LA VIDEOVIGILANCIA LABORAL Y EL DERECHO A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

ANA GUDE FERNÁNDEZ

SUMARIO

Fecha recepción: 17.03.2014
Fecha aceptación: 9.09.2014

LA VIDEOVIGILANCIA LABORAL Y EL DERECHO A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

ANA GUDE FERNÁNDEZ

Profesora titular de Derecho constitucional
Universidad de Santiago de Compostela

1. LOS NUEVOS INSTRUMENTOS DE CONTROL DEL EMPRESARIO: LAS VIDEOCÁMARAS

Hoy se hace realidad el modelo de sociedad ortopédica que formulaba el Panóptico benthiano, representado como un edificio de forma circular en medio del cual había un patio con una torre en el centro dividida en pequeñas celdas que daban al interior y al exterior y en las que se encontraba en cada una, un obrero trabajando. En la torre central había un vigilante y, como cada celda daba al mismo tiempo al exterior y al interior, su mirada podía atravesar toda la estancia sin que quedara ningún lugar oculto y, por tanto, todo lo que hacían sus habitantes estaba expuesto al vigilante, que, a su vez, veía sin ser observado[1].

Las posibilidades de la electrónica en la actualidad permiten esta función panóptica de un modo ampliado, llegando a generar incluso en la conciencia de los individuos la necesidad de autolimitarse[2], convencidos de la imposibilidad de escapar al siempre presente ojo del vigilante que ni parpadea, ni se fatiga, ni descansa. Las características de las nuevas tecnologías aplicadas a la

[1] Medina Castillo, E., *Las nuevas tecnologías en las relaciones laborales*, en *www.quadernsdigitals.net/index.php?accionMenu=hemeroteca.*

[2] Medina Castillo, E., *Las nuevas tecnologías en las relaciones laborales*, *op. cit.*

empresa facilitan, en primer lugar, la sustitución del control periférico, discontinuo y parcial que anteriormente efectuaban los controladores antiguos que, cronómetro en mano, recorrían la planta de las fábricas tomando tiempos, por un sistema de inspección más avanzado, centralizado, objetivo y realizado por máquinas[3].

La aparición de técnicas de control avanzadas convierte a esta nueva sociedad en una sociedad virtual que no puede prescindir de un trabajo, también transparente[4]. Mientras el sistema de control tayloriano utilizaba al capataz como un agente represivo que apremiaba y presionaba a los obreros para que aumentaran sus rendimientos, los nuevos instrumentos de control están incorporados a la maquinaria empresarial moderna que se nutre de nuevos mecanismos de control. La utilización, por ejemplo, de técnicas como lo que se ha denominado *software in accounting* permite, previa identificación personal del titular, memorizar el número de operaciones efectuadas, los errores cometidos, el tiempo empleado para cada prestación, la cantidad total de trabajo y la frecuencia y duración de las interrupciones en la actividad del empleado[5].

Estos sorprendentes niveles de inspección empresarial, alcanzados con los nuevos dispositivos tecnológicos, plantean, sin embargo, importantes problemas ético-jurídicos al poner en peligro, no solo la libertad y la dignidad de los observados, sino también su propio equilibrio psíquico, y elevar el poder empresarial al grado de «omnipotente, anónimo e invisible»[6].

En investigaciones empíricas se ha demostrado que el control en el lugar de trabajo tiene algunos efectos negativos. De acuerdo con ellas, los trabajadores que son objeto de monitorización tienen más probabilidades de sentirse desconfiados, desmotivados, con menores sentimientos de lealtad y con mayor *stress*. En un estudio en el que fueron analizadas las respuestas de empleados del sector de la comunicación industrial se comprobó que quienes estaban sometidos a vigilancia desarrollaban ciertos «efectos panópticos», incluyendo entre ellos, un sentido reducido de la privacidad, una creciente incertidumbre —inseguridad en el trabajo— y una menor comunicación[7].

---

[3] Agustina Sanllehí, J. R., «Prevención del delito en la empresa. Límites ético-jurídicos en la implementación de los sistemas de videovigilancia», *Revista Electrónica de Ciencia Penal y Criminología,* n.º 11-10, 2009, pág.10: 6.

[4] Mercader Urguina, J. R., *Derecho del trabajo. Nuevas tecnologías y Sociedad de la información*, ed. Lex Nova, Valladolid, 2002, pág. 99.

[5] Medina Castillo, E., Las nuevas tecnologías en las relaciones laborales, *op. cit.*

[6] Bellavista, A., *Il controllo sui lavoratori*, ed. Giappichelli, Turín, 1995, pág. 67.

