EL CONTROL EMPRESARIAL POR VIDEOVIGILANCIA EN LA LOPD*

Mercedes López Balaguer

Profesora Titular de Derecho del Trabajo y de la Seguridad Social

Universitat de València

EXTRACTO **PALABRAS CLAVE:** videovigilancia, protección de datos, control empresarial.

El presente trabajo revisa los criterios que pueden servir de fundamento argumental a la hora de aplicar el art. 89 LOPD. En primer lugar, se analiza la lectura que del precepto cabe hacer desde la perspectiva de la STC 29/2013, de 11 de febrero, llegando a la conclusión de que la argumentación que sirvió al Alto Tribunal para sostener la inconstitucionalidad de las cámaras identificadas, pero no informadas, sirve para interpretar el alcance aplicativo del primer párrafo del actual art. 89 LOPD, esto es, el referido precisamente a las cámaras informadas. Además, se apunta que la doctrina jurisprudencial en materia de videovigilancia también debe ser tenida en cuenta para llegar a esta conclusión. En segundo lugar, en relación con la referencia que se encuentra en el precepto a la posibilidad de sancionar los *ilícitos flagrantes* a partir de la prueba obtenida por cámaras identificadas, pero no informadas, se considera en este estudio que cabe entender aplicable la argumentación de la STC 39/2016, de 3 de marzo, teniendo también en cuenta la jurisprudencia del TS en la materia posterior a esta sentencia. Finalmente, se plantea en el trabajo la pregunta de si cabe admitir o no el uso de cámaras ocultas, es decir, ni identificadas ni informadas, como herramienta de control habilitada en el marco legal del art. 89 LOPD. Obviamente para responder a esta última cuestión en el trabajo se analiza la STEDH (Gran Sala) de 17 octubre 2019, *Caso López Ribalda y otros contra España*, concluyendo, a la luz de la misma, que será una posibilidad absolutamente la excepcional.

ABSTRACT **KEYWORDS:** video camera, Data Protection, business control

This paper reviews the criteria that can serve to apply art. 89 LOPD. First, the reading of the precept can be analyzed from the perspective of the STC 29/2013, of February 11, and concludes that the argument that served the High Court to support the unconstitutionality of the cameras identified, but not informed serves to interpret the scope of the first paragraph of the current art. 89 LOPD, that is, the one referring precisely to the informed cameras. In addition, it is pointed out that the jurisprudential doctrine regarding video surveillance should also be taken into account to reach this conclusion. Secondly, in relation to the reference found in the precept to the possibility of sanctioning the flagrant offenses from the test obtained by identified, but not informed, cameras, it is considered in this study that the argumentation of the STC 39/2016, of March 3, also taking into account the jurisprudence of the TS in the matter after this ruling. Finally, the question arises at the question of whether or not the use of hidden cameras can be admitted, that is, neither identified nor informed, as a control tool enabled in the legal framework of art. 89 LOPD. Obviously, to answer this last question at work, the ECHR (Great Hall) of October 17, 2019, *López Ribalda* et al. Case against Spain, is analyzed, concluding, in light of it, that it will be an absolutely exceptional possibility.

* Desarrollado en el marco del Sub-proyecto DER2017-83488-C4-3-R "Los derechos fundamentales del trabajo subordinado en la era digital" financiado por el Ministerio de Ciencia, Innovación y Universidades, la Agencia Estatal de Investigación y FEDER

 Recepción original: 07.01.2020. Aceptación: 03.02.2020

ÍNDICE

1. LA APLICACIÓN DE LA LOPD EN LA EMPRESA: PODER DE CONTROL *VERSUS* DERECHO A LA INTIMIDAD Y A LA PROTECCIÓN DE DATOS

Que los trabajadores no quedan desamparados en el marco de la relación laboral desde la perspectiva de los derechos fundamentales es un axioma ampliamente repetido por el Tribunal Constitucional. La doctrina constitucional clásica –y desde luego perfectamente actual- nos habla de la modulación o adaptación de los derechos fundamentales, pero nunca de la pérdida de los derechos o de la cesión total de los mismos. En este sentido, hay que tener en cuenta que esa modulación, como es sabido, es consecuencia del juego de la dependencia y se produce porque esta esencial característica del contrato de trabajo sitúa al trabajador bajo el poder de dirección y control de la empresa[1].

De este modo, es obvio que no todos los derechos fundamentales que cada persona tiene reconocidos se van a ver afectados en la misma medida por el hecho de ser persona trabajadora. Así ocurrirá en mucha menor medida, por poner algún ejemplo, con derechos como el de educación (art. 27 CE), participación en asuntos públicos (art. 23 CE), asociación (art. 22 CE), etc. Sin embargo, al margen evidentemente de los derechos fundamentales de libertad sindical y huelga –y, en su caso, del derecho a la negociación colectiva-, la confrontación del poder de dirección y control empresarial con otros derechos fundamentales es especialmente intensa.

En la materia que ahora nos ocupa no cabe duda de que esa intensidad en la confrontación ha ido en aumento con la incorporación de la tecnología digital. En efecto, cuando hablamos hoy de derecho a la intimidad frente al poder de control, hablamos muchas veces de limitar que este pueda ser constante en el tiempo y en el espacio, incluso aunque de ese control pueda obtenerse prueba de un incumplimiento de las obligaciones laborales. La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y Garantía de los Derechos Digitales (en

[1] Por todas, SSTC 57/1994, de 28 de febrero; y, 143/1994, de 9 de mayo.

adelante, LOPD) ha venido a reconfigurar en el ámbito laboral el derecho del trabajador a la intimidad y a la protección de datos y el derecho de la empresa al control de las obligaciones laborales. Y lo ha hecho además diferenciando el alcance de ambos derechos *en el uso* y *frente al uso* de los dispositivos digitales en los arts. 87, 89 y 90 LOPD.

