no cumpla debidamente su contrato? Si fuera esto último, como lamentablemente así me lo parece, no alcanzo a entender la conexión entre esa intención, no ya de controlar sino de «atrapar» al trabajador, con la libertad de empresa o el derecho a la propiedad que consagra la Constitución». Parece a mi juicio claramente preferible este enfoque al de algún sector doctrinal que, como en el caso de Desdentado Bonete y Muñoz Ruiz, consideran que dar primacía al deber de información constituiría un «formalismo enervante» o «una vía para eludir controles lícitos, [o] para lograr la inmunidad de conductas censurables». Vid. DESDENTADO BONETE, A., y MUÑOZ RUIZ, A.B., «Trabajo, videovigilancia...», *ob. cit.*, pág. 16.

³⁴ Vid. en tal sentido GOÑI SEIN, J.L., *La videovigilancia empresarial y la protección de datos personales*, Thomson Civitas, Madrid, 2007, págs. 44-50. Señala el autor cómo siempre se podrá considerar que la medida de colocar cámaras fue idónea para la prevención y persecución de actos ilícitos,



del deber de informar no alcanza a tener relevancia constitucional, de modo que pasarán a ser tratadas igual en todos esos casos las personas ajenas a la empresa que tendrán con esta un contacto puntual y los trabajadores de la misma, vinculados contractualmente a ella de manera estable: parece difícil pensar que la idea del legislador en 2018 fuera esa³⁵.

Esa misma buena fe a la que aludíamos se pone también en duda en función de cómo se ubique el distintivo. Es decir, como señala García Rubio, es relevante concretar el «alcance “espacial” del dispositivo informativo (...). Así, por ejemplo, si a la entrada de un centro de trabajo se coloca el cartel informativo de videovigilancia, cabe preguntarse a qué dependencias —a todas o algunas— se extiende la posibilidad de entender cumplido el requisito de información previa en caso de constatar en ellas un ilícito laboral». La autora recuerda cómo la jurisprudencia ordinaria ha examinado casos en que, por la estructuración del centro de trabajo en dependencias autónomas o diferenciadas, a algunas de las cuales accede el público y a otras no, resultaría excesivo entender que un cartel en un punto de entrada las cubre a todas³⁶. Tampoco la sentencia de 2022 da respuesta a esta cuestión, lo que teniendo en cuenta la devaluación del deber de informar que la misma supone puede llevar a que dicha información devenga aún más irrelevante en la práctica.

III. Entre la flagrancia y la mera sospecha. ¿Qué autoriza a acudir a las grabaciones realizadas? El concepto de acto ilícito

De la sentencia analizada se desprenden otras cuestiones de interés y otros riesgos para la real aplicación de la actual regulación legal. El TC considera en su sentencia que las cámaras se usaron para «comprobar un hecho concreto, que resultó flagrante, y sobre la base de una sospe-

siempre podrá decirse que fue necesaria para obtener pruebas de estos, y en cuanto a la proporcionalidad en sentido estricto, salvo que la actuación empresarial haya sido muy burda en su alcance y características, tampoco resultará difícil de cumplimentar, aunque dependerá de cada caso y del criterio judicial. En parecido sentido se pronuncian en su voto particular a la STC 39/2016 los magistrados Valdés Dal-Re y Asua Batarrita: «Con semejante proceder metodológico, el contenido esencial (...) se diluye y la razón empresarial termina siempre imponiéndose, pues en la práctica totalidad de los conflictos entre las dos partes del contrato de trabajo resulta una tarea sencilla el crear recursos dialécticos para su empleo en una lógica de proporcionalidad» (apartado II.a.3).

³⁵ Debemos por ello coincidir con García Rubio cuando señala que «ahora [tras la ley de 2018] ya contamos con una regulación legal específica [sobre videograbaciones] en el ámbito de las relaciones laborales; supuestamente, por tanto, las empresas tienen una mayor seguridad jurídica sobre lo que deben y pueden hacer; y lo que no tendría sentido es que, por la vía de hacer interpretaciones amplias de las excepciones, se acabara haciendo perder virtualidad a la Ley y a las garantías que con ella se han querido instaurar». Vid. GARCÍA RUBIO, M.A., «Control tecnológico...», *ob. cit.*, pág. 44.

