PROTECCIÓN DE DATOS, VIDEOVIGILANCIA LABORAL Y DOCTRINA DE LA SENTENCIA LÓPEZ RIBALDA II: UN PELIGROSO CAMINO HACIA LA DEGRADACIÓN DE LA OBLIGACIÓN DE INFORMACIÓN

Sebastián Henríquez Tillería[1]
Profesor de Legislación Laboral y Seguridad Social
Universidad Católica de la Santísima Concepción, Chile

Abstract

El problema derivado de la colisión entre el derecho a la protección de datos personales y la videovigilancia laboral sigue teniendo plena vigencia y actualidad. Este artículo pretende dar una visión desde la evolución de la jurisprudencia del Tribunal Constitucional en la materia, con consideraciones doctrinarias acerca de la naturaleza jurídica del deber de información, a fin de realizar un contrapunto con las definiciones del Tribunal Europeo de Derechos Humanos contenidas en la reciente sentencia López Ribalda II, poniendo énfasis en los peligros que conlleva una posible degradación del deber de información.

The problem arising from the conflict between the right to the protection of personal data and labor video surveillance remains fully valid and current. This article intends to give a vision from the evolution of the jurisprudence of the Constitutional Court in the scope with doctrinal considerations about the legal nature of the duty of information, in order to make a counterpoint with the definitions of the European Court of Human Rights contained in the recent sentence López Ribalda II, emphasizing the dangers of a possible degradation of the duty of information.

IUSLabor 3/2019, ISSN 1699-2938, p. 55-80
DOI. 10.31009/IUSLabor.2019.i03.03

Fecha envío: 3.12.2019 | Fecha aceptación: 12.12.2019

Title: Data protection, labor video surveillance and doctrine of the sentence López Ribalda II: A dangerous road to the degradation of the information obligation.

[1] Abogado, Licenciado en Derecho, Universidad Católica de la Santísima Concepción (Chile); Magister en Derecho del Trabajo y Previsión Social, Universidad de Concepción (Chile); Máster en Derechos Sociolaborales y doctorando en Derecho, Universitat Autònoma de Barcelona.

Palabras clave: videovigilancia laboral, obligación de información, protección de datos, sentencia López Ribalda II.
Keywords: video surveillance, obligation of information, data protection, sentence López Ribalda II.

Sumario

1. Planteamiento

La irrupción del derecho a la protección de datos en el concierto normativo español no es nueva. En una notable premonición de los problemas derivados de los voraces avances de la tecnología, la Constitución de 1978 vino a consagrar la autodeterminación informativa y el establecimiento de límites legales al uso de la informática, en pos de la protección del honor e intimidad personales y familiar de las personas físicas. Esto, encuentra su máxima expresión en las Leyes Orgánicas de Protección de Datos.

La primera de ellas es la Ley Orgánica de Protección de Datos de Carácter Personal 15/1999[2] (en adelante LO 15/1999), para posteriormente ser derogada y reemplazada por la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales 3/2018[3] (en adelante LOPD 3/2018), como norma de desarrollo y adaptación del Reglamento General (UE) de Protección de Datos 2016/679[4] (en adelante RGPD). Pero es incluso antes de la entrada en vigor de dichos cuerpos normativo que la jurisprudencia del Tribunal Constitucional (en adelante TC) se volcó a la tarea de dar contenido a este derecho, y trató su desarrollo y márgenes en el contexto de la videovigilancia laboral.

De esta manera, haremos un repaso por la evolución de esta doctrina, a fin de determinar su estado actual y la vigencia de esta respecto de ciertas consideraciones fundamentales relativas a la naturaleza jurídica de una pieza clave en la materia: la obligación de información como elemento de la esencia del derecho a la protección de datos personales. La naturaleza jurídica de esta obligación va a tener radicales consecuencias a la hora de analizar supuestos de videovigilancia laboral, no siendo baladí la determinación de sus caracteres jurídicos particulares, toda vez que dependiendo de la postura que se tome, las secuelas jurídicas de su incumplimiento serán absolutamente opuestas.

Esto, quedará de manifiesto en el giro doctrinario dado en el *asunto López Ribalda y otras vs España*, por parte del Tribunal Europeo de Derechos Humanos (en adelante TEDH), manifestado en la sentencia de la Gran Sala[5], en virtud de la cual se produce una peligrosa degradación en el deber de información que pesa sobre el responsable en el tratamiento de datos personales. Veremos las razones de esta degradación, así como

[2] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Caracter Personal.

[3] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de Derechos Digitales.

[4] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.

[5] Sentencia Tribunal Europeo de Derechos Humanos, Gran Sala, de 17 de octubre de 2019 (demanda 1874/13).

otros aspectos problemáticos, a fin de aquilatar esta doctrina respecto al panorama normativo actual en España, y si es que es dable sostener la aplicabilidad de esta interpretación jurisprudencial en el presente contexto.

2. Transición de la doctrina del Tribunal Constitucional en materia de videovigilancia laboral y derecho a la protección de datos personales

A fin de dejar asentado el escenario de la actual doctrina del Tribunal Constitucional -para su posterior contraste con la doctrina de la sentencia López Ribalda II- debemos hacer una breve revisión del camino recorrido hasta ahora, el cual se ha caracterizado por ser una sinuosa carretera de decisiones más o menos compatibles con la propia definición y principios consagrados las primeras sentencias que delimitaron el núcleo esencial del derecho a la protección de datos personales.

Para ello, primeramente señalemos que el contenido esencial del derecho a la protección de datos personales ha sido definido[6] en la STC 292/2000[7] -refrendada en lo sucesivo por la STC 39/2016-, en la cual se señala por parte del Máximo Intérprete constitucional español que "*el contenido esencial del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso*"[8]. De esta forma estos poderes de disposición se concretan en la capacidad de consentir la obtención y acceso a esos datos, sumado a la facultad de conocer en todo momento quién dispone o puede disponer de esos datos y la finalidad a la que estarán sometidos.

[6] La primera vez que el derecho fundamental garantizado en el art. 18.4 de la C.E. fue esgrimido por un ciudadano, se dio en un caso resuelto por la STC 254/1993, de 20 de julio, en que el Gobierno Civil de Guipúzcoa le negó acceso a la información que de él poseía. Esta sentencia se vio aquilatada con las posteriores STC 143/1994 de 9 de mayo; la STC 11/1998, de 13 de enero, que declaró contrario a la libertad sindical con relación al artículo 18.4 de la C.E. el uso de una empresa del dato de la afiliación sindical para detraer haberes de los trabajadores por motivo de una huelga o la STC 202/1999, de 8 de noviembre, con ocasión de la denegación a un trabajador de la cancelación de sus datos médicos en un fichero informatizado de una entidad de crédito sobre bajas por incapacidad temporal, se apreció que el almacenamiento sin cobertura legal en soporte informático de los diagnósticos médicos del trabajador sin mediar su consentimiento expreso constituía una desproporcionada restricción del derecho fundamental a la protección de datos personales. Todo ello, de conformidad a lo expuesto en el fundamento jurídico 5 de la STC 292/2000 que define el contenido esencial del derecho a la protección de datos personales.

[7] STC 292/2000, Pleno, de 30 de noviembre de 2000 (Rec. de inconstitucionalidad núm. 1463/2000), Fundamento Jurídico 8º.

[8] STC 39/2016, Pleno, 3 de marzo de 2016 (Rec. núm. 7222/2013), Fundamento Jurídico 3º.

Este derecho a la protección de datos personales, si bien es posible afirmar que pertenece a los derechos de tercera generación[9], corresponde situarlo dentro de los denominados derechos fundamentales de cuarta generación, teniendo en cuenta que la llegada del Siglo XXI marcó un periodo en que la sociedad se identifica con la vinculación de sus integrantes mediante las nuevas tecnologías de la información y comunicación, lo cual conlleva la ocurrencia de fenómenos de agresión a los derechos que emanan de la personalidad, siendo necesaria la reivindicación de nuevas herramientas que permitan la protección de la esfera privada de los individuos y el derecho a determinar cómo se tratarán sus datos personales[10], ya sea por parte del Estado o de terceros[11].