En efecto, la LOPD reconoce y regula el derecho a la protección de datos y a la intimidad de los trabajadores tanto desde una perspectiva dinámica o proactiva como desde una perspectiva estática o pasiva. Y es que el derecho fundamental existe y se reconoce en tanto son trabajadores usuarios de dispositivos digitales y en tanto son trabajadores objeto de control mediante dispositivos digitales.

Por una parte, como usuarios de dispositivos digitales puestos a su disposición por el empresario para la prestación del servicio, el art. 87 LOPD viene a reconocer el derecho a la intimidad de los trabajadores imponiendo a la empresa una obligación de información en base al reconocimiento de un doble y gradual estándar de intimidad de los trabajadores, cuya graduación depende de la prohibición o admisión del uso privado de los dispositivos digitales que los empresarios deben comunicar de manera previa a los trabajadores tras decidirlo con la participación de los representantes de los trabajadores[2]. El cumplimiento de este deber de información, que debe ser considerado contenido esencial del derecho a la intimidad del trabajador[3], implica que de antemano el trabajador sabe que nos podemos encontrar dos escenarios:

- Si los criterios de uso quedan limitados única y exclusivamente al ámbito profesional la consecuencia será que el empresario deberá respetar los *estándares mínimos de protección de la intimidad de acuerdo con los usos sociales y los derechos reconocidos constitucional y legalmente.*
- Si los criterios de uso permiten el uso de los dispositivos digitales con fines privados la consecuencia será que el empresario *deberá especificar de modo preciso los usos autorizados y se establecerán garantías para preservar la intimidad de los trabajadores, tales como, en su caso, la determinación de los períodos en que los dispositivos podrán utilizarse para fines privados*.

[2] Con esta exigencia, asume la LOPD una de las recomendaciones del importante *Dictamen 2/2017 del GT 29 sobre el tratamiento de datos en el trabajo* que recomienda que, en todos los casos, una muestra representativa de trabajadores participe en la evaluación de la necesidad del control, así como en la lógica y accesibilidad de la política. [Dictamen consultado en versión digital Sitio web: http://ec.europa.eu/justice/data-protection/index_en.htm].

[3] Serrano Olivares, R., "Los derechos digitales en el ámbito laboral: comentario de urgencia a la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales", IusLabor, 3/2018, [versión digital], p. 219.

En el primer escenario de prohibición total del uso privado, que es hoy posible desde una interpretación literal de la norma[4], nos moveríamos en lo que legislador ha denominado *estándar mínimo* de protección de la intimidad. Y, en el segundo, nos moveríamos en lo que podríamos llamar *estándar reforzado* de protección de la intimidad.

Por otra parte, como trabajadores cuya actividad laboral se controla mediante dispositivos digitales, los arts. 89 y 90 LOPD regulan el derecho a la intimidad y a la protección de datos de los mismos frente al control a través de videovigilancia y frente al control a través de sistemas de geolocalización.

Pues bien, en las páginas que siguen nos vamos a ocupar específicamente del análisis del art. 89 LOPD y de la regulación de la videovigilancia como medio de control de la actividad de los trabajadores. Concretamente, el presente estudio se quiere plantear desde la premisa de asumir una interpretación de este nuevo marco legal a la luz de la jurisprudencia ya conocida tanto del TC como del TS y del TEDH.

2. EL CONTROL DEL TRABAJADOR MEDIANTE SISTEMAS DE VIDEOVIGILANCIA EN EL ART. 89 LOPD

El art. 89 LOPD es el precepto que se ocupa de regular, tal y como acabamos de ver, la videovigilancia como sistema de control empresarial. En este sentido, en relación con el derecho fundamental a la intimidad de los trabajadores, es el precepto que establece el marco legal para que la obtención de pruebas mediante esta técnica de vigilancia no implique una vulneración de aquel. Es, en definitiva, el precepto que marca hasta dónde es constitucionalmente aceptable la modulación del derecho fundamental y, por lo tanto, cual es el perfil que enmarca la legitimidad del poder de control empresarial.

Pues bien, tras una primera lectura del precepto se podría decir que, en comparación con el art. 87 LOPD, que hemos revisado en el epígrafe anterior, el legislador ha ido de más a menos. Este precepto, como hemos visto antes, de forma ordenada, reconoce primero el derecho a la intimidad del trabajador; en segundo lugar, el poder de control de la empresa; y, en tercer lugar, delimita el espacio de concurrencia de este derecho y este deber imponiendo límites a la empresa para que el control no supere el marco del derecho a la intimidad que el

[4] En este sentido, Serrano Olivares, R., "Los derechos digitales en el ámbito laboral: comentario…", *op. cit.,* p. 219; y, Mercader Uguina, J.R., *Protección de datos y garantía de los derechos digitales en las relaciones laborales*, Ed. Francis Lefebvre. Claves Prácticas, Madrid, 2019, p. 132. Para ambos autores la dicción literal del art. 87 LOPD lleva a interpretar que es posible que el empresario limite absolutamente el uso privado de los dispositivos digitales.

trabajador mantiene en el ámbito laboral. Sin embargo, el art. 89 LOPD no hace alusión expresa al reconocimiento del derecho a la intimidad y a la protección de datos del trabajador, sino que comienza con el reconocimiento del poder empresarial de tratamiento de las imágenes obtenidas a través de sistemas de cámaras o videocámaras para el ejercicio de las funciones de control de los trabajadores, limitando este poder mediante la imposición de una obligación de información, que plantea importantes dudas interpretativas.