³⁶ Vid. GARCÍA RUBIO, M.A., «Control tecnológico...», *ob. cit.*, pág. 35. Resulta ilustrativo de ello la mencionada STSJ de Galicia de 15 de febrero de 2021 (rec. 4586/2020), FJ 3.



cha indiciaria concreta», lo que hace que resulte «válida la utilización de las imágenes captadas para verificar una conducta ilícita cometida por un trabajador» (FJ 6b)³⁷. Dicha sospecha se le habría suscitado al gerente «al haber apreciado el día anterior que, en la zona interior del mostrador de atención al público donde prestaba servicios el trabajador despedido, se encontraba una bolsa con el signo identificativo de una empresa de la competencia, conteniendo en su interior un producto de su propia empresa. Cuando, al final de la jornada del día siguiente, observó que la bolsa no se encontraba en ese lugar, y ante lo irregular de la situación, comprobó la grabación de ese día, advirtiendo la conducta determinante del despido» (antecedente de hecho 2). Dicha conducta constatada en la grabación consistió en que el trabajador entregó «unos productos propiedad de la empresa (...) a un tercero que le abona un dinero en metálico del que [aquél] se apropia, absteniéndose de entregar albarán de entrega ni recibo de pago alguno» (ídem).

Obsérvese, pues, cómo se partía de una sospecha (por lo demás débil, sin que quepa fácilmente inferir qué proceso deductivo lleva a vincular la presencia o ausencia de una bolsa con la comisión de un acto ilícito) y cómo el TC señala que el acto ilícito «resultó flagrante», es decir, la «flagrancia» (o el concepto *sui generis* de la misma que se sostiene) no se afirma hasta que, llevado el gerente por esa sospecha que de tan débil el propio TC la califica de «indiciaria concreta», procede al visionado del sistema de grabación, un sistema del que en cinco años la empresa no había considerado oportuno dar noticia expresa a los trabajadores.

Observamos, pues, cómo el concepto de flagrancia, como mecanismo de activación de la excepción al deber de informar de manera clara, precisa y expresa, cobra toda su relevancia. Y en este punto nos encontramos con una noción de flagrancia distinta a la propia de otros ámbitos como el penal: flagrante será todo aquello que haya quedado grabado por una cámara, y a dicha grabación se podrá acceder a posteriori siempre que haya una sospecha, que por otra parte se permite que sea meramente indiciaria. El resultado es que la flagrancia deja de ser algo que

³⁷ Tampoco desde la perspectiva del derecho a la intimidad considera el TC que haya vulneración pues la medida resultaba a su juicio justificada, idónea, necesaria y proporcionada en sentido estricto. En relación con la admisión de la grabación como prueba, por otra parte, el voto particular sostiene que el TC debió de haberse limitado a examinar si su inadmisión por parte del TSJ resultó inmotivada y arbitraria, lo que hubiera conducido a concluir que no y a validar dicha inadmisión. Ir más allá de esto y analizar el derecho de prueba de la empresa demandante no desde el indicado parámetro de motivación suficiente y adecuada sino desde la perspectiva del examen de si la aplicación del derecho del trabajador fue correcta o no, como hace la sentencia, resultaría, a juicio de los magistrados que emiten el voto, erróneo y alteraría la naturaleza del recurso de amparo, que debe dirigirse a comprobar si ha habido vulneración de un derecho fundamental (en este caso, el derecho de prueba de la empresa demandante frente a la inadmisión de dicha prueba por el TSJ) y no a analizar el entendimiento que el TSJ hizo del derecho a la protección de datos.



mientras ocurre es percibido por alguien a través de los sentidos, para pasar a ser cualquier cosa que haya quedado registrada en la grabación, a la que se podrá acceder no cuando alguien haya presenciado el acto sino cuando desde la empresa se albergue una mera sospecha, en tanto que esta abrirá la puerta a comprobar en diferido mediante el visionado de la grabación si esta había registrado un determinado acto, sirviendo al mismo tiempo dicha sospecha, combinada con esa concepción de la flagrancia, para excusar el deber de informar al trabajador de manera clara, precisa y expresa de la existencia de mecanismos de videovigilancia.