En el caso de la evolución de la doctrina judicial del TC referida a la videovigilancia laboral y los derechos fundamentales del trabajador, nos encontramos ante un escenario en que es difícil encontrar uniformidad de criterios, dado que las primeras construcciones argumentativas jurisdiccionales se basaban en la afectación de los derechos a la intimidad y propia imagen, de forma casi exclusiva. No es sino la invocación del derecho a la protección de datos personales lo que vino a alterar por completo el análisis del conflicto, dada la exigencia al empresario del deber u obligación de información previa a los trabajadores, como especial medio de protección de la autodeterminación informativa[12].

---

[9] OJEDA BELLO Z., "El derecho a la protección de datos personales desde un análisis histórico-doctrinal", *Tla-melaua*, Volumen 9, Nº 38, 2015, p. 60.

[10] *Ibíd.*, p. 61.

[11] En esta parte RIASCOS GÓMEZ, L., expone la evolución del derecho a la protección de datos, a través de una progresión histórica desde el derecho a la intimidad aplicado a la realidad de las nuevas tecnologías de la información y comunicación, conceptualizado en la llamada "libertad informática" en cuanto facultad para acceder a todo tipo de información que derive de su individualidad, que lo identifique o lo haga identificable, y a efectos de consultarla y revisarla. Desde ese punto de vista las facetas preinformáticas e informáticas del derecho a la intimidad se basan en el *habeas data*, lo que conforma la libertad informática, en cuanto a derecho a acceso, rectificación y cancelación de los datos. Esto se ve reflejado en la mencionada STC 254/1993 de 20 de julio de 1993, en cuanto señala "[l]*a garantía de la intimidad adopta hoy un contenido positivo en forma de derecho de control sobre los datos relativos a la propia persona. La llamada "libertad informática", es así también el derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data)*" Fundamento jurídico 7. RIASCOS GÓMEZ, L., "El derecho a la intimidad, la visión iusinformática y el delito de datos personales", tesis doctoral, Universidad de Lleida, 1999 [en línea], [Fecha de consulta: 19/102019], Disponible en https://www.tdx.cat/bitstream/handle/10803/8137/Tlorg1de2.pdf?sequence=1&isAllowed=y, pp. 60-61.

[12] 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, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales", *Aranzadi Digital*, 1/2018, 2018, p. 2.

De esta manera, podemos encontrar en la doctrina judicial del TC una evolución caracterizada por esta distinción, con un claro cambio de criterio a través de los años, marcada por un vuelco radical en la última sentencia disponible en la materia. Así, podemos clasificar esta doctrina jurisprudencial en tres periodos, según el elemento predominante: a) Periodo del principio de proporcionalidad; b) Periodo de exigencia informativa estricta y c) Periodo de flexibilidad.

2.1. Periodo del principio de proporcionalidad

Este periodo se va a caracterizar por la consagración -matizada- de la obligación de información previa a los trabajadores, aplicada en conjunto con el principio de proporcionalidad, en la utilización de dispositivos de videovigilancia laboral. Se va a admitir la posibilidad de un control oculto, y por ende carente de información previa, sólo en aquellos casos en que "*con ella se frustraría la finalidad pretendida respecto de un trabajador concreto, sin que exista un medio más inocuo, siendo suficiente con el cumplimiento de los criterios de idoneidad, necesidad y proporcionalidad en sentido estricto*"[13]. De esta manera, "*la falta de información previa y de proporcionalidad de la medida de control determinará la ilicitud de la actuación empresarial y la nulidad de las pruebas que se obtengan derivadas de dichas actuaciones, así como en su caso, de la medida disciplinaria adoptada con base en dichas pruebas (doctrina del fruto del árbol envenenado). Es decir, puede faltar información previa, pero sólo en aquellos casos en que sea estrictamente justificado*"[14].

En esta etapa tenemos como principales referentes[15] a las sentencias del TC 98/2000[16] y 186/2000[17], las cuales establecieron los requisitos para la validez de la videovigilancia laboral, respecto de las cuales expondremos sintéticamente su doctrina junto con los requisitos que establece. El término de este periodo está marcado por la STC 29/2013[18], que va a complementar el criterio de dichas sentencias, aumentando las exigencias, y dando paso al periodo que denominaremos de la exigencia informativa estricta.

El asunto de la STC 98/2000 abre paso al control jurisdiccional del poder de dirección y vigilancia de la empresa, al considerarse que no existía a la fecha una regulación legal

[13] RODRÍGUEZ ESCANCIANO, S., "Videovigilancia empresarial: límites a la luz de la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales", *La Ley Digital*, 15103/2018, 2018, p. 3.

[14] ROJAS ROSCO, R., Y LÓPEZ CARBALLO, D., "El impacto del RGPD en el ámbito del control laboral y la era de la innovación", *Actualidad Civil*, Nº 5, 2018, p. 6.

[15] Podemos agregar además las STC 14/2003, 89/2006 y 96/2012.

[16] STC 98/2000, 1º, de 10 de abril de 2000 (Rec. núm. 4015/1996).

[17] STC 186/2000, 1º, de 10 de julio de 2000 (Rec. núm. 2662/1997).

[18] STC 29/2013, 1º, de 11 de febrero de 2013 (Rec. núm. 10522/2009)

en la materia. En dicho caso, se trata de la instalación permanente por parte de la empresa Casino de La Toja S.A., de micrófonos en la zona de caja y ruleta francesa, a fin de captar el audio de los trabajadores y clientes, y así complementar un sistema de videovigilancia ya existente, sin sospechas previas y concretas de irregularidades -a pesar de ser la denuncia referirse sólo de la captación de audio, el fallo hace aplicable la doctrina a cualquier elemento de control que colisione con la intimidad.

Las conclusiones del TC se oponen a lo fallado en la STSJ de Galicia, el cual consideró que "*el centro de trabajo no constituye por definición un espacio en el que se ejerza el derecho a la intimidad por parte de los trabajadores*"[19], considerando que si bien los derechos fundamentales admiten modulación en el medio laboral, en virtud de la facultad de dirección empresarial, estas limitaciones deben derivar de la naturaleza del trabajo, y que sea acreditada una necesidad e interés empresarial, "*sin que sea suficiente su mera invocación para sacrificar el derecho fundamental del trabajador(...) debiendo ser indispensables, tratándose en definitiva, de la aplicación del principio de proporcionalidad*"[20]. Para el TC, la celebración del contrato de trabajo no priva al trabajador de su derecho fundamental a la intimidad, y si la medida no respeta el test de proporcionalidad, "*constituye una actuación que rebasa ampliamente las facultades que al empresario otorga el artículo 20.3 LET y supone una intromisión ilegítima en el derecho a la intimidad*"[21]. La sentencia sólo se referirá a la afectación de los derechos fundamentales a la intimidad y propia imagen.

Por su parte, la STC 186/2000 trata sobre la instalación de un sistema de videovigilancia oculto tras sospechar de la apropiación de dinero por parte de tres trabajadores, lo cual es verificado con las imágenes obtenidas de las videocámaras, procediendo al despido de un trabajador, el cual impugna dicha medida. La sentencia de instancia declaró procedente el despido, lo que fue confirmado en suplicación ante el TSJ de Asturias, declarándose inadmisible el recurso de unificación de doctrina. Finalmente se recurre de amparo, aduciendo el derecho a la intimidad y propia imagen, con relación al debido

[19] Fundamento de Derecho 6 de la STC 98/2000. Exponemos a su vez con mayor extensión el criterio del TSJ de Galicia: "*de tal manera que las conversaciones que mantengan los trabajadores entre sí y con los clientes en el desempeño de su actividad laboral no están amparadas por el art. 18.1 CE y no hay razón alguna para que la empresa no pueda conocer el contenido de aquéllas, ya que el referido derecho se ejercita en el ámbito de la esfera privada del trabajador, que en el centro de trabajo hay que entenderlo limitado a los lugares de descanso o esparcimiento, vestuarios, lavabos o análogos, pero no a aquéllos lugares en los que se desarrolla la actividad laboral*". Esta doctrina, desconoce garrafalmente la doctrina de ciudadanía en la empresa, o constitucionalización de los derechos laborales, al considerar prácticamente inexistente el derecho a la intimidad y el respeto a la vida privada en el trabajo. Creemos que la rectificación jurisprudencial realizada por el Tribunal Constitucional era imprescindible para despejar las dudas y poner cortapisas a esa peligrosa doctrina.

[20] Fundamento de Derecho 7 de la STC 98/2000.