En efecto, el art. 89 LOPD, tras reconocer el derecho de los empresarios a tratar las imágenes obtenidas a través de sistemas de cámaras o videocámaras para el ejercicio de las funciones de control "siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo" establece:

- Primero, que los empleadores habrán de informar con carácter previo, y de forma expresa, clara y concisa, a los trabajadores y, en su caso, a sus representantes, acerca de esta medida –«cámaras informadas»-.
- Segundo, que en el supuesto de que se haya captado la comisión flagrante de un acto ilícito por los trabajadores se entenderá cumplido el deber de informar cuando existiese al menos el dispositivo al que se refiere el artículo 22.4 de la LOPD –«cámaras identificadas no informadas»-.
- Tercero, que se prohíbe absolutamente la instalación de sistemas de grabación de sonidos y de videovigilancia en lugares destinados al descanso o esparcimiento de los trabajadores, tales como vestuarios, aseos, comedores y análogos.
- Y, finalmente, en relación con la grabación de sonidos, que solo se admitirá si resultan "relevantes los riesgos para la seguridad de las instalaciones, bienes y personas" y si, además, se respeta "el principio de proporcionalidad, el de intervención mínima y las garantías previstas en los apartados anteriores".

De este modo, nos encontramos ante un precepto que, respecto del uso de la videovigilancia, delimita el derecho fundamental a la protección de datos y a la intimidad de manera específica en función de criterios relacionados con el contenido de la información captada, el espacio donde esta se obtiene y con la captación de sonidos.

2.1. El control empresarial mediante videovigilancia: la actividad laboral y la comisión de *ilícitos flagrantes*

Según lo dispuesto en el art. 89.1 LOPD, para que la empresa pueda utilizar la videovigilancia de manera ajustada al derecho de protección de datos y a la intimidad del trabajador será necesario que lo haga dentro del marco legal y con los límites inherentes al mismo. En este sentido, teniendo en cuenta la doctrina

constitucional, es preceptivo, en primer lugar, que el empresario ejerza su función de control legalmente y dentro de los límites relativos a la proporcionalidad, necesidad e idoneidad del sistema. Y, en segundo lugar, que el trabajador -y los representantes de los trabajadores si los hay- hayan sido informados de la finalidad de control de la actividad laboral a la que va dirigida la videovigilancia.

Comenzando por el ejercicio de la función de control dentro de los límites legales, hemos de recordar la clásica STC 186/200, de 10 de julio, que se refería precisamente a videovigilancia. Según su doctrina, los límites para entender válido el recurso a esta medida de control en el marco del derecho a la intimidad personal se acotan en: a) la idoneidad de la videovigilancia para la finalidad pretendida por la empresa -verificar si el trabajador cometía efectivamente las irregularidades sospechadas y en tal caso adoptar las medidas disciplinarias correspondientes)-; b) la necesidad de la medida -ya que la grabación serviría de prueba de tales irregularidades-; y, c) la proporcionalidad del control por videovigilancia –limitación espacial y temporal-.

En este sentido, hay que tener en cuenta que la videovigilancia como sistema permanente y continuado de control no será admisible en general en las empresas. Y es que, tal y como ha apuntado la doctrina científica[5], resultará desproporcionado un sistema que permita el seguimiento continuo de la actividad laboral monitorizando por completo su actividad laboral, dado que una videovigilancia genérica y permanente con finalidad de control laboral no es admisible en el marco del derecho fundamental, ni siquiera cumpliendo con la obligación de información[6].

En segundo lugar, respecto de la obligación de que el trabajador -y los representantes de los trabajadores si los hay- hayan sido informados de la finalidad de control de la actividad laboral a la que va dirigida la videovigilancia[7],

[5] Mercader Uguina, J.R., *Protección de datos y garantía de los derechos…, op. cit.,* p. 139; y, García Murcia, J. y Rodríguez Cardo, I.A., "La protección de los datos personales en el ámbito del trabajo: una aproximación desde el nuevo marco normativo", Revista Española de Derecho del Trabajo, núm. 216, 2019 [versión digital], p. 39.

[6] De hecho, el GT-29 en el *Dictamen 2/2017 sobre el tratamiento de datos en el trabajo*, de 8 de junio de 2017, 17/ES WP 249, advierte específicamente que la videovigilancia sigue presentando los mismos problemas para la privacidad de los trabajadores que antes: la capacidad de grabar de forma continuada el comportamiento del trabajador. Y, en relación con ello apunta que la posibilidad de que un empresario observe las expresiones faciales del trabajador por medios automatizados, identifique desviaciones con respecto a los patrones de movimiento predefinidos (por ejemplo, una fábrica), etc. sería desproporcionada a efectos de los derechos y libertades de los trabajadores y, por tanto, ilegal en general.

[7] En sede de suplicación ya encontramos numerosas sentencias que, de acuerdo con lo previsto en el art. 89.1 LOPD, entienden lícita la prueba obtenida cuando "la empresa ha emitido con el Comité Intercentros acta conjunta para informar sobre las cámaras de videovigilancia y su utilización en actuaciones disciplinarias y que podrán ser utilizadas para la detección de acciones

ha de destacarse, de acuerdo con la doctrina constitucional[8], que esa información deberá concretar las características y el alcance del tratamiento de datos que va a realizarse, esto es, en qué casos las grabaciones pueden ser examinadas, durante cuánto tiempo y con qué propósitos, explicitando "muy particularmente" que pueden utilizarse para la imposición de sanciones disciplinarias por incumplimientos del contrato de trabajo.