Se constata, pues, que a una idea más clásica de flagrancia (una persona contempla o escucha cómo otra realiza un acto ilícito de modo que en un caso como este, sobre la base de esa percepción directa y para re-frendarla, se acudiría al visionado de la grabación) la sustituye otra concepción, digamos, de naturaleza tecnológica: no hay flagrancia en lo que se ha visto u oído (pues no se ha visto u oído a nadie realizar un acto ilícito, sino que meramente hay sospechas de tal realización) y la flagrancia se va a buscar, días o semanas después, al visionado de la grabación; quien ha «contemplado» los hechos, pues, es la cámara. Una flagrancia, por tanto, en diferido y a cuya verificación se puede acceder casi libremente, sin otro requisito que el de poder aportar algún tipo de sospecha, por leve que sea.

Así, lo que en la regulación de 2018 se pretende ganar por un lado en cuanto a limitar el acceso indiscriminado a las imágenes y potenciar el deber de informar (quedando la solución del distintivo como excepción pensada para un determinado supuesto) se pierde por otro, pues todo es flagrante aunque nadie lo haya visto (ya lo habrá visto la cámara), cualquier sospecha da lugar a poder visionar las grabaciones³⁸, y el deber de informar debidamente se convierte así en plenamente voluntario para el empresario: con colocar un distintivo en alguna pared, aquél ya gana, *de facto*, acceso general a todo cuanto grabe. ¿Era este el propósito del legislador? No lo parece. Con la solución a la que llega la sentencia, tal como señala el voto particular a la misma, «se ha configurado un estándar que prácticamente anula esa garantía [de información al tra-

³⁸ Como señalan los magistrados De Gaetano, Yudkivska y Grozev en su voto particular a la STEDH López Ribalta II, dar como suficiente «la existencia de «una sospecha razonable de que se ha cometido una falta grave» (...) puede dar lugar a investigaciones privadas y podría utilizarse como justificación en un número inaceptablemente elevado de casos. Si bien, en principio, el requisito de la «sospecha razonable» es una salvaguardia importante, no es suficiente para proteger los derechos de privacidad cuando se enfrenta a una vigilancia electrónica de carácter encubierto». También en tal sentido incide Henríquez Tillería, para quien «ante las llamadas sospechas razonables de comisión de delitos, se opta por una medida altamente intrusiva, la videovigilancia oculta, actuando así la empresa como un verdadero ente persecutor, pero con poca o nula fiscalización inmediata de los poderes públicos, y con bajos estándares de garantía de derechos de los afectados». HERNÁNDEZ TILLERÍA, S., «Protección de datos...», *ob. cit.*, pág. 76.



bajador] por la desmesurada extensión que se da a las posibilidades excepcionales de su modulación en caso de flagrancia» (apartado 18)³⁹. Como ha señalado Beltrán de Heredia, en definitiva, «el criterio seguido por la opinión mayoritaria ha vaciado de contenido al art. 89.1 LO 3/2018 (relegándolo a un mero formalismo)» lo que puede facilitar «un efecto perverso, al debilitar los efectos del incumplimiento empresarial del deber general de información y, por consiguiente, los incentivos para cumplir con él»⁴⁰. Así pues, el TC, lejos de poner el derecho fundamental del art. 18.4 CE en el centro de su argumentación y fijar en todo caso una interpretación restrictiva de la excepción que posibilita el art. 89 de la ley⁴¹,

³⁹ Por ello el voto afirma igualmente que no debe bastar con «que se verifique que concurre una situación de flagrancia en la captación de la imagen y la presencia en el lugar de trabajo de los carteles anunciadores de la existencia del sistema para legitimar, desde la perspectiva del art. 18.4 CE, el uso de esa imagen con fines disciplinarios. Será preciso, además, en atención a la naturaleza esencial y principal del deber específico de información a los trabajadores, en cuanto garantía del derecho fundamental, que se den cumplidas razones por parte del empleador respecto de su incumplimiento. En un sentido contrario, se estaría poniendo en un mismo nivel valorativo la regla general y la excepción. Además, contra la voluntad del legislador orgánico, se estaría propiciando que el empleador optara por el incumplimiento continuado de la regla general del deber específico de información a sus trabajadores fiándolo todo, ante la existencia de carteles genéricos informativos, a la eventual concurrencia de la flagrancia en la captación para legitimar el uso disciplinario de las imágenes obtenidas». Ello, además, «puede producir el efecto de abrir las puertas a la utilización de videovigilancia oculta absoluta, dado que la calificación de las circunstancias en que se pondera su contenido es esencialmente casuístico, y requiere una ponderación y control judicial necesariamente ex post». Vid. HERNÁNDEZ TILLERÍA, S., «Protección de datos...», *ob. cit.*, págs. 74 y 78.