[21] GONZÁLEZ GONZÁLEZ C., *op. cit.*, p. 5.

proceso, por tratarse de utilización de prueba ilícita, no habiéndose probado por otros medios la irregularidad en juicio. Reitera el TC que "*la constitucionalidad de cualquier medida restrictiva de derechos fundamentales viene determinada por la estricta observancia del principio de proporcionalidad*"[22], y estudiada la medida bajo ese parámetro, se concluye que esta se ajusta dicho principio, toda vez que se aplicó sólo tras sospechas fundadas, además era necesaria para acreditar la irregularidad y se limitó a la zona de caja y durante un tiempo limitado[23], descartando que se haya producido lesión al derecho a la intimidad. Es decir, admite el control oculto, pero de manera excepcional y proporcionada. Se señala por la doctrina que este fallo sirve de primer antecedente para la sentencia 39/2016[24], que flexibiliza el deber de información.[25]

2.2. Periodo de exigencia informativa estricta

La etapa anterior, caracterizada por valorar exclusivamente la afectación de los derechos a la intimidad y propia imagen, culmina con la dictación de la STC 29/2013, en la cual cobra relevancia el derecho a la protección de datos, siendo "*determinante el derecho del trabajador a la información previa y expresa, pues, de lo contrario, se despoja al trabajador de la necesaria protección*"[26]. De ella, es antecedente la STC 292/2000[27], la cual define el contenido esencial del derecho a la protección de datos personales. La relevancia de esta sentencia es que pone como centro de la valoración jurídica al deber de información previa a los trabajadores, y para el caso de no respetarse, no sería siquiera necesario analizar la proporcionalidad de la medida. Por ende, establece dos estadios de análisis: primero, el cumplimiento del deber informativo previo -el que debe ser expreso-, y cumplido este requisito, se pasa un segundo nivel de análisis, en base al principio de proporcionalidad. De no cumplir con cualquiera de estos dos estadios de valoración, la medida se considera lesiva del derecho fundamental a la protección de datos.

Así, la STC 29/2013 se refiere a un Director de Servicio de la Universidad de Sevilla, sancionado con suspensión de empleo y de salario por incumplimiento de horario y jornada de trabajo. Frente a las sospechas, la empleadora utiliza las cámaras destinadas a la seguridad para acreditar el incumplimiento. No obstante, que por aplicación del Convenio Colectivo se preveía la posibilidad de control por medios audiovisuales, a los

[22] Fundamento de Derecho 6, STC 186/2000.
[23] Fundamento de Derecho 7, STC 186/2000.
[24] STC 29/2013, 1º, de 11 de febrero de 2013 (Rec núm. 10522/2009)
[25] CHACARTEGUI JAVEGA, C., "Videovigilancia en el lugar de trabajo y "expectativa razonable de privacidad" según el Tribunal Europeo de Derechos Humanos. Comentario a la sentencia de 9 de enero de 2018 (caso López Ribalda contra España)", *Revista de Derecho Social*, Nº 183, 2018, p. 120.
[26] *Ibíd.*, 124.
[27] STC 292/2000, Pleno, de 30 de noviembre de 2000 (Rec. núm. 1463/2000)

trabajadores no se les informó expresamente la finalidad del tratamiento de sus datos personales[28].

Así, la sentencia expresa que la situación difiere de las STC 98/2000 y 186/2000, en las que se invocan los derechos fundamentales del art. 18.1 de la CE, a diferencia de esta, en que se trata del 18.4.[29] En este punto es importante una distinción con la STC 186/2000, en la cual se considera que el derecho a la información dimanante del art. 64.1.3. d) del Texto Refundido del Estatuto de los Trabajadores[30] -que obligaba a emitir informe de los representantes de los trabajadores previo a la implantación de sistemas de control- es una dimensión de nivel legal -y no constitucional- de los derechos fundamentales del art. 18.1, y, por ende, su omisión, carece de relevancia constitucional.

Ahora, no ocurre lo mismo con el deber de información previa en el caso del derecho fundamental contemplado en el art. 18.4, "*no pudiendo operar una interpretación restrictiva del derecho a la información*"[31]. Parte del núcleo esencial del derecho a la protección de datos es saber quien posee los datos y con qué fin, el cual subsiste, aunque los datos se hayan obtenido sin el consentimiento del afectado, y sobre la base jurídica de la ejecución de un contrato de trabajo. A pesar de existir distintivos anunciando la instalación de cámaras de vigilancia[32], era necesaria la "*información previa y expresa, precisa, clara e inequívoca, de la finalidad laboral a que esa captación podría ser dirigida*"[33]. Finalmente, al constatarse en los hechos probados, además, que las cámaras estaban situadas fuera de las instalaciones donde se prestaban los servicios, y tenían sólo fines de seguridad y no de control laboral, al alterar su finalidad[34] y omitir el derecho a la información[35], se concluye la inconstitucionalidad del tratamiento, declarando nulas las sentencias precedentes y la medida disciplinaria aplicada.

---

[28] GONZÁLEZ GONZÁLEZ C., *op. cit.*, p. 9.

[29] Fundamento Jurídico 6 STC 29/2013.

[30] Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el Texto Refundido del Estatuto de los Trabajadores.

[31] Fundamento Jurídico 6 STC 29/2013, específicamente párrafo 6.

[32] Conforme a la Instrucción 1/2006, de la Agencia Española de Protección de Datos.

[33] ROJAS ROSCO, R., Y LÓPEZ CARBALLO, D., *op. cit*., p. 9.

[34] Como sostiene RODRÍGUEZ ESCANCIANO, S., *op. cit.,* p. 4, "*el parámetro de la finalidad se debe entender de manera restrictiva* (…) *explicitando muy particularmente si pueden llegar a utilizarse para la imposición de sanciones disciplinarias por incumplimientos de las obligaciones dimanantes del contrato de trabajo*"

[35] Al no ser un caso en que se recaba el consentimiento del trabajador para el tratamiento, debe entenderse que "*no hay habilitación legal expresa para hacerlo con omisión del derecho a la información sobre el tratamiento de datos personales*". SANTIAGO REDONDO, M., 2013, "Intimidad, secreto de las comunicaciones y protección de datos de carácter personal. El art. 18 CE", *La Ley Digital*, 11091/2013, 2013, p. 16.

2.3. Periodo de flexibilidad informativa

La doctrina anterior viene a ser modificada sustancialmente por la STC 39/2016, que de manera fundamental viene a concretar una "*atenuación del requisito de información previa*"[36]. De ahora en adelante, lo va a considerar cumplido cuando la empresa coloca los dispositivos informativos en las condiciones que establece la Instrucción 1/2006[37] de la AEPD, aun cuando no se haya informado de forma expresa de la existencia de cámaras de videovigilancia.

El caso resuelto en la STC 39/2016[38] se refiere a la empresa Bershka BSK España S.A., que, frente a irregularidades detectadas en una caja registradora, decide contratar una empresa de seguridad, a fin de instalar un sistema de videovigilancia que grabara dicha caja, sin que se informara a los trabajadores, pero colocando en un lugar visible un distintivo informativo. Se constata que una trabajadora sustrae dinero en distintos horarios y fechas y por ende se le despide, frente a lo que demanda la nulidad del despido, por vulneración del art. 18.1. de la CE.

En instancia se declara procedente el despido, y posteriormente se desestima en suplicación el recurso, por parte del TSJ de Castilla y León. Frente a ello, la trabajadora recurre al amparo constitucional por afectación del art. 18.4.[39] Según la propia STC 39/2016, el caso "*permite perfilar o aclarar su doctrina respecto con el uso de cámaras de videovigilancia en la empresa, siendo la finalidad de la misma aclarar el alcance del deber de información (...) sobre la finalidad de la videovigilancia: si es suficiente la información general, o debe existir una información específica*"[40]. El TC, considera que, mediante el dispositivo informativo perfectamente visible, aunque sea genérico, se cumple con el deber informativo previo, además de cumplir, en el caso, con el principio de proporcionalidad.

Además, se sostiene que el caso no es equiparable al de la STC 29/2013, pues no se trata de un dispositivo que capte todo el interior o exterior del centro de trabajo y de forma permanente, sino que se ha instalado previa constatación de irregularidades, apuntando a un lugar preciso, que es la caja registradora, siendo mas bien equiparable al

[36] CHACARTEGUI JAVEGA, C., *op. cit.,* p. 125.