No obstante, como veíamos antes, en su párrafo segundo el art. 89.1 LOPD hace alusión a la posibilidad de que el sistema de videovigilancia no haya sido informado, permitiendo que la prueba obtenida a través de este medio pueda entenderse válida si con ella se constata "la comisión flagrante de un acto ilícito". En este caso, el único requisito que el precepto exige en relación con el deber de información es el recogido en el art. 22.4 LOPD que, como es sabido, se refiere a "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".

Con ello el legislador español estaría admitiendo que, de manera excepcional y solo ante la comisión flagrante del ilícito, la prueba obtenida por la empresa sería válida si el sistema de videovigilancia estaba identificado de modo ordinario, sin exigirse en este caso la información específica a que se refiere el primer párrafo del art. 89.1 LOPD[9].

A mi modo de ver, la regulación actual que configura estos dos niveles de videovigilancia asumiría, por una parte, la doctrina constitucional de la STC

irregulares, sean éstas realizadas por personas ajenas a la empresa, por personal que presta servicios en la misma, sirviendo en su caso, como base para actuación disciplinaria laboral" (STSJ de Andalucía de 11 de abril de 2019, rec. 1125/2018); o, por poner otro ejemplo, cuando se acredita que "la empresa llegó a un acuerdo con el Comité Intercentros sobre la existencia de cámaras de videovigilancia en los centros comerciales y de trabajo, en las zonas de trabajo, sean de acceso, tránsito, venta, elaboración o almacenamiento, muelle o aparcamiento, implantadas para controlar la seguridad de personas, bienes, instalaciones y mercancías a la venta, pudiendo ser utilizadas legítimamente para la detección de acciones irregulares, sean éstas realizadas por personas ajenas a la empresa, o por personal que presta servicios en la misma, sirviendo, en su caso como base para actuación disciplinaria laboral y dicho acuerdo se comunicó a los trabajadores a través de circulares internas colgadas en los tablones de anuncios y en el Sistema de Información de Empresa" (STSJ de Madrid de 25 de enero de 2019, rec. 971/2018).

[8] En estos precisos términos STC 29/2013, de 11 de febrero. En este mismo sentido, considera Serrano Olivares, R., "Los derechos digitales en el ámbito laboral: comentario…", *op. cit.,* p. 222, que, aunque la ley no exige que el empleador deba informar expresamente sobre la finalidad y el alcance concreto de la instalación, parece lógico pensar que se trata de uno de los contenidos esenciales que integran el deber de información empresarial, sin que la ley aclare, por otra parte, cuáles serían los efectos de un eventual incumplimiento del deber empresarial de información.

[9] Para García Murcia, J. y Rodríguez Cardo, I.A., "La protección de los datos personales en

29/2013, de 11 de febrero, caso *Universidad de Sevilla*, que consideró insuficiente en el plano del derecho de protección de datos el hecho de que "existieran distintivos anunciando la instalación de cámaras y captación de imágenes" en el centro de trabajo, en el entendido de que "era necesaria además la información previa y expresa, precisa, clara e inequívoca a los trabajadores de la finalidad de control de la actividad laboral a la que esa captación podía ser dirigida" y que, como es conocido, se refería a incumplimientos relacionados con la jornada de trabajo. En efecto, aunque se ha considerado que esta doctrina queda superada por la nueva regulación de la LOPD[10], desde mi punto de vista, es posible sostener que la doctrina constitucional de la sentencia 29/2013 sigue estando vigente, como seguidamente explicaré.

Por otra parte, creo que, a la luz de la regulación del art. 89.1. 2ºpárr. LOPD, se ha de entender que se ha asumido y superado a la vez la doctrina de la STC 39/2016, de 3 de marzo, caso *Berska,* porque actualmente no es posible sostener legalmente que si la instalación de la videovigilancia tiene por objeto controlar la actividad laboral, es válida la prueba obtenida de la misma "sin que haya que especificar, más allá de la mera vigilancia, la finalidad exacta que se le ha asignado a ese control" [11]. Pero, sin embargo, con la nueva regulación, sí se admitiría que, en el concreto supuesto que se cuestionaba en esta sentencia de 2016 –que, como también es sabido, se refería a la transgresión de la buena fe contractual por la

el ámbito del trabajo: una aproximación desde…", *op. cit*. p. 39, este precepto es de redacción "un tanto equívoca y deficiente", pues en lugar de establecer una regla clara y precisa sobre el alcance de las facultades empresariales en esos casos, y sobre lo que puede hacer el empresario *ex ante* con esos fines de control particularizado, parte de la hipótesis de que en un momento determinado se haya captado, a través de los dispositivos existentes, la «comisión flagrante de un acto ilícito», en cuyo caso basta con la existencia de ese tipo de «dispositivos» para que se entienda cumplido el preceptivo deber de información.

[10] Serrano Olivares, R., "Los derechos digitales en el ámbito laboral: comentario…", *op. cit.,* p.223, que entiende que la excepción de las cámaras solo identificadas ampararía tanto el uso para fines disciplinarios de seguridad (personas, bienes o instalaciones) como la instalación temporal de cámaras con fines de control laboral cuando existieran fundadas sospechas previas de incumplimientos laborales. Interpretada en estos términos, la nueva regulación vendría a rectificar la doctrina del Tribunal Constitucional en el asunto Universidad de Sevilla (sentencia 29/2013, de 11 de febrero) y a otorgar carta de naturaleza, en cambio, a la doctrina del mismo Tribunal Constitucional en el caso Bershka (sentencia 39/2016, de 3 de marzo).