⁴⁰ Vid. BELTRÁN DE HEREDIA RUIZ, I., «Cámaras de vigilancia, intimidad y protección de datos: prueba lícita y despido procedente (STC 119/2022)», en el Blog «Una mirada crítica a las relaciones laborales», 25 de octubre de 2022m pág. 16 (accesible en: ignasibeltran.com/2022/10/25/camaras-de-vigilancia-intimidad-y-proteccion-de-datos-prueba-licita-y-despido-procedente-stc-119-2022/). También Baz Rodríguez señala a mi juicio acertadamente que «la aplicación generalizada e inmatizada de esta previsión normativa a los supuestos de videovigilancia ordinaria (esto es, a la genérica puesta en marcha tales sistemas como mecanismos disuasorios, sin haberse producido previamente quiebra alguna de la seguridad) acabaría vaciando de facto el deber general de información en los términos previamente proclamados en el primer párrafo del artículo 89.1, aniquilando completamente la interpretación adaptativa y tutelar de los principios de transparencia y de lealtad efectuados por la norma laboral: la eventual constatación a posteriori de una conducta ilícita acabaría blanqueando o regularizando, de hecho, la puesta en marcha inicialmente irregular de un sistema de videovigilancia sin información previa y expresa a los trabajadores y a sus representantes». Vid. BAZ RODRÍGUEZ, J., «La Ley Orgánica...», *ob. cit.*, pág. 12.

⁴¹ Interpretación restrictiva que algún sector doctrinal ha intentado fijar reservando la excepción del art. 89 para los casos de cámaras instaladas *ad hoc* tras la constatación de sospechas de acto ilícito que se atribuye a un trabajador (además, se debería superar el test de proporcionalidad a partir de la consideración de su alcance temporal, subjetivo, etc.); tal es la propuesta de BAZ RODRÍGUEZ, J., «La Ley Orgánica...», *ob. cit.*, pág. 13. No cabría, así, tener con carácter permanente un sistema de grabación al que se fuera accediendo cada vez que hubiera una sospecha, sino que dicho sistema debe instalarse a partir de generarse la sospecha y por el tiempo necesario para hacer la averiguación en torno a la misma; un control defensivo, en palabras del propio autor, «ex post» y «en concreto», frente al «ex ante» y «en abstracto» de la videovigilancia ordinaria. Una tesis como la propuesta por este autor hubiera podido servir al TC para resolver este caso de manera más consciente con el valor del derecho fundamental en juego. También en semejante sentido vid. GARCÍA-PERROTE ESCARTÍN, I., «A proba no proceso laboral: algúns puntos críticos recentes», en *Revista Galega de Dereito Social*, num. 13, 2021, pág. 26.



lo que ha hecho es posibilitar que dicha excepción devenga la regla, a elección del empresario.

Los efectos amplificadores que posibilita un concepto extensivo de flagrancia combinado con el elemento de la sospecha se pueden asimismo intensificar aún más si ampliamos también el concepto de acto ilícito. Es decir: además de que permita acudir a las grabaciones la existencia de la sospecha de que se haya cometido un ilícito penal, ¿podría también autorizar a recurrir a ellas el hecho de que se sospeche que el trabajador ha llevado a cabo alguna conducta no relevante penalmente sino solo desde el punto de vista laboral, merecedora de una sanción disciplinaria por parte de la empresa? De ser la respuesta afirmativa, las cámaras (meramente identificadas con un distintivo) y esa flagrancia «difundida», permitirían controlar cualquier caso de incumplimiento laboral. Aunque el concepto de «acto ilícito» que emplea la ley admite una interpretación que lo lleve más allá de lo penal (lo que se está poniendo de manifiesto en algunas sentencias aunque de momento la jurisprudencia está ofreciendo en este punto respuestas dispares⁴²) no es menos cierto que en tal caso el empresario pierde cualquier incentivo para cumplir con la regla del art. 89.1 LOPDGD (puede acogerse a la excepción para cualquier cosa, y fácilmente se superarán a la hora de enjuiciar su actuación los criterios de necesidad, adecuación y proporcionalidad en sentido estricto⁴³), y que por otra parte se induce a error al trabajador, que podía legítimamente creer que las cámaras están para prevenir problemas de seguridad con el público, pero no para la vigilancia laboral.