[37] Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de videovigilancia a través de sistemas de cámaras o videocámaras, que impone la obligación de instalar distintivos con el deber de información del art. 5 de la L.O. 15/1999. No obstante, la Instrucción se entenderá derogada en su totalidad por la nueva LOPD 3/2018.

[38] STC 39/2016, Pleno, de 3 de marzo de 2016 (Rec. núm. 7222/2013)

[39] GONZÁLEZ GONZÁLEZ C., *op. cit*., p. 14.

[40] ROJAS ROSCO, R., Y LÓPEZ CARBALLO, D., *op. cit*., p. 9.

supuesto de hecho de la STC 186/2000, dado además el cumplimiento del principio de proporcionalidad en la medida[41]. De esta forma, concretando un cambio abrupto con relación a su doctrina afianzada en la STC 29/2013, se desestima el recurso de amparo constitucional, no sin tener la sentencia dos votos particulares, de los Magistrados Fernando Valdés Dal-Ré, al que se adhiere la magistrada Adela Asua Batarrita, y el voto particular del Magistrado Juan Antonio Xiol Ríos, ambos con sendas críticas al giro doctrinal, denunciando la gravedad de la argumentación expuesta y la levedad de su fundamentación[42].

Vemos de esta forma que, bajo este criterio, la existencia de sospechas razonables se convierte en una base jurídica para el tratamiento de datos personales sin información previa, lo cual creemos, a la luz del nuevo RGPD y la LO 3/2018, constituye una afectación al contenido esencial del derecho fundamental a la protección de datos personales. Veremos a su vez que este concepto se solidifica en la sentencia López Ribalda II.

3. Naturaleza jurídica de la obligación de información

La obligación o deber de información se entiende como una garantía instrumental del derecho a la protección de datos y se considera parte de su núcleo esencial[43]. Creemos que la naturaleza jurídica de esta garantía es una cuestión clave para determinar dogmáticamente las instancias de afectación de este contenido esencial, frente a lo que intentaremos proponer una estructura de análisis dogmático para verificar la vulneración de derechos fundamentales derivada de medidas de videovigilancia, basado en planteamientos doctrinarios de la jurisprudencia del TC en su etapa de exigencia informativa estricta, encarnada en la doctrina de las sentencias 292/2000 y 29/2013.

Para ello, debemos tener en cuenta la distinción doctrinaria entre normas que establecen reglas y normas que establecen principios, y determinar a cuál de las dos categorías corresponde la obligación de información. Así, "*la diferencia entre las reglas y los principios (...) no es su contenido, sino su función: los principios son enunciados normativos que ordenan hacer algo en la mayor medida de lo posible, fáctica y jurídicamente (mandatos de optimización)*"[44], en cambio las reglas corresponden a

[41] Fundamento Jurídico 1, STC 39/2016.

[42] Apartado I.1. y II. C) del voto particular Magistrado Valdés Dal-Ré.

[43] En los términos de la doctrina contenida en la STC 29/2013, 1ª, Fundamento Jurídico 7, y en la STC 292/2000, que define el contenido esencial del derecho a la protección de datos personales en su fundamento jurídico 7.

[44] UGARTE CATALDO, J. L., "La Colisión De Derechos Fundamentales En El Contrato De Trabajo Y El Principio De Proporcionalidad. tesis doctoral, Universidad de Salamanca, 2011 [en línea], [Fecha de consulta: 25/10/2019], Disponible en:

mandatos que ordenan, prohíben o permiten una determinada conducta, y en caso de infringir el enunciado, la norma se entiende contravenida, sin que admita contravenciones parciales o incompletas o modulaciones basadas en otro interés jurídico relevante. En este sentido, dada su formulación y función, somos partidarios de calificar el deber informativo como una regla normativa, en los términos establecidos en el RGPD y la LOPD 3/2018, pues este no admite modulaciones, y su enunciado contiene un mandato concreto y preciso, en orden a poner a disposición del afectado por el tratamiento de datos, cierta información determinada en la ley[45]. De no hacerlo, la regla que establece el deber de información se entiende incumplida.

Pues bien, en el contrato de trabajo, los derechos fundamentales del trabajador van a admitir modulaciones, en base a una medida adoptada por la empresa fundada en un interés de relevancia constitucional (propiedad o libertad de empresa), debiendo efectuarse, en su caso, un juicio de ponderación. Pero van a existir casos en que no estaremos frente a una colisión de derechos fundamentales, dado que el propio ordenamiento jurídico, a través de una regla legal, ha resuelto cómo debe acomodarse el ejercicio del poder empresarial a dichos derechos. En estos casos, es el mismo legislador quien realiza una suerte de ponderación legislativa, mediante las reglas contenidas en la ley. Aquí es donde va a existir una regla que va a resolver el modo de ejercicio de un derecho fundamental en la empresa, y no un conflicto entre derechos fundamentales como tal[46].

Así, en el caso de contravenir un derecho fundamental cuya formulación está efectuada en base a un principio jurídico, como lo podría ser el respeto a la vida privada o la intimidad, al ser susceptible de modulaciones, si queremos determinar la existencia de afectación, debemos realizar un juicio de ponderación en base al principio de proporcionalidad. Ahora, si el derecho fundamental está formulado a través de la técnica legislativa de regla normativa, o bien, si algunas de las ramificaciones legales de su contenido esencial se expresan en reglas, el ejercicio de las facultades empresariales deberá ajustarse a dicho canon, y de no ser respetado, no cabe hablar de colisión de derechos, sino que cabe hablar directamente de una contravención jurídica que genera un resultado lesivo, prescindiendo de la ponderación constitucional[47] como primera línea de protección, conservándola para un análisis posterior.

---

http://gredos.usal.es/jspui/bitstream/10366/115628/1/DDTTS_Ugarte_Cataldo_J.L._La_colision.pdf p. 53.

[45] Art. 13 del RGPD y art. 11 de la LOPD 3/2018.

[46] UGARTE CATALDO, J. L., *op cit.*, p. 54.

[47] Si bien creemos que otros derechos derivados de la personalidad y dignidad del individuo, como lo son la intimidad y el respeto a la vida privada, también para su modulación legítima requieren de transparencia informativa por parte del empleador -como el denominado *Test Barbulescu*, según TERRADILLOS ORMAETXEA, E., *op. cit.*, p. 144, en el caso del derecho a la protección de datos personales,

Ante este escenario, frente al incumplimiento total o parcial del deber de información, se va a producir una medida de control que afecta directa o, al menos, indirectamente el contenido esencial del derecho a la protección de datos personales, dado que el deber informativo es parte consustancial de este contenido esencial, como una garantía instrumental o externa, integrando el "*núcleo esencial del elemento positivo del derecho a la autodeterminación informativa: el habeas data*"[48].

De esta manera, frente al control por videovigilancia, encontraremos dos estadios de análisis: a) El que estará referido a constatar el cumplimiento del deber informativo, actuando el derecho a la protección de datos como una primera barrera jurídica de contención. Si de los hechos se extrae un incumplimiento de esta obligación de transparencia, debemos necesariamente, entender que se ha producido en esta etapa una vulneración del derecho a la protección de datos personales. b) Sólo para el caso de haber cumplido el deber de información en todos sus extremos[49], pasamos al segundo nivel de análisis, en el cual someteremos las circunstancias fácticas de la medida de control a una ponderación, en base a las reglas del principio de proporcionalidad[50]. Es en esta etapa donde podremos entender vulnerado el derecho a la intimidad, a la vida privada, o el derecho a la protección de datos en alguna otra de sus facetas.

No obstante, en el primer estadio de análisis, vulnerado el derecho a la protección de datos personales -por ejemplo, por incumplimiento imperfecto la obligación de información-, los estándares del principio de proporcionalidad servirán ahora para determinar la entidad de la afectación y el daño producido, y, por ende, para efectos indemnizatorios, como ocurrió en la sentencia López Ribalda I[51]. A su vez, servirá para establecer la posibilidad de, paralelamente, haber sido afectado también el núcleo esencial de otro derecho fundamental, como puede ser el del derecho a la intimidad o el respeto a la vida privada, susceptibles de afectación conjunta o separada. Esto, representa una seria ventaja a la hora de analizar un supuesto de videovigilancia laboral, sobre todo teniendo en cuenta la doctrina edificada en la sentencia López Ribalda II, la

---

esta transparencia informativa tiene manifestaciones positivas concretas, que, en base a su finalidad y formulación, poseen la naturaleza de reglas.