[7] Agustina Sanllehí, J. R., «Prevención del delito en la empresa. Límites ético-jurídicos en la implementación de los sistemas de videovigilancia», *op. cit.*, pág. 10: 17.

Un segundo estudio basado en los resultados de la misma encuesta, efectuado por otro experto analista, Vorvoreanu, alude a ciertos efectos perjudiciales. Por ejemplo, algunos trabajadores concebían la vigilancia como si se tendiera una trampa a alguien para poder practicar un despido o para adoptar medidas disciplinarias. Otros se sentían tratados de forma infantil. Por último los más intensamente vigilados manifestaban sufrir un descenso en la motivación para sobrellevar mayores cargas de trabajo o para desempeñar puestos de responsabilidad. Asimismo expresaban una lealtad menor a la organización, un nerviosismo creciente y un inferior entusiasmo, incluso, para ir a trabajar[8].

En la actualidad ningún Estado prohíbe con carácter absoluto el control electrónico en el puesto laboral, ni siquiera aquellos países en los que está arraigada una fuerte cultura de protección de la intimidad[9]. El empleador ha pasado a controlar no solo la actividad productiva sino también al propio trabajador. Por eso, se habla de «trabajadores transparentes o de cristal», en alusión a la posibilidad de que toda su vida, laboral y extralaboral pueda ser fiscalizada[10]. En este punto esta actividad de inspección total por parte del empresario puede colisionar claramente con los derechos de los empleados, en especial con su derecho a la intimidad, al secreto de las comunicaciones, a la libertad sindical, a la huelga o a la protección de datos.

El instrumento tecnológico de control al que vamos a prestar atención en este trabajo es la videovigilancia, que puede establecerse por el empresario en el ámbito laboral tanto con fines de seguridad y prevención del delito como para controlar la prestación de trabajo, proporcionándole a aquél una amplia e incontrovertible información, a los efectos de acreditar posteriormente en un juicio los posibles incumplimientos laborales y actuaciones ilícitas.

Una vez en funcionamiento, las cámaras registrarán indistintamente tanto la posible comisión de un delito o un incumplimiento laboral, como algunas manifestaciones inherentes a la intimidad de los vigilados. En su condición de mecanismo de fiscalización de la actividad de los trabajadores no pueden afectar a su esfera personal atendiendo por tal la no relacionada con la prestación labo-

[8] Agustina Sanllehí, J. R., «Prevención del delito en la empresa. Límites ético-jurídicos en la implementación de los sistemas de videovigilancia», *op. cit.*, pág. 10: 17.

[9] Agustina Sanllehí, J. R., «Prevención del delito en la empresa. Límites ético-jurídicos en la implementación de los sistemas de videovigilancia», *op. cit.*, pág. 10: 12.

[10] Segoviano Astaburuaga, M. L., «El difícil equilibrio entre el poder de dirección del empresario y los derechos fundamentales de los trabajadores», *Revista jurídica de Castilla y León,* n.º 2, 2004, pág. 149.

ral[11]. Aunque el lugar de trabajo no constituye un límite infranqueable, sino que es admisible la supervisión de las conductas del operario realizadas fuera del mismo, ésta ha de efectuarse únicamente en circunstancias excepcionales y en todo caso, las actividades observadas deberán tener una relación directa e inmediata con las obligaciones derivadas del contrato[12].

Es preciso tener en cuenta que las videocámaras invaden los derechos de la personalidad de los trabajadores de diferente forma. Las menos agresivas de todas son aquellas en las cuales las imágenes se envían directamente a la pantalla de un monitor en el que no es posible ni la transmisión ni el almacenamiento de las grabaciones. Por el contrario, en los casos en que las cámaras sí permiten realizar estas operaciones, el empresario puede efectuar un aprovechamiento de las imágenes durante más tiempo. Asimismo es conveniente diferenciar entre cámaras analógicas y digitales. La tecnología digital posibilita la transmisión de las imágenes a larga distancia sin cable mientras que en la analógica es necesaria esta conexión entre el monitor y la cámara lo que limita las posibilidades de observación. Los recursos técnicos de estos instrumentos son también un factor a tener en cuenta, esto es, si disponen o no de *zomm*, si son fijos o móviles, etc. Cuanto más completo sea el equipamiento electrónico más grave será el ataque a los derechos de la persona observada, sin perjuicio de que a través de un *software* adecuado se podrá limitar de forma automática la vigilancia o dejar ocultos ciertos espacios de la empresa[13].