Las interpretaciones posibles en este punto son múltiples. Por un lado, la tesis indicada de que abrir el uso de esas cámaras a la captación de cualquier acto ilícito, incumplimientos laborales incluidos, frustraría fácilmente la finalidad de la ley de primar la información clara y expresa,

⁴² Señala García Rubio que la respuesta favorable a aceptar las grabaciones para fines no penalmente relevantes se aprecia desde 2017 y se manifiesta con especial claridad en sentencias como la del TS de 26 de abril de 2021 (Sala Tercera, al ser parte una administración frente a una funcionaria) en que se dio por bueno el uso de las grabaciones para acreditar incumplimientos en la jornada laboral. Pero al mismo tiempo se encuentran sentencias de diversos TSJs que desde 2019 sostienen la opción contraria y no admiten las grabaciones para finalidades meramente laborales en ausencia de información previa y expresa. *Vid.* sobre todo ello GARCÍA RUBIO, M.A., «Control tecnológico...», *ob. cit.*, págs. 37-39. La autora subraya la necesidad de realizar una interpretación restrictiva de los casos que pudiera abarcar la posibilidad de acceder a las grabaciones a partir del mero dispositivo.

⁴³ Considera Cuadros Garrido que en la jurisprudencia en esta materia «se utiliza la técnica [de la proporcionalidad] como un mero formalismo, pero sin justificación o argumentación material sólida y ello de por sí ya es suficiente para justificar la fiscalización de la prestación por videovigilancia». *Vid.* CUADROS GARRIDO, M.E., «A vueltas con la videovigilancia como control de la prestación laboral y el juicio de ponderación», en *Revista Justicia & Trabajo*, num. 1, 2022, pág. 91. No obstante, algunos autores consideran que una videovigilancia permanente y genérica de la actividad laboral no superaría dicho test. *Vid.* en tal sentido LÓPEZ BALAGUER, M. y RAMOS MORAGUES, F., «Derecho a la intimidad y a la protección de datos y licitud de la prueba en el proceso laboral», en MONREAL BRINGS-VAERD, E. *et al.*, *Derecho del trabajo y nuevas tecnologías*, Tirant lo Blanch, Valencia, 2020, pág. 408.



al tiempo que el trabajador puede verse confundido en relación con la finalidad de la utilización de cámaras, tesis sostenida, en mi opinión con buen criterio, entre otros por Goñi Sein⁴⁴ de modo que solo debieran poder perseguirse ilícitos penales. Una interpretación intermedia (que aunque no evitaría los riesgos que acaban de mencionarse intenta al menos limitarlos) y que sostienen López Balaguer y Ramos Moragues⁴⁵ sería la de considerar que podrían perseguirse las infracciones disciplinarias relevantes laboralmente (pero no penalmente) cuando afecten a la seguridad de personas y cosas, pero no cuando aludan a otras cuestiones ajenas a dicha seguridad (como el cumplimiento del horario de trabajo o el nivel de rendimiento del trabajador, por ejemplo). Por último, estaría la tesis que abogaría por permitir el uso de las cámaras de seguridad para captar ilícitos laborales sin mayores limitaciones: para Lahera Forteza, por ejemplo, «el término específico «control de los trabajadores» del art. 89 LOPD es más extensivo que la mera preservación de la «seguridad» del art. 22 LOPD y habilita, respetando los límites correspondientes, la instalación de cámaras con esta finalidad, sirviendo la imagen como prueba lícita de sanción o despido disciplinario», de modo que, por más que la medida deba cumplir con los requisitos que se estimen necesarios tendentes a no vulnerar la privacidad del trabajador o la protección de sus datos, «ello no conduce a restringir la cámara a supuestos de seguridad como robos de bienes o dinero a la empresa»⁴⁶.