[48] GARRIGA DOMÍNGUEZ A., *Nuevos retos para la protección de datos personales en la era del Big Data y de la computación ubicua*", Dykinson, Madrid, 2016, p. 180.

[49] Como expone TERRADILLOS ORMAETXEA, E., *op. cit.*, p. 162, en cuanto al principio de proporcionalidad señalando que *"también es peligroso si se repara en él levantándose antes el dique que supone el deber de información previa en el caso de los derechos relativos a la privacidad del trabajador*"

[50] Siendo cercano este planteamiento a la técnica argumentativa del TEDH en la sentencia del caso "López Ribalda y otras vs. España. CHACARTEGUI JAVEGA, C., *op. cit.,* p. 127.

[51] GOÑI SEIN, J. L., "Video vigilancia empresarial mediante cámaras ocultas: su excepcional validez como control defensivo <<ex post>>", *Trabajo y derecho: nueva revista de estudios actualidad y relaciones laborales*, Nº 47, 2018, p. 79.

cual reduce o relativiza la exigencia expuesta en este acápite, confundiendo el deber de información con una instancia o etapa del principio de proporcionalidad, y, permitiendo, bajo ciertos supuestos, el tratamiento de datos a través de videovigilancia oculta.

4. Doctrina de la sentencia López Ribalda I

El supuesto de hecho del asunto López Ribalda trata sobre la instalación de cámaras de videovigilancia en un supermercado de la cadena española Mercadona, el cual registraba considerables pérdidas, identificando diferencias entre las ventas y el inventario de productos. En virtud de ello, se decide instalar un sistema de cámaras de videovigilancia, con unas visibles que se instalaron en la entrada del supermercado, y otras ocultas, en el área de las cajas registradoras, a fin de captar los posibles ilícitos por parte de la plantilla. La utilización de dichos dispositivos se realizó de manera permanente, por un extenso periodo de tiempo y captando imágenes de manera indiscriminada, sólo informándose a los órganos de representación y a los trabajadores de las cámaras visibles, pero omitiendo cualquier información respecto de las cámaras ocultas.

De esta forma, recayeron sospechas sobre cinco trabajadoras, acusadas de ayudar a clientes y colegas a hurtar productos, así como de hurtarlos ellas directamente. Luego de exhibirle las grabaciones a la representación legal de los trabajadores, ellas reconocieron los hechos y fueron objeto de despidos disciplinarios. Posteriormente, las trabajadoras recurrieron a la justicia española, la que en la instancia declaró la procedencia de los despidos, lo cual fue ratificado por el Tribunal Superior de Justicia de Cataluña, al considerar legítimas las grabaciones que acreditaban los hechos fundantes del despido. Frente a estas decisiones, optan por recurrir al Tribunal Europeo de Derechos Humanos, por violación del artículo 8 (el derecho al respeto de la vida privada) y del artículo 6.1 (derecho a un proceso justo) del Convenio Europeo de Derechos Humanos.

La sentencia de la Cámara del TEDH, de 9 de enero de 2018, considera vulnerado el derecho al respeto de la vida privada de las trabajadoras[52], por infringir los principios de la normativa de protección de datos. Interesante es este punto, pues aborda la afectación del derecho a la privacidad, pero desde la perspectiva de la recogida de datos y de las normas y principios que la regulan, tanto comunitarios como nacionales. Recordemos que a la fecha de los hechos vulneratorios, aun no entraba en vigencia ni el RGPD ni la LOPD 3/2018, por lo que la normativa interna aplicable al caso es la LO15/1999, que

[52] En este punto, CHACARTEGUI JAVEGA, C., *op. cit.*, p. 121, sostiene que la aplicación del derecho al respeto de la vida privada consagrado en el art. 8 del CEDH es de aplicación o eficacia horizontal, estando obligados a respetarlo no sólo los estados, sino que también los particulares, como se sostiene en la sentencia del TEDH en análisis.

era la norma de transposición de la Directiva 95/46/EC sobre protección de datos. De esta forma, se estima infringido el art. 5 de la antigua LOPD 15/1999, el que establecía el deber de información frente al tratamiento de datos, debiendo haber sido informadas las afectadas de forma previa, expresa, precisa e inequívoca de la existencia de un fichero de datos personales o tratamiento de datos, de la finalidad de la recogida de estos y de los destinatarios de la información[53].

Por otro lado, se entendió infringido el artículo 3 de la Instrucción 1/2006, que obligaba precisamente a instalar un distintivo con la información del art. 5 de la LOPD 15/1999. Considera además el Alto Tribunal[54] que el actuar de la empresa no se condice con el principio de proporcionalidad, estimando que existían otros medios para proteger la propiedad de la empresa[55].

5. Doctrina de la sentencia López Ribalda II

El Estado español decide recurrir en contra de la sentencia de la Cámara, ante la Gran Sala del Tribunal de Estrasburgo, esgrimiendo como argumentos fundamentales que la violación de la privacidad de las solicitantes fue producto del actuar de un privado, y no de los tribunales nacionales, por lo que, siguiendo el enfoque del *asunto Von Hannover v Alemania,* lo que el TEDH debía examinar era si la jurisdicción española había sopesado con prudencia los intereses en juego. Por ende, la obligación positiva del Estado español estaba constituida por lograr un justo equilibrio entre los derechos de las partes, obligación que en el asunto *sub lite* se habría satisfecho totalmente. Por otro lado, se aduce que el caso presenta más similitudes con el *asunto Köpke*, debiendo alejarse de la hipótesis del *asunto Barbulescu*, toda vez que la intromisión en la vida privada se daba por razones justificadas, persiguiendo un objetivo legítimo, reducida en el tiempo y limitada a un grupo de trabajadores, los cuales prestaban servicios en las cajas registradoras.

Es así como la Gran Sala, en cuanto a la naturaleza de la obligación de los Estados derivada del artículo 8 del Convenio Europeo de Derechos Humanos, tiene en cuenta

[53] GOÑI SEIN, J. L., *op. cit.*, p. 77.

[54] Digamos en este punto que la sentencia del TEDH finalmente considera que la incorporación a juicio de las pruebas constituidas por las imágenes de videovigilancia oculta no afectó el debido proceso, toda vez que las afectadas tuvieron oportunidad para impugnar la validez de la prueba, y que los hechos imputados fueron probados principalmente con otros medios de prueba, como testigos, habiendo sido entregadas por el Estado Español las garantías de un juicio justo. No obstante, considera vulnerado su derecho a la protección de la vida privada. Frente a esta última afectación, el Tribunal otorga una indemnización de 4.000 euros por daños morales y entre 500 y 568.86 euros por gastos y costas. GOÑI SEIN, J. L., *op. cit.*, p. 79.

[55] ROJAS ROSCO, R., Y LÓPEZ CARBALLO, D., *op. cit*., p.16.

que las obligaciones positivas y negativas derivadas de dicha norma no presentan una definición precisa y clara, debiendo tener en cuenta mas bien un justo equilibrio entre los intereses privados y públicos en colisión, lo cual se encuentra dentro del margen de apreciación y competencia de cada Estado[56]. Para ello, cada país obligado tiene la facultad de definir discrecionalmente si para cumplir esa obligación dimanante del artículo 8 del CEDH va a adoptar un marco legislativo específico, o lo va a hacer mediante el establecimiento de instancias o recursos suficientes para dar protección eficiente al derecho en cuestión. En particular, respecto del control de la actividad laboral, con independencia de esta discrecionalidad relativa a la normativa interna, cada Estado debe asegurar la proporcionalidad y la protección frente al abuso empresarial[57].

Se deja asentado que, al momento de ocurrir los hechos, el marco legal destinado a la protección de la vida privada de los afectados por videovigilancia estaba constituido por la LO 15/1999 y la Instrucción 1/2006[58] de la Agencia Española de Protección de Datos[59], además del artículo 20 Nº 3 del TRET. Por otro lado, se constata el marco jurisprudencial de los tribunales ordinarios y del Tribunal Constitucional[60], en virtud de la cual, se debía dar pleno cumplimiento al principio de proporcionalidad en la medida -siendo coetáneo a los hechos el que denominamos *periodo del principio de proporcionalidad*-. En este entendido, y no siendo debatido dicho contexto legal ni de doctrina judicial, se ponderarán por el Tribunal los factores tenidos en cuenta por la judicatura española al momento de sopesar los intereses en contradicción.