[11] Según esta STC "lo importante será determinar si el dato obtenido se ha utilizado para la finalidad de control de la relación laboral o para una finalidad ajena al cumplimiento del contrato, porque sólo si la finalidad del tratamiento de datos no guarda relación directa con el mantenimiento, desarrollo o control de la relación contractual el empresario estaría obligado a solicitar el consentimiento de los trabajadores afectados". Un análisis extenso de la doctrina constitucional en materia de videovigilancia puede encontrarse en Taléns Visconti, E., "Vídeo-vigilancia y protección de datos en el ámbito laboral: una sucesión de desencuentros", *Revista Internacional y Comparada de Relaciones Laborales y Derecho del Empleo*, Volumen 6, núm. 3, julio-septiembre de 2018, p. 59 y ss.

comisión de pequeños hurtos-, la prueba obtenida con cámaras identificadas y no informadas sería lícita en el plano del derecho del derecho de protección de datos.

Entiendo que cabe alcanzar esta doble conclusión porque, como ya he dicho, el cumplimiento de la obligación de información es condición esencial hoy desde la perspectiva de la licitud de la prueba si el sistema de videovigilancia se utiliza específicamente para el control de la actividad laboral. Por lo tanto, la mera identificación de la cámara en estos casos no sería hoy suficiente y, así, si la prueba obtenida se refiere al incumplimiento de las obligaciones laborales ordinarias y no a las vinculadas con la seguridad, cuando solo conste este único elemento informativo, deberemos considerar que, de acuerdo con el art. 89 LOPD, se ha vulnerado del derecho fundamental a la intimidad del trabajador. De este modo, creo que la cuestión más controvertida se centra, tras la LOPD, en la delimitación de lo que deba considerarse un ilícito flagrante porque, dado que nos movemos en un terreno relativo al respeto al derecho fundamental de protección de datos y de intimidad, será necesario acotar de modo preciso el espacio de la excepción a la regla general de la información previa, expresa, clara y concisa. Creo pues que será necesario delimitar, en primer lugar, a qué ilícitos se refiere el art. 89.1.2ºparr (a); y, en segundo lugar, en qué casos debe considerarse flagrante su comisión (b)

a) Es evidente, por una parte, que no podemos identificar el ilícito a que se refiere el art. 89 LOPD con ilícito penal porque la tramitación parlamentaria de la LOPD nos lleva sin duda a esta conclusión[12].

En este sentido, como se ha apuntado[13], "aunque una lectura en clave tuitiva de la ley nos conduciría a interpretar restrictivamente la expresión "actos ilícitos", reservándola a los ilícitos de tipo penal, es lo cierto que tanto una interpretación literal como histórica de la ley, nos aboca a la interpretación contraria". Así pues, debemos entender que el ilícito sancionable a partir de la prueba videográfica identificada y no informada podrá tener o no relevancia a efectos penales. Y, en este punto, la cuestión a dilucidar pasa por concretar si deberá o no quedar acotado al ámbito de la protección por motivos seguridad o, dicho de otro modo, para la

[12] Como señala Serrano Olivares, R., "Los derechos digitales en el ámbito laboral: comentario…", *op. cit.,* p. 225, el primer texto del proyecto de ley presentado por el Gobierno al Congreso se refería expresamente a la "comisión flagrante de un acto delictivo", de suerte que la nueva expresión empleada por la ley obedece claramente a la voluntad de extender la excepción prevista a cualquier supuesto de comisión flagrante de un incumplimiento laboral. En este sentido, Taléns Visconti, E., "Vídeo-vigilancia y protección de datos en el ámbito…", *op. cit.,* p. 84, comentando el texto del Proyecto de LOPD, consideraba que "esta excepción iría destinada para su valor probatorio en el proceso penal, en el sentido de que las imágenes captadas sin información probablemente no sirvan para sustentar una sanción laboral, pero sí que tendrían validez para una eventual sanción por la vía penal".

[13] Serrano Olivares, R., "Los derechos digitales en el ámbito laboral: comentario…", *op. cit.,* p. 225

protección de las personas y las cosas; o si, dado que con ello también podríamos entender que nos movemos en el terreno penal, asumir que las cámaras solo identificadas y no informadas podrían legalmente captar cualquier ilícito laboral.

A mi entender, un argumento que el TS utilizó ya en 2017 podría servir también hoy para dar respuesta a esta cuestión en términos equilibrados desde la perspectiva del derecho fundamental a la intimidad. En la STS de 31 enero de 2017, rec. 3331/2015, se consideró que la prueba obtenida de cámaras de seguridad no específicamente utilizadas para el control laboral era "una medida justificada por razones de seguridad (control de hechos ilícitos imputables a empleados, clientes y terceros, así como rápida detección de siniestros), idónea para el logro de ese fin (control de cobros y de la caja en el caso concreto) y necesaria y proporcionada al fin perseguido, razón por la que estaba justificada la limitación de los derechos fundamentales en juego, máxime cuando los trabajadores estaban informados, expresamente, de la instalación del sistema de vigilancia, de la ubicación de las cámaras por razones de seguridad, expresión amplia que incluye la vigilancia de actos ilícitos de los empleados y de terceros y en definitiva de la seguridad del centro de trabajo pero que excluye otro tipo de control laboral que sea ajeno a la seguridad, esto es el de la efectividad en el trabajo, las ausencias del puesto de trabajo, las conversaciones con compañeros, etc."[14].