La variedad de interpretaciones existentes en la doctrina es expresiva, pues, de una regulación escasa e insuficiente de la videovigilancia labo-

⁴⁴ Señala este autor que, aunque durante la tramitación parlamentaria de la ley se pasó de hablar de «acto delictivo» a «acto ilícito» (lo que podría abonar la inclusión de actos sin relevancia penal), ello sería rechazable por un doble motivo: «primero, porque no tendría sentido la doble regulación establecida [en la ley de 2018 cuando recoge la regla y la excepción en relación con el deber de información, pues si se incluye en esta lo no penal, el empresario no tendría por qué cumplir nunca con la regla], y segundo, porque no está amparado por el RGPD y se llegaría a una especie de quiebra del principio de finalidad», al tiempo que «cuando la medida de videovigilancia se adopta con fines de seguridad, se genera en los trabajadores una razonable expectativa de que las imágenes no serán utilizadas con fines laborales, que debe ser respetada. La extensión de la excepción prevista en el art. 89.1 de la Ley a cualquier supuesto de comisión flagrante de incumplimiento laboral supondría una quiebra del principio de confianza legítima». Vid. GOÑI SEIN, J.L., «Vigilancia empresarial...», *ob. cit.*, págs. 205-206. Sobre el principio de finalidad antes mencionado *vid.* el art. 5.1 b del Reglamento (UE) 2016/679 (RGPD).

⁴⁵ Vid. LÓPEZ BALAGUER, M. y RAMOS MORAGUES, F., «Derecho a la intimidad...», *ob. cit.*, págs. 412-413.

⁴⁶ Vid. LAHERA FORTEZA, J., «Videovigilancia...», *ob. cit.*, pág. 148. Señala asimismo el autor en apoyo de su tesis el hecho de que el artículo 42.4 de la Ley 5/2014, de Seguridad Privada, «al declarar que las grabaciones obtenidas por la videovigilancia de seguridad no pueden destinarse a uso distinto de su finalidad» se distingue netamente de la regulación contenida en los arts. 22 y 89 LOPDGD, en que no se hace esa expresa mención. Con todo, ofrece como alternativa permitir la videovigilancia para ilícitos penales y para ilícitos laborales «especialmente relevantes», pero no para el resto (infracciones disciplinarias menores). *Idem*, *ob. cit.*, pág. 272.



ral por parte de la ley de 2018. Por más que esta haya venido a cubrir la laguna antes existente en este ámbito de la videovigilancia laboral, lo ha hecho de una manera que deja aún demasiadas dudas y flancos abiertos, que la jurisprudencia constitucional no ha cerrado, aunque dada la amplitud que la STC 119/2022 otorga al uso de la videovigilancia cabe imaginar que, si se sigue en esta línea, es fácil que el TC acabe dando por buena en el futuro la tercera tesis.

No cabe duda, en cualquier caso, que en los últimos años se ha venido imponiendo, tanto en el plano jurisprudencial (TC, TEDH) como en el normativo (RGPD UE, LOPDGDD) con matices diversos en cada caso, una orientación más favorable al poder de control del empleador que a la protección del derecho a la protección de datos del trabajador. Como señala Molina Navarrete, sin embargo, «el ordenamiento jurídico no está para dar la máxima eficacia tecnológicamente posible para que el empleador pueda obtener la prueba del incumplimiento, asegurándole el éxito en la acción sancionadora, sino para procurar el efecto disuasorio-preventivo de tales incumplimientos», y sin que quepa erigir el mencionado derecho a la protección de datos como barrera insalvable ante cualquier medida de control, no es menos cierto que «hay otros modelos de hallar el “justo equilibrio” distintos al favor hacia la autotutela razonable del empleador». Por ello, cuando la información sobre la videovigilancia prevista para captar actos ilícitos pudiera poner en riesgo el éxito de la misma, podría pensarse en recurrir por ejemplo a la autorización judicial previa, como vía más razonable y preferible a la de dar por suficiente la presencia de un distintivo⁴⁷.