El Tribunal sostiene que para efectuar la ponderación de las medidas de control laboral mediante videovigilancia se deben tener en cuenta ciertos principios, denominados por la doctrina como *Test Barbulescu*, consagrados en la sentencia homónima, y que serían aplicables *mutatis mutandi* al caso en cuestión, los cuales serían: i) Comunicación de la

[56] Fundamento 111 Sentencia López Ribalda II (en adelante se citará sólo en base al número del fundamento).

[57] Fundamento 114.

[58] Instrucción que, si bien, en su artículo 3 letra b) ordena comunicar al menos la información mandatada en el artículo 5.1 de la LO 15/1999, su existencia fue criticada por alguna parte de la doctrina en su momento, dado que daba lugar a distorsiones en la forma de comunicar la información a toda la plantilla de forma efectiva. Véase SEPÚLVEDA GÓMEZ, M., "Poder de control empresarial mediante cámaras de videovigilancia y derecho de los trabajadores a la protección de datos personales", *Revista Temas Laborales*, Nº 133/2016, 2016, p. 233, toda vez que se considera que *"una mera Instrucción de un organismo público no es fuente formal ni material de Derecho como para que se pueda interpretar que la colocación de un distintivo informativo previsto en el Instrucción sustituye sin más y en todo caso, el deber de información previsto en una Ley Orgánica*".

[59] Fundamento 119.

[60] SSTC 186/2000 y 98/2000 en el que denominamos periodo del principio de proporcionalidad; 29/2013 en el periodo de exigencia informativa estricta y 39/2016 en el periodo de flexibilidad informativa. Recordemos que, a la fecha de los hechos, sólo se había dictado el primer grupo de sentencias.

posibilidad de aplicar medidas de vigilancia y su implementación; ii) El alcance del monitoreo; iii) Razones legítimas por parte del empleador; iv) Las consecuencias del monitoreo, en cuanto al uso de los datos y si se han utilizado para fundar alguna medida; y v) Contar con garantías adecuadas cuando el monitoreo es de naturaleza intrusiva[61]. Por ende, la Gran Sala utilizará dichos principios a fin de determinar si, tanto la legislación como la aplicación de ésta por parte de los tribunales nacionales -mediante una justa ponderación de intereses-, dio efectiva garantía al derecho a la protección de la vida privada de las solicitantes[62].

Es así como la Gran Sala del Tribunal de Estrasburgo determinó que los tribunales nacionales ponderaron de manera adecuada que la instalación de videocámaras había sido justificada por razones legítimas (sospecha del gerente del supermercado ante constantes pérdidas), y en virtud de un interés legítimo (descubrir y sancionar a los responsables), considerando que el alcance de vigilancia fue limitado (en cuanto al lugar y al personal afectado) y en un lapso acotado de pocos días. Esta evaluación, para el TEDH, no puede considerarse irrazonable.

Por otro lado, y en un aspecto no menos relevante, para la Gran Sala, el hecho de haber efectuado la videovigilancia en un espacio abierto al público es un factor para valorar el nivel de afectación del derecho en cuestión, pues mientras más abierto al público el lugar del control, menor es la expectativa de privacidad que puede esperar el trabajador razonablemente[63]. Finalmente considera que la medida fue necesaria, pues se empleó para descubrir a los agentes de la conducta denunciada y obtener el material probatorio pertinente, no habiendo otros medios menos lesivos para conseguir la finalidad propuesta -dejando establecido que la transparencia de la vigilancia hubiese anulado su objetivo-.

5.1. Doctrina relativa al deber de información

Uno de los elementos centrales de la decisión del Tribunal de absolver al Estado español, es la consideración jurídica de la obligación o deber de información y su naturaleza jurídica. En una verdadera revolución copernicana se convierte este pronunciamiento, toda vez que, a pesar de reconocer la plena vigencia de la obligación legal[64] de informar[65], considera que su omisión es plenamente excusable, basado en la protección de un interés público o privado de relevancia, pasando a ser un criterio más

[61] Fundamento 116.
[62] Fundamentao 117.
[63] Fundamento 93.
[64] Contenida en el artículo 5 de la LO 15/1999.
[65] Fundamento 133.

en la ponderación del principio de proporcionalidad[66], sufriendo una verdadera absorción doctrinaria.

Así, en caso de faltar esta información, la consecuencia sería, en cada caso en concreto, aumentar el estándar de exigencia de la idoneidad, necesidad y proporcionalidad en sentido estricto. Esto, sumado al hecho de no haber utilizado las solicitantes otros recursos existentes en el ordenamiento jurídico español, como los contenidos en la LO 15/1999, o bien, el ejercicio de un posible reclamo ante la Agencia Española de Protección de Datos, crean en la Gran Sala la convicción de no haberse configurado violación al artículo 8 del CEDH ni tampoco incumplimiento por parte de España de las obligaciones positivas emanadas de dicha norma[67].

6. Aspectos especialmente problemáticos de la sentencia

Expuestos los términos de la sentencia López Ribalda II, debemos analizar, desde el punto de vista doctrinario, cuáles son los principales conflictos que su fundamentación jurídica puede traer aparejada en materia de protección de la vida privada de los trabajadores. Si bien es claro que cada Estado tiene un margen de reserva en la adopción de medidas legislativas destinadas a garantizar este derecho fundamental, debemos poner acento en aquella expresión de la discrecionalidad relativa a la ponderación de intereses efectuada al momento de aplicar dicha legislación interna. Por ello, la doctrina de la sentencia de la Gran Sala, eventualmente, en la praxis jurídica, puede significar una suerte de *reformatio in peius* en contra de la parte trabajadora, si no se toman en cuenta ciertas consideraciones doctrinarias relevantes.

Actualmente, a nivel legislativo, es claro el reemplazo orgánico de la normativa comunitaria y nacional. Tanto el Reglamento de Protección de Datos 2016/679 -como norma europea de aplicación directa- y la Ley Orgánica de Protección de Datos Personales -como norma de desarrollo y adaptación de la primera- rigen con plenitud en el ordenamiento jurídico español. Esto, conlleva que, al menos a nivel normativo, el principio de transparencia y la obligación de información hayan sido consagrados como parte del edificio central del derecho a la protección de datos personales, y, en consecuencia, de la vida privada de las personas físicas. Esta nueva regulación confirma y profundiza el deber de información como una obligación positiva, esta vez con delimitación expresa de sus dimensiones formales y sustanciales[68].

[66] Fundamento 131.
[67] Fundamento 137.
[68] En los artículos 12 y 13 del RGPD y en los artículos 11, 22 y 89 de la LOPD 3/2018.

Por otro lado, en cuanto a la forma que tiene el Estado, a través de sus tribunales, de ponderar los intereses y derechos contrapuestos en la ecuación, creemos que se crean problemas aplicativos complejos, ello, en razón de fundir a la obligación de información en el crisol del principio de proporcionalidad, restándole fuerza normativa. Por otro lado, la utilización del concepto -en sentido amplio- de *sospecha razonable* como legitimación de controles no informados, puede terminar legitimando la utilización de videovigilancia oculta o clandestina, como veremos a continuación.

6.1. La expresión difusa de la obligación de información

En particular, respecto del estado en que esta doctrina deja posicionado al deber de información, debemos plantear una clara preocupación. Ello, pues 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, obligando a una necesaria apreciación judicial de los hechos, en desmedro de la garantía legal concreta entregada al trabajador consistente en el cumplimiento irrestricto del derecho a ser informado. En otras palabras, se abre una peligrosa puerta a la legitimación de videovigilancia oculta condicionada.

A fin de determinar la incidencia de esta doctrina en el quehacer interpretativo de los tribunales españoles en la actualidad, debemos hacer una comparativa entre el contexto normativo vigente a la época de los hechos del asunto López Ribalda y el actual, a fin de calificar la procedencia de la doctrina analizada. El año 2009, regía con plenitud la LO 15/1999, de 13 de diciembre, sobre Protección de Datos de Carácter Personal. Esta, en su artículo 5 número 1, sobre "*Derecho de información en la recogida da datos*", ya establecía que "*Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco: a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de estos y de los destinatarios de la información*". Es decir, al momento de ocurrir los hechos litigiosos, existía la obligación determinada y positiva de transparentar el tratamiento, incluyendo la finalidad de este.