De igual modo es preciso aplicar en materia de videovigilancia empresarial, reglas diversas teniendo en cuenta las personas y el lugar que son objeto de observación así como la duración de la misma. Con respecto al colectivo afectado, se debe tomar en consideración si lo que se pretende con las cámaras es prevenir la criminalidad intra-empresarial o por el contrario tiene como objetivo exclusivamente el control laboral, ambas finalidades no son excluyentes, sin perjuicio de que una pueda prevalecer sobre la otra en la mente del empresario. Es preciso examinar la medida en sí misma, cualitativamente no puede tener la misma intensidad el control preventivo sobre un trabajador que sobre clientes o terceras personas ajenas a la empresa. Sin olvidar que la peligrosidad de ambos agentes puede ser la misma, el trabajador pertenece a la empresa con todo lo que ello significa. La relación contractual se convierte en un elemento

[11] Agustina Sanllehí, J. R., «Prevención del delito en la empresa. Límites ético-jurídicos en la implementación de los sistemas de videovigilancia», *op. cit.*, pág. 10: 12.

[12] Rodríguez Escanciano, S., *Vigilancia y control en la relación de trabajo, La protección de datos de carácter personal en los centros de trabajo*, ed. Cinca, Madrid, 2006, pág. 100.

[13] Byers, P., *Die Videoüberwachung am Arbeitsplatz unter besonderer Berücksichtigung des neuen § 32 BDSG*, ed. Peter LangGmbH, Frankfurt, 2011, pág. 20.

distintivo y decisivo. El empleado que se ha incorporado a la esfera de organización del empresario es objeto de una confianza que se manifiesta en una mayor accesibilidad a los bienes de la empresa. En igualdad de predisposiciones o inclinaciones personales al delito, la vulnerabilidad delictiva del empresario es considerablemente mayor frente a sus propios trabajadores que frente a un tercero. Todo ello justifica la adopción de medidas de control más intensas o intrusivas[14].

En lo que se refiere al lugar de observación, habrá que distinguir si el espacio físico sobre el que recae el control pertenece al ámbito estrictamente interno de la empresa o se trata de una zona semipública, en el sentido de que sea un lugar destinado o abierto al público en general en donde deberán extremarse las garantías. En el derecho alemán, por ejemplo, dependiendo si el puesto de trabajo videovigilado se sitúa en un lugar de acceso público o no, los preceptos aplicables de la legislación de protección de datos son diferentes.

Por último, con relación al límite temporal, en tanto que el trabajador no somete toda su persona y obrar al empresario, convendría limitar la duración de la videovigilancia —tenga lugar dentro o fuera del recinto físico de la empresa—. No hay que ignorar las objeciones éticas y las consecuencias psicológicas que comporta una vigilancia permanente en general y de manera especial en los trabajadores. En este sentido es ilustrativo el contenido de la disposición 6.14 del Repertorio de recomendaciones prácticas de la OIT (1997): «Como norma general, no se prohíbe la vigilancia de los trabajadores, pero se fijan límites muy claros. El repertorio señala que los empleadores no tienen la libertad de elegir el método y los medios de vigilancia que ellos consideren como los mejor adaptados a sus objetivos. Por el contrario, deben dar preferencia a aquellos que tengan los menores efectos sobre la intimidad de los trabajadores y velar por las consecuencias que se puedan derivar de la implementación de las medidas de vigilancia».

En el ordenamiento jurídico español no existe ninguna regulación concreta sobre el uso de cámaras o videocámaras en el ámbito laboral, debiéndose estar por tanto a la legislación general sobre la materia que tampoco es muy prolija. La utilización de la videovigilancia por las Fuerzas y Cuerpos de Seguridad del Estado en lugares públicos se contiene en la Ley Orgánica 4/1997 de 4 de agosto (en adelante LOV). Algunos autores propugnan que los principios que en esta norma se contienen deberían ser extrapolados al ámbito laboral, lo que aportaría garantías y derechos a los trabajadores que en la actualidad carecen. El legislador estatal, sin embargo, no ha introducido normativa específica

[14] Agustina Sanllehí, J. R., «Prevención del delito en la empresa. Límites ético-jurídicos en la implementación de los sistemas de videovigilancia», *op. cit.*, págs. 10: 26 y 10: 27.

alguna, expresando así una completa falta de interés por el tema[15]. Únicamente el artículo 20.3 del Estatuto de los trabajadores atribuye al empleador la posibilidad de adoptar las medidas que estime más oportunas de inspección para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales. La utilización de las videocámaras está por tanto admitida en este ámbito, siempre eso sí, tal y como establece el precepto citado, que se guarde en su adopción y aplicación la consideración debida a la dignidad humana de los asalariados.