IV. Conclusiones: un paso más en la devaluación del reconocimiento al derecho a la protección de datos en los casos de videovigilancia laboral

La STC 119/2022 culmina un itinerario claramente restrictivo para el derecho a la protección de datos de los trabajadores ante el uso de la videovigilancia. Frente a las dos opciones opuestas que representaron la STC 29/2013 y la STC 39/2016, la nueva sentencia de 2022 profundiza en la línea de esta y añade además elementos de nueva devaluación del derecho del art. 18.4 CE, posibilitando que, frente a lo que la LOPDGDD dispone, la excepción se convierta en la regla si el empresario así lo quiere, de modo que este no informe de las finalidades de control laboral que las cámaras pueden tener y, aun así, se beneficie con tal fin de lo que estas graben.

⁴⁷ Vid. en torno a ello MOLINA NAVARRETE, C., «¿Son legítimos...», *ob. cit.*, págs. 5-7.



Frente a la finalidad clara de la LOPDGDD, que era la de reducir a un caso concreto (captación por la videocámara de la comisión flagrante de un acto ilícito) el alcance de la excepción a la regla de informar claramente al trabajador, el TC pone al mismo nivel excepción y regla y permite al empresario elegir qué prefiere. Se va mucho más allá de lo que había expresado el TEDH en su sentencia López Ribalda II, y desde luego muchísimo más allá que la LOPDGDD, que concretaba en sentido restrictivo el alcance de dicha línea jurisprudencial y se ve, *de facto*, reescrita por la interpretación del TC. Combínese ello con la extensión de la interpretación de lo que sea acto ilícito, con la suficiencia de una mera sospecha indiciaria para poder acudir a las cámaras, y con la concepción de flagrancia en su vertiente digital, según la cual flagrante es cualquier cosa que en el pasado haya registrado la videocámara, y se concluirá que, si en algún momento el derecho a ser informado de la captación de los propios datos estuvo conectado con el contenido esencial del derecho del art. 18.4 CE (y lo estuvo en la STC 29/2013 claramente) esa conexión parece haberse perdido del todo, refrendándose así lo que ya sucediera en la STC 39/2016. El TC, en fin, ha reescrito en la práctica el art. 89.1 LOPDGDD en su sentencia de 2022 y lo ha hecho de la manera más restrictiva posible para la posición de los trabajadores y la eficacia del art. 18.4 CE, que en este punto pasa a ser un derecho en manos de la decisión libérrima del empresario, cuya conducta previa y observancia o no del régimen de la LOPDGDD pasan a ser irrelevantes. No parece, desde luego, que reinterpretar leyes en detrimento de la eficacia de un derecho fundamental sea la mejor manera de que un Tribunal Constitucional lleve a cabo su función, y solo cabe por ello esperar un replanteamiento por parte de este en el futuro de su actual línea jurisprudencial en este ámbito, y si fuera posible con algo más de explicación que la que se dio (o mejor dicho, que la que no se dio, pues no hubo explicación de ningún tipo) para abandonar bruscamente el enfoque de la STC 29/2013 en la 39/2016 y abrir así una deriva reduccionista del derecho fundamental en la que profundiza la 119/2022.

V. Bibliografía

- ALTÉS TÁRREGA, J.A., «La videovigilancia encubierta en la nueva regulación sobre derechos digitales laborales y la incidencia de la STEDH López Ribalda (II)», en *Revista General de Derecho del Trabajo y de la Seguridad Social*, núm. 55, 2020, págs. 327-362.
- BAZ RODRÍGUEZ, J., «La Ley Orgánica 3/2018 como marco embrionario de garantía de los derechos digitales laborales. Claves para un análisis sistemático», en *Trabajo y Derecho*, núm. 54, 2019, págs. 1-28.