De este modo, para el TS los incumplimientos laborales que deberían entenderse lícitamente probados mediante cámara identificada y no informada expresamente para controles laborales quedaban circunscritos a los relacionados con la seguridad de las cosas o de las personas. En consecuencia, quedaban al margen de este ámbito de licitud las pruebas relacionadas con incumplimientos de las obligaciones laborales que podríamos denominar ordinarias. En este sentido, a mi juicio, el actual art. 89.2 LOPD debería interpretarse de manera restringida por lo que a los ilícitos laborales se refiere, haciendo una distinción entre:

- Obligaciones del trabajador referidas a condiciones de trabajo ordinarias: tiempo de trabajo, rendimiento, etc.
- Obligaciones de trabajo relativas al cumplimiento del deber de buena fe contractual respecto de la protección de las personas o las cosas.

El incumplimiento de las primeras detectado por cámaras no identificadas e informadas no podría ser sancionado lícitamente con la prueba obtenida de las mismas, debiendo entender que esta no podría considerarse válida por vulneración del derecho a la intimidad de los trabajadores. En cambio, el incumplimiento de las segundas detectado por cámaras identificadas y no informadas podría ser sancionado lícitamente con la prueba obtenida de las mismas, asumiendo que

[14] Siguiendo esta doctrina jurisprudencial, los TSJ interpretan mayoritariamente que

estos ilícitos laborales van más allá de la objetiva configuración de las obligaciones contractuales que ambas partes han de cumplir y que el empresario ha de controlar de modo ordinario. De hecho, el art. 22 LOPD, a cuyo apartado cuarto se remite el art. 89, regula precisamente a los sistemas de cámaras o videocámaras que se instalan con la finalidad de "preservar la seguridad de las personas y bienes, así como de sus instalaciones"[15].

b) Por lo que se refiere al carácter flagrante de la comisión del ilícito, entiendo que cabría apuntar dos interpretaciones. Por una parte, de manera restrictiva, cabría entender que la conducta sancionable debería ser aquella que se descubre por la cámara identificada y no informada de manera sorpresiva e insospechada por la empresa. Evidentemente, en estos casos la obtención de la prueba debería considerarse lícita, puesto que, conocida por el trabajador la existencia de la videocámara identificada, la comisión del ilícito que transgrede la buena fe contractual podrá ser sancionada porque se ajustará literalmente al "ilícito flagrante" a que se refiere el art. 89 LOPD.

No obstante, también cabe entender, en mi opinión, que cumplirá el requisito del carácter flagrante, el ilícito que se descubre por la videocámara identificada y no informada cuando esta sea utilizada para controlar específicamente, a partir de fundadas sospechas, alguna conducta irregular que se pueda estar cometiendo. En estos casos, la existencia de las cámaras sugiere, como señaló con claridad la STS de 7 de julio de 2016, rec. 3233/2014, "una finalidad protectora del patrimonio empresarial y la grabación de conductas que atenten contra esa finalidad"; por lo que, ante sospechas que sirven como justificación legítima al empresario, la prueba obtenida de las mismas habrá de reputarse válida, ya que, continua la citada sentencia, "semejante entorno específico excluye el factor sorpresa y muestra claramente la situación de riesgo asumido por la demandante y por cualquier otro responsable de conductas análogas".

En definitiva, considero que, de acuerdo con los argumentos apuntados, la interpretación del segundo párrafo del art. 89.1 LOPD debe llevar a considerar que cabrá admitir las pruebas obtenidas con videocámaras identificadas y no informadas siempre y cuando se trate, por un lado, de ilícitos laborales que

[15] En este sentido, Serrano Olivares, R., "Los derechos digitales en el ámbito laboral: comentario…", *op. cit.,* p. 223; para Rodríguez Escanciano, S., "Videovigilancia empresarial: límites a la luz de la Ley Orgánica 3/2018, de 5 diciembre, de protección de datos personales y garantía de los derechos digitales, *Diario La Ley*, Nº 9328, 2 de Enero de 2019 [versión digital], p. 5, "mayor será la posibilidad de supervisión cuanto más clara sea la fundada sospecha de comportamiento irregular por parte del empleado, pues no es igual comprobar el cumplimiento normal de las obligaciones laborales ordinarias, donde el deber de información debe de cumplimentarse en todos los extremos, que actuar ante el temor fundado de la perpetración de infracciones donde el principio de transparencia puede sufrir alguna modulación".

queden limitados a la transgresión de la buena fe contractual desde la perspectiva de la protección de las personas o las cosas en el ámbito de la empresa. Y, por otro, de ilícitos cometidos de manera flagrante y captados por las cámaras solo identificadas bien de manera sorpresiva –sin que se haya tenido previa sospecha de su concurrencia- bien tras un control más específico a partir de una justificación legítima de la empresa que actúa en base a determinados indicios de irregularidades.

2.2. ¿Son admisibles las cámaras ocultas en el marco legal de la LOPD?: *López Ribalda II* STEDH (Gran Sala) de 17 octubre 2019

Tras el análisis anterior de la interpretación que cabe hace del art. 89 LOPD a la luz de la doctrina del TC y del TS, aun quedarían dos preguntas por responder en relación con el tema de la videovigilancia tras la LOPD: ¿Son admisibles las cámaras ocultas? ¿Puede la empresa recurrir a ellas ante sospechas de un ilícito laboral?

La respuesta inicial a estas cuestiones podría ser negativa en el entendido de que el art. 89 LOPD viene a limitar la opción legal de la videovigilancia «como mínimo» a las cámaras identificadas y no informadas y, en consecuencia, las cámaras ocultas no serían una opción en términos de licitud de la prueba obtenida porque implicarían en todo caso la vulneración del derecho fundamental a la intimidad. Así, a mi modo de ver, la dicción literal de este precepto habría perfilado, como límite absoluto de la modulación de este derecho en el marco de la relación laboral, el relativo a la necesidad de que la videovigilancia sea identificada.