Actualmente, la LO 3/2018 consagra igualmente el deber de información, mediante la técnica de información por capas[69], es decir, crea la obligación de entregar al afectado cierta información básica, indicando a la vez una dirección electrónica u otro medio que permita acceder al resto de la información con un nivel superior de detalle. A pesar de ello, dentro de la primera capa de información, se encuentra el contenido básico del artículo 11, sobre "*Transparencia e información al afectado"* que en su número 2 dispone que se deberá entregar al menos como información básica "*a) La identidad del responsable del tratamiento (...); b) La finalidad del tratamiento y c) La posibilidad de ejercer los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679*". De esta manera, es indudable que dentro de la información que debe proporcionarse está tanto la existencia del tratamiento como la finalidad de este. Esto en materia específicamente laboral, se ve refrendado en el artículo 89 de la misma ley, en cuanto mandata en materia de videovigilancia que "[l]*os empleadores habrán de informar con carácter previo, y de forma expresa, clara y concisa, a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de esta medida*"[70].

Tomando en consideración el contrapunto de estos dos marcos legislativos -en ambos se consagra de forma positiva y determinada el deber de informar el tratamiento, sin excepciones[71]- y teniendo en cuenta la reciente doctrina del TEDH -que relativiza las consecuencias jurídicas del incumplimiento de esta obligación- no podemos sino deducir que la amenaza de legitimar la videovigilancia oculta condicionada es cierta y

[69] En este punto es interesante lo afirmado por BAZ RODRÍGUEZ, J., en cuanto se reconocen las dificultades y riesgos de conciliar el sistema de información por capas (que busca minimizar los contenidos) con "l*a exigencia de concisión y claridad que preside la filosofía general del RGPD en relación a los principios de licitud, lealtad y transparencia*". BAZ RODRÍGUEZ, J., "La Ley Orgánica 3/2018 como marco embrionario de garantía de los derechos digitales laborales. Claves para un análisis sistemático", *La Ley Digital,* 6823/2019, 2019, p. 15.

[70] A esto sumemos las disposiciones 12 y 13 del RGPD, las cuales consagran el deber de información en su dimensión material y formal. La dimensión material está constituida por el contenido de la información que deberá facilitarse al interesado cuando los datos se obtengan directamente del él. Así, entre otros aspectos, en base al art. 13 del Reglamento, se deberá informar: a) la identidad y los datos de contacto del responsable; b) los datos del delegado de protección de datos, en su caso; c) los fines del tratamiento a que se destinen los datos personales y la base jurídica del tratamiento. la dimensión formal del derecho a la información la encontramos en el art. 12, en cuanto exige al responsable tomar todas las medidas oportunas para facilitar al interesado la información completa del art. 13, de manera concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, por escrito o por otros medios, incluso electrónicamente.

[71] Salvo la del art. 89.1 párrafo segundo de la LOPD 3/2018, el cual establece una verdadera excepción al deber de información, pero en ningún caso legitima la videovigilancia oculta. La norma establece que, para efectos de captar un acto ilícito en el entorno laboral, se entenderá cumplido el deber informativo cuando existiese al menos el dispositivo del art. 22.4, es decir, un distintivo con información básica indicando la existencia de videovigilancia, pero no obligando a informar la finalidad del control, por lo que habilita para un control oculto relativo y no absoluto.

actual, en plena vigencia de la LO 3/2018 y del RGPD. Si bien la normativa vigente eleva los estándares en materia de transparencia, creemos que de la misma forma como no fue suficiente la LO 15/1999 para confirmar el criterio de la sentencia López Ribalda I, es factible que la LOPD 3/2018 tampoco sea una barrera infranqueable para la doctrina que introduce al deber de información en la lógica del juicio de proporcionalidad, restándole mérito y relevancia jurídica a su incumplimiento.

Sostenemos que una respuesta a lo anterior, es lo planteado en el punto 3 de este estudio, en cuanto se considera a la obligación de información como una regla normativa -y no un principio, que admitiría modulaciones basadas en otro interés de relevancia-, la cual en caso de contravención, genera necesariamente una afectación al contenido esencial del derecho a la protección de datos personales, dado que dicho deber de información se encuentra indisolublemente unido al núcleo irreductible del mencionado derecho fundamental. Sin cumplimiento de esta obligación de información no pueden operar los derechos de acceso, rectificación, cancelación, etc., y por ende, se priva de cimientos al evolucionado edificio de la protección de datos, que, en este caso, constituye una manifestación interna o nacional del mandato de protección al respeto a la vida privada, consagrado en el artículo 8 del CEDH, cuya arquitectura y revestimientos están contenidos en la LOPD 3/2018.

Esta problemática fue de alguna forma recogida en el voto conjunto disidente de los jueces De Gaetano, Yudkivska y Grosev, el cual en sus apartados 6 y 7, visibiliza la relativización de la obligación de información, la que constituía un deber legal claro y determinado, contenido expresamente en el artículo 5 de la LOPD 15/1999. Denuncia además este voto particular que la determinación de la Gran Sala degrada el deber de información a la categoría de obligación meramente legal, bajo el tenor de la STC 186/2000[72], obviando la doctrina que lo considera parte del contenido esencial del derecho a la protección de datos personales.

6.2. El concepto de "sospecha razonable"

Absolutamente vinculado al punto anterior está el concepto utilizado por la Gran Sala de "*sospecha razonable*". Ello, toda vez que se le entrega a este la entidad de eximir de responsabilidad al empleador que incumple con la obligación de información, degradando así las consecuencias jurídicas de la referida contravención legal. Sin perjuicio de ello, en la sentencia se aclara que no es aceptable la premisa referida a que la más mínima sospecha produciría este efecto jurídico. Por ende, veamos qué entendemos por sospecha razonable para poder después analizar sus implicancias.

[72] Fundamento 7º del voto conjunto disidente.

Este concepto, no ha sido definido en la ley, por lo que han sido la jurisprudencia, especialmente en materia penal, que ha interpretado y delimitado el término *sospecha* como "*el estado de conjetura o suposición que carece de las condiciones necesarias para probar un hecho, (...) es la que surge en el momento inicial de una investigación o en un momento inmediatamente anterior y que debe llegar a su fin cuando se hayan obtenido suficientes pruebas prima facie incriminatorias*"[73]. Por su parte, el término *razonable* de la sospecha se ha entendido como "*la creencia de buena fe del policía que realiza la detención, aunque no existan datos objetivos en donde basar dicha creencia*"[74].

Si bien estos alcances han sido formulados por la doctrina y jurisprudencia penal en materia de los fundamentos de una detención, estos pueden ser aplicados *mutatis mutandis* al caso en cuestión, tomando en cuenta que, a pesar de ser un asunto dado en el contexto laboral, los amplios poderes de dirección y disciplina del empleador se expresan en una suerte de poder punitivo en el contexto empresarial, derivando de ello la teoría de la ciudadanía en la empresa, nacida, precisamente, con la finalidad de imponer límites a este poder y entregar garantías en el ejercicio de los derechos fundamentales específicos e inespecíficos del trabajador. 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.

Por otro lado, creemos que el mayor problema no pasa por el contenido y alcances del concepto, sino por las consecuencias que se le atribuyen en la sentencia. Estas sospechas razonables se utilizan con la finalidad de justificar la videovigilancia no informada, tal y como lo declaró el Tribunal Superior de Justicia de Cataluña[75] en las instancias nacionales del caso en análisis.

Esto, es coincidente con la doctrina de la STC 186/2000, propio de lo que denominamos *periodo del principio de proporcionalidad* en el apartado 2 de este artículo. Cabe hacer presente que la doctrina consagrada en dicha de dicha etapa está marcada por la inexistencia de una legislación específica en materia de protección de datos y la carencia de un deber de información concreto establecido en la ley[76]. Por ende, no deja de ser cuestionable la argumentación jurídica de la Gran Sala, toda vez que homologa,

[73] CUADRADO SALINAS C., Claves "La investigación policial del delito", *La Ley Digital*, 13625/2010, p. 13.
[74] *Ibídem*
[75] Fundamento 34.
[76] Como se constata en la STC 98/2000.

en la praxis, el contexto legislativo del asunto López Ribalda a uno carente de obligación positiva de informar la videovigilancia.