- BELTRÁN DE HEREDIA RUIZ, I., «Cámaras de vigilancia, intimidad y protección de datos: prueba lícita y despido procedente (STC 119/2022)», pág. 16, en el Blog «Una mirada crítica a las relaciones laborales», 25 de octubre de 2022 (accesible en: ignasibeltran.com/2022/10/25/camaras-de-vigilancia-intimidad-y-proteccion-de-datos-prueba-licita-y-despido-procedente-stc-119-2022/).
- CABELLOS ESPIÉRREZ, M.A., «El derecho a ser informado como elemento esencial del derecho a la protección de datos. Una visión crítica de la jurisprudencia del Tribunal Constitucional y de su cambio de doctrina en la STC 39/2016», en *Revista Vasca de Administración Pública*, núm. 106, 2016, págs. 191-216.
- CUADROS GARRIDO, M.E., «A vueltas con la videovigilancia como control de la prestación laboral y el juicio de ponderación», en *Revista Justicia & Trabajo*, núm. 1, 2022, págs. 57-93.
- DESDENTADO BONETE, A., MUÑOZ RUIZ, A.B., «Trabajo, videovigilancia y controles informáticos. Un recorrido por la jurisprudencia», en *Revista General de Derecho del Trabajo y de la Seguridad Social*, núm. 39, 2014, págs.1-24.
- GARCÍA RUBIO, M.A., «Control tecnológico empresarial y nuevos problemas aplicativos tras la L.O. 3/2018. Una mirada desde el deber de información previa», *Labos*, vol. 3, núm. 1, 2022, págs. 21-46.
- GARCÍA-PERROTE ESCARTÍN, I., «A proba no proceso laboral: algúns puntos críticos recentes», en *Revista Galega de Dereito Social*, núm. 13, 2021, págs. 9-30.
- GONZÁLEZ GONZÁLEZ, C., «Control empresarial de la actividad laboral mediante la videovigilancia y colisión con los derechos fundamentales del trabajador. Novedades de la Ley Orgánica 3/2018», en *Revista Aranzadi Doctrinal*, núm. 4, 2019, págs. 103-142.
- GOÑI SEIN, J.L., «Vigilancia empresarial y protección de datos: Doctrina Jurisprudencial», en *Revista del Ministerio de Trabajo, Migraciones y Seguridad Social*, núm. 143, 2019, págs. 191-212.
- GUDE FERNÁNDEZ, A., «La videovigilancia laboral y el derecho a la protección de datos de carácter personal», en *Revista de Derecho Político*, núm. 91, 2014, págs. 45-89.
- HENRÍQUEZ TILLERÍA, S., «Protección de datos, videovigilancia laboral y doctrina de la sentencia López Ribalda II: un peligroso camino hacia la degradación de la obligación de información», en *IUSLabor*, núm. 3, 2019, págs. 55-80.
- LAHERA FORTEZA, J., «Videovigilancia laboral y grabación de sonidos en el lugar de trabajo», en *Revista del Ministerio de Trabajo y Economía Social*, núm. 148, 2021, págs. 261-282.
- LÓPEZ BALAGUER, M. y RAMOS MORAGUES, F., «Derecho a la intimidad y a la protección de datos y licitud de la prueba en el proceso laboral», en MONREAL BRINGSVAERD, E. *et al.*, en *Derecho del trabajo y nuevas tecnologías*, Tirant lo Blanch, Valencia, 2020, págs. 387-424.
- MOLINA NAVARRETE, C., «¿Son legítimos los usos laborales de cámaras ocultas?: no, pero sí; sí, pero no», en *La Ley Privacidad*, núm. 3, 2020, págs. 1-7.



RODRÍGUEZ ESCANCIANO, S., *Poder de control empresarial, sistemas tecnológicos y derechos fundamentales de los trabajadores*, Tirant lo Blanch, Valencia, 2015.

ROJO TORRECILLA, E., «Después de las Jornadas Catalanas de Derecho Social. ¿Constitucionalización del poder de dirección empresarial en la relación de trabajo? Nota crítica a la sentencia del Tribunal Constitucional de 3 de marzo de 2016 (sobre instalación de cámaras de videovigilancia) (II)», en el Blog: *El nuevo y cambiante mundo del trabajo. Una mirada abierta y crítica a las nuevas realidades laborales*, 21 de marzo de 2016 (accesible en: http://www.eduardorojotorrecilla.es/2016/03/despues-de-las-jornadas-catalanas-de_21.html).

VALLE MUÑOZ, F. A., «Las cámaras de videovigilancia en la empresa como medio de prueba en el proceso laboral», en *IUSLabor* núm. 3, 2021, págs. 31-59.