Sin embargo, es obvio que la respuesta a las preguntas que hacíamos debe hoy reformularse necesariamente a la luz de la doctrina del TEDH en la sentencia *López Ribalda II*. Como es sabido, con esta sentencia la Gran Sala modifica la interpretación que en la anterior resolución –STEDH (Sección Tercera) de 9 de enero de 2018[16]- consideró que, aunque la videovigilancia se había aplicado en el supuesto concreto ante sospechas legítimas de robo, su alcance fue amplio en el tiempo y desde una perspectiva subjetiva. Por lo tanto, se incumplía la regulación española de protección de datos de 1995 en relación con la obligación de información previa a los afectados respecto de la recogida y tratamiento de sus datos personales y de la existencia, finalidad y modalidades de la medida de vigilancia. De este modo, se declaró que los órganos jurisdiccionales españoles no habían ponderado adecuadamente los derechos de privacidad de las trabajadoras y otros

[16] Un comentario de esta sentencia en Taléns Visconti, E., "Vídeo-vigilancia y protección de datos en el ámbito…", *op, cit.,* p. 61 y ss.

intereses en juego, produciéndose, en consecuencia, una vulneración del artículo 8 CPDHLF.

Pues bien, siguiendo lo que se ha venido a llamar, acertadamente a mi juicio, "un camino de ida y vuelta"[17], la STEDH (Gran Sala) de 17 octubre 2019, *Caso López Ribalda y otros contra España,* ha rectificado esta conclusión y ha venido a admitir la videovigilancia con cámara oculta pero, como no podía ser de otro modo, de manera absolutamente condicionada. En este sentido, el pronunciamiento del TEDH se ha producido teniendo en cuenta los siguientes factores que me parecen especialmente importantes:

- Que la doctrina *Barbulescu II* es aplicable *mutatis mutandis* a la videovigilancia (ap. 116)[18].
- Que, teniendo en cuenta esta doctrina, son claves para la admisión de la videovigilancia oculta, por una parte, el ámbito espacial, el temporal y el subjetivo (ap. 125 a 127); y, por otra, la prueba de que la información sobre las cámaras podía "poner en riesgo la finalidad de la videovigilancia" (ap. 128).
- A partir de la anterior afirmación, que la exigencia de transparencia y el derecho a la información son fundamentales en el contexto de las relaciones laborales, pero que la información proporcionada a la persona objeto de vigilancia y su alcance "son sólo uno de los criterios a considerar a la hora de valorar la proporcionalidad de tal medida en un caso determinado. Sin embargo, si falta esa información, las garantías derivadas de los demás criterios serán aún más importantes" (ap. 131).
- Y, en consecuencia, que no cabe aceptar que "la mínima sospecha de robos u otras irregularidades cometidas por los empleados, pueda justificar la instalación de un sistema de videovigilancia encubierta por parte del empleador", pero en las particulares circunstancias del caso planteado, las sospechas razonables de que se habían cometido "graves irregularidades" por la acción

[17] Mercader Uguina, J., "López Ribalda II: un camino de ida y vuelta", entrada de 30.10.19: https://forodelabos.blogspot.com/2019/10/lopez-ribalda-ii-un-camino-de-ida-y.html. El autor señala que en esta sentencia son especialmente relevantes las reflexiones dedicadas al cumplimiento del deber de información, considerando que el TEDH plantea que "no puede aceptarse que la más mínima sospecha de que las irregularidades han sido perpetradas por los empleados puede justificar la implementación de videovigilancia secreta por parte del empleador, la sospecha razonable de que se habían cometido graves irregularidades y el alcance de las mismas producidas en este caso pueden considerarse justificaciones serias. Más aún en un caso como el analizado en el que se sospechaba la acción concertada de varios empleados".

[18] En la sentencia se traslada el *test Barbulescu* al ámbito de la videovigilancia, incorporando las preguntas relacionadas con la proporcionalidad, necesidad e idoneidad a esta tecnología de control (véase, apartado 116).

> conjunta de varios empleados y "el alcance de los robos constatados" pueden parecer una justificación seria, teniendo en cuenta que esta situación podía crear en la empresa un clima general de desconfianza (ap. 134).

Con estas premisas, el Tribunal de Estrasburgo acaba considerando, en sentido contrario a la sentencia de 9 de enero de 2018, que en el caso planteado no se vulneró el art. 8 CPDHLF. Tras esta resolución, creo que es posible extraer tres conclusiones que servirían, desde la perspectiva del derecho fundamental a la protección de datos y a la intimidad, para confirmar de algún modo algunas de las afirmaciones que he hecho ya.

Estas tres conclusiones implican asumir que el espacio que estos derechos fundamentales dejan al recurso de la videovigilancia como sistema de control es inversamente proporcional a la justificación legítima de la empresa. Dicho de otro modo, cuanto menor es esta mayor es el límite que perfila el derecho fundamental. Y así, si estamos ante un uso de la videovigilancia como medio de control del cumplimiento de las obligaciones laborales del trabajador, la justificación legítima sería también la elemental relacionada con el poder de dirección y control de la empresa. Sin embargo, si estamos ante un uso de la videovigilancia como medio de control de un acto ilícito flagrante, la justificación legítima vendrá reforzada por la sospecha de la empresa y su derecho de protección de la seguridad de las personas y las cosas en la empresa.