Para el voto disidente, el hecho de estar frente a conductas constitutivas de delito crea la necesidad de canalizar dicha situación a través de los cuerpos policiales, previo a tomar la decisión de acudir a métodos de videovigilancia ocultos. Ante la ausencia de garantías procesales claras deviene en insuficiente el concepto de sospechas razonables como justificante del actuar ilegal o como eximente de responsabilidad frente al incumplimiento de la obligación de informar. Si bien se trataría de una salvaguardia importante, no sería suficiente para garantizar los derechos a la privacidad, teniendo presente incluso, que, en materia penal la vigilancia secreta procede frente al estricto cumplimiento de garantías procesales de relevancia.

7. Consideraciones finales

En la actualidad la doctrina preponderante del TC español es aquella que denominamos de flexibilidad informativa, pues autoriza un tipo de videovigilancia oculta relativa, es decir, tolera que no se comunique la finalidad específica del tratamiento, pero a la vez exige, como mínimo, la instalación de un distintivo que alerte al afectado de la presencia de videocámaras. Esta tendencia, si bien es menos protectora de la vida privada de los trabajadores que su antecesora consagrada en la STC 29/2013, de alguna forma establece un marco informativo mínimo, a fin de transparentar los controles por videovigilancia, con prescindencia incluso de la justificación esgrimida por la empresa. Aun cuando existan sospechas razonables o atendibles acerca de comisión de actos ilícitos, debe cumplirse con un nivel de información mínimo.

Esto es en alguna medida consistente con la doctrina -expuesta en el apartado 3- relativa a la naturaleza jurídica de la obligación de información en materia de protección de datos personales. Al entender esta obligación como una regla normativa consustancial al núcleo irreductible de este derecho, su contravención dará lugar a un resultado que lesiona indefectiblemente este contenido esencial. Dado que no estamos en presencia de un principio jurídico, es decir un enunciado que da lugar a una posible colisión con otro mandato de similar entidad y naturaleza, el cumplimiento irrestricto de este deber de información se transforma en un requisito indispensable para que la recogida de datos sea calificada como legítima, y que a su vez, no admitiría modulaciones a partir de un interés igualmente relevante o justificaciones de su incumplimiento en base a conceptos como el de sospecha razonable.

Teniendo en cuenta el actual contexto normativo europeo y español, caracterizado por recientes modificaciones legales en materia de protección de datos personales, así como

la evolución de la doctrina del TC, podemos sostener que los razonamientos jurídicos consagrados en la sentencia López Ribalda II vienen a establecer un serio retroceso en materia de garantías a la privacidad de las personas físicas, específicamente en el espacio de trabajo. Ello, dado que -sin perjuicio de las discusiones que han generado ciertas disposiciones problemáticas de la LOPD 3/2018- la tendencia va encaminada a la prohibición de los controles por medio de videovigilancia oculta, en pos de cumplir con el deber de información. Actualmente resulta difícil encontrar alguna disposición nacional o comunitaria que legitime esta práctica, inclusive en caso de ilícitos, optando al menos, por aceptar el cumplimiento del deber de informar mediante la colocación de un dispositivo con información minimizada[77].

El principal riesgo de la doctrina consagrada en la sentencia del TEDH está en la aceptación jurisprudencial de los controles clandestinos, sin tomar en consideración las disposiciones que obligan al responsable del tratamiento de datos personales a cumplir con la obligación de información, pieza clave y presupuesto jurídico básico para el ejercicio de la plena autodeterminación informativa. Uno de los aspectos más problemáticos de esta doctrina está dado por el reconocimiento de la Gran Sala de la existencia de la obligación de información consagrado en la derogada LO 15/1999, y que, a pesar de ello, no se le considerara crucial en la calificación de la apreciación realizada por los tribunales españoles. Es más, el peligro de irradiación de esta sentencia para el actual contexto doctrinal español es cierto, toda vez que, a pesar de la actualización de la normativa en materia de protección de datos, no ha existido una modificación sustancial en la carga que pesa sobre el empresario de informar este tipo de controles.

Finalmente, el concepto de "*sospecha razonable*" como elemento de exención de responsabilidad frente al incumplimiento del deber de información, 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*. Todo esto, puede incluso hacer aplicable esta doctrina a las decisiones jurisprudenciales venideras, lo cual, nos lleva a un estado de alerta, en que los esfuerzos de la doctrina bien podrían orientarse en asegurar el respeto irrestricto de las garantías destinadas a la protección de la vida privada de los trabajadores en el medio laboral. Creemos que cualquier ponderación derechos en colisión debe partir de la base del escrupuloso cumplimiento de la obligación de información frente al monitoreo y control laboral por

[77] Tal y como ocurre con el artículo 89.1 párrafo segundo de la LOPD 3/2018 *"En el supuesto de que se haya captado la comisión flagrante de un acto ilícito por los trabajadores o los empleados públicos se entenderá cumplido el deber de informar cuando existiese al menos el dispositivo al que se refiere el artículo 22.4 de esta ley orgánica"*.

medio de videovigilancia, como pieza central del ajedrez de intereses en el que se desenvuelve actualmente la autodeterminación informativa.

8. Bibliografía

BAZ RODRÍGUEZ, J., "La Ley Orgánica 3/2018 como marco embrionario de garantía de los derechos digitales laborales. Claves para un análisis sistemático", *La Ley Digital,* 6823/2019, 2019.

CHACARTEGUI JAVEGA, C., "Videovigilancia en el lugar de trabajo y "expectativa razonable de privacidad" según el Tribunal Europeo de Derechos Humanos. Comentario a la sentencia de 9 de enero de 2018 (caso López Ribalda contra España)", *Revista de Derecho Social*, Nº 183, 2018, p. 119-132.

CUADRADO SALINAS C., Claves "La investigación policial del delito", *La Ley Digital*, 13625/2010.

GARRIGA DOMÍNGUEZ A., *Nuevos retos para la protección de datos personales en la era del Big Data y de la computación ubicua*", Dykinson, Madrid, 2016.

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, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales", *Aranzadi Digital*, 1/2018, 2018.

GOÑI SEIN, J. L., "Video vigilancia empresarial mediante cámaras ocultas: su excepcional validez como control defensivo <<ex post>>", *Trabajo y derecho: nueva revista de estudios actualidad y relaciones laborales*, Nº 47, 2018, p. 74-81.

OJEDA BELLO Z., "El derecho a la protección de datos personales desde un análisis histórico-doctrinal", *Tla-melaua*, Volumen 9, Nº 38, 2015, pp. 58-71.

SANTIAGO REDONDO, M., 2013, "Intimidad, secreto de las comunicaciones y protección de datos de carácter personal. El art. 18 CE", *La Ley Digital*, 11091/2013, 2013.

RIASCOS GÓMEZ, L., "El derecho a la intimidad, la visión iusinformática y el delito de datos personales", tesis doctoral, Universidad de Lleida, 1999 [en línea], [Fecha de consulta: 19/102019], Disponible en https://www.tdx.cat/bitstream/handle/10803/8137/Tlorg1de2.pdf?sequence=1&isAllowed=y

RODRÍGUEZ ESCANCIANO, S., "Videovigilancia empresarial: límites a la luz de la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales", *La Ley Digital*, 15103/2018, 2018.

ROJAS ROSCO, R., Y LÓPEZ CARBALLO, D., "El impacto del RGPD en el ámbito del control laboral y la era de la innovación", *Actualidad Civil*, Nº 5, 2018, pp. 1-18.

SEPÚLVEDA GÓMEZ, M., "Poder de control empresarial mediante cámaras de videovigilancia y derecho de los trabajadores a la protección de datos personales", *Revista Temas Laborales*, Nº 133/2016, 2016, 219-235.

TERRADILLOS ORMAETXEA, E., "El principio de proporcionalidad como referencia garantista de los derechos de los trabajadores en las últimas sentencias del TEDH dictadas en materias de ciberderechos, un contraste con la doctrina del Tribunal Constitucional español", *Revista de Derecho Social*, Nº 80, 2017, p. 139-162.

UGARTE CATALDO, J. L., "La Colisión De Derechos Fundamentales En El Contrato De Trabajo Y El Principio De Proporcionalidad. tesis doctoral, Universidad de Salamanca, 2011 [en línea], [Fecha de consulta: 25/10/2019], Disponible en: http://gredos.usal.es/jspui/bitstream/10366/115628/1/DDTTS_Ugarte_Cataldo_J.L._La_colision.pdf