De acuerdo con esto, tras la sentencia *López Ribalda II,* podríamos considerar, en primer lugar, que la videovigilancia como sistema de control ordinario en la empresa solo será posible en relación con el derecho a la intimidad del trabajador cuando se haya informado previamente de la existencia de las cámaras y de manera clara y exhaustiva sobre la finalidad del control y siempre dentro de los márgenes de la proporcionalidad, idoneidad y necesidad. En segundo lugar, que la videovigilancia identificada pero no informada será admisible cuando exista sospecha «siquiera mínima» de "robos o de otras irregularidades", esto es, cuando se vea afectada la protección de las personas o las cosas en clave de seguridad. Entendemos que cabe alcanzar esta segunda conclusión porque, en tercer lugar, para que quepa admitir que la videovigilancia oculta o encubierta no vulnera el derecho a la intimidad, el TEDH refuerza la sospecha que actúa como justificación legítima de la empresa al exigir que aquella sea de especial gravedad en el sentido de que "atente al buen funcionamiento de la empresa" y "al clima general de desconfianza en la empresa".

2.3. La grabación del sonido: justificación legítima, proporcionalidad e intervención mínima

Para acabar con el análisis de la regulación de la videovigilancia en la LOPD hemos de hacer mención especial a la grabación del sonido como dato especialmente protegido porque el propio art. 89.3 LOPD así lo hace y además precisamente para aportar una estricta consideración de este control[19]. El precepto viene considerar exigibles respecto de la grabación de sonidos, además de la aplicación de las garantías previstas en los apartados anteriores y que ha hemos analizado, tres condiciones:

- Que concurran relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo.
- Que la grabación respete el principio de proporcionalidad y el de intervención mínima.
- Que los sonidos conservados por estos sistemas de grabación se supriman en el plazo máximo de un mes desde su captación, salvo cuando hubieran de ser conservados para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones.

Es evidente que en relación con la grabación de la voz, el legislador ha tenido muy en cuenta la doctrina constitucional clásica porque se refuerza de manera especial en relación con el control que incluya el sonido tanto el requisito de la justificación legítima como el requisito de la proporcionalidad e intervención mínima[20]. En este sentido, la dicción literal del 89.3 LOPD acoge la argumentación de la conocida y clásica STC 98/2000, de 10 de abril, que, reconociendo la "utilidad" para la empresa de un sistema de control que graba el sonido, matiza que "la mera utilidad o conveniencia para la empresa no legitima sin más la instalación de los aparatos de audición y grabación, habida cuenta de que la empresa ya disponía de otros sistemas de seguridad que el sistema de audición pretende complementar". De este modo, la sentencia acaba considerando que la implanta-

[19] Como ha señalado Rodríguez Escanciano, S., "Videovigilancia empresarial: límites a la…", *op. cit.,* p. 6, estos contornos más estrictos encuentran justificación en el solo hecho de tener en cuenta que las conversaciones están amparadas tanto por el derecho a la intimidad (art. 18.1 CE) cuanto por el derecho al secreto de las comunicaciones (art. 18.3 CE) y únicamente mediante autorización judicial es posible una injerencia en las mismas. La grabación de un diálogo suele ser más sensible que la de una imagen porque las palabras pueden revelar pensamientos y sentimientos internos, permitiendo comprobar fácilmente incumplimientos en el trabajo y adoptar medidas disciplinarias, de ahí que el Tribunal Europeo de Derechos Humanos –Asunto *Haldorf*- haya sido claro en la necesidad de que se avise al trabajador sobre la posible interceptación de los diálogos.

[20] Serrano Olivares, R., "Los derechos digitales en el ámbito laboral: comentario…", *op. cit.,* p. 224.

ción de este sistema no resulta conforme "con los principios de proporcionalidad e intervención mínima que rigen la modulación de los derechos fundamentales por los requerimientos propios del interés de la organización empresarial" porque, sin ningún filtro, recoge todas las conversaciones que se producen en el lugar de trabajo. Así pues, de la sentencia se desprende claramente que la grabación del sonido afecta a un dato especialmente protegido porque "permite captar comentarios privados" lo que ha de considerarse "una intromisión ilegítima en el derecho a la intimidad consagrado en el art. 18.1 CE, pues no existe argumento definitivo que autorice a la empresa a escuchar y grabar las conversaciones privadas que los trabajadores del casino mantengan entre sí o con los clientes"[21].

El art. 89.3 LOPD ha de ser interpretado a la luz de esta sentencia y, de ese modo, desde la perspectiva del art. 90.2 LRJS, habrá que entender que la licitud de la prueba en estos casos no será nada fácil de acreditar, dado que, primero, será necesario demostrar que la grabación del sonido responde a una justificación legítima reforzada y limitada a la seguridad. En segundo lugar, que el sistema que se utilice implica una intromisión lo menos invasiva posible. De este modo, queda descartado desde la perspectiva del derecho a la intimidad el uso de sistemas que permitan la audición continuada e indiscriminada de todo tipo de conversaciones. Y, en tercer lugar, deberá tratarse siempre de un sistema informado tanto a los trabajadores como a sus representantes, dado que el precepto declara aplicables las garantías previstas en los apartados anteriores[22].

[21] En este sentido, recuerda Mercader Uguina, J.R., *Protección de datos y garantía de los derechos…, op. cit.,* p. 147, que las grabaciones de sonido son especialmente sensibles porque con ellas se permite identificar a la persona, tal y como recoge la LOPD.

[22] Mercader Uguina, J.R., *Protección de datos y garantía de los derechos…, op. cit.,* p. 148. Véanse en materia de información los Informes de la AEDP en esta materia que recoge el autor (p.148-149).