Esta laguna legal contrasta con el tratamiento concedido al asunto por otros ordenamientos jurídicos de nuestro entorno más cercano, en los cuales, o bien se establece la prohibición absoluta del empleo de la videovigilancia con una finalidad exclusiva de control a distancia de los trabajadores como ocurre, por ejemplo, en Italia con el Estatuto de los trabajadores o en Portugal con el Código de trabajo[16]; o bien se exige la observancia de una serie de requisitos o garantías procedimentales como la transparencia, proporcionalidad y consulta previa a los representantes de los trabajadores como sucede en Francia[17] o Alemania[18].

---

[15] Goñi Sein, J. L., «Videovigilancia y nuevas formas de control del empleador: La perspectiva de la protección de datos», *Anuario de conferencias del Consejo andaluz de Relaciones laborales*, ed. Consejo andaluz de relaciones laborales, 2008, pág. 151.

[16] De acuerdo con el artículo 20.2 del Código de trabajo portugués, el empresario puede utilizar equipamiento tecnológico de vigilancia en el lugar de trabajo siempre que tenga como finalidad la protección y seguridad de las personas y bienes o cuando particulares exigencias inherentes a la naturaleza de la actividad así lo justifiquen. Por el contrario no está permitido si tiene por objetivo exclusivamente controlar el desempeño de la actividad profesional del trabajador tal y como establece el artículo 20.1. del Código laboral de este país.

[17] La Comisión nacional de Informática y libertades públicas (CNIL) de Francia recientemente, a través de una decisión de se ha pronunciado sobre la colocación de un sistema de videovigilancia en los locales del centro comercial E. LECLERC de Bourg-en-Bresse. La instalación constaba de 240 cámaras de las cuales 180 estaban dispersas a lo largo del centro y las otras 60 se situaron en las cajas del hipermercado. La CNIL juzgó desproporcionado el sistema debido al excesivo alcance de las cámaras al filmar el acceso a los servicios, vestuarios, al gabinete médico y a las salas de descanso; y a la permanente vigilancia a la que sometía los trabajadores. Además, como fue constatado por el propio CNIL, tras examinar ciertas secuencias de vídeo extraídas de las cámaras, el dispositivo era utilizado, contrariamente a lo que se había indicado inicialmente, para controlar los horarios de los trabajadores. Por otro lado, las personas grabadas contaban con una información insuficiente, el período de conservación de las imágenes era excesivo y los datos eran almacenados con medidas de seguridad deficientes. En http://www.cnil.fr/les-themes/videosurveillance/actualite/article-videosurveillance-videoprotection/article/videosurveillance-mise-en-demeure-dun-centre-commercial-e-leclerc-pour-surveillance-excessiv/.

[18] En Alemania la videovigilancia en el lugar de trabajo es posible siempre que cuente con la autorización, según establece el § 87.1.6 del Código de trabajo (*Betriebsverfassungsgesetz*), del Comité de empresa (*Betriebsrat*).

2. LA VIDEOVIGILANCIA Y EL DERECHO A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

2.1. El derecho a la protección de datos de carácter personal: Sus rasgos identificadores frente al derecho a la intimidad

Este trabajo se centra en el análisis de los problemas que plantea la videovigilancia en el ámbito laboral a la vista de la normativa reguladora de la protección de datos personales, por eso, hemos considerado oportuno antes de adentrarnos en su estudio, realizar unas consideraciones generales acerca de este derecho denominado también derecho a la autodeterminación informativa, resumiendo de manera muy breve su evolución[19] en el ordenamiento jurídico español hasta alcanzar su plena autonomía del derecho a la intimidad con el que guarda una conexión muy estrecha.

El derecho a la protección de datos ha sido regulado en el derecho español en la Constitución, en el artículo 18.4, como un mandato al legislador para que limite el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos. Nuestra Norma suprema ha sido el segundo texto constitucional después del portugués en advertir la necesidad de proteger a los ciudadanos frente a las tecnologías de la información[20].

La Ley Orgánica 5/1992, de 29 de octubre, de Regulación de Tratamiento Automatizado de los Datos de Carácter Personal (en adelante LORTAD), en un primer momento y luego, la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante LOPD), se encargaron de afrontar esta tutela. Las dos normas se inspiraron en las legislaciones de los países europeos, fundamentalmente en la normativa internacional: la LORTAD en el Convenio 108 del Consejo de Europa, de 28 de

[19] Hernández López, J. M., distingue en la evolución jurisprudencial del derecho a la protección de datos tres fases. La primera, de 1981 a 1993, se caracteriza por la preocupación acerca de los peligros de las nuevas tecnologías y sus repercusiones en los derechos fundamentales. Una segunda, de transición entre 1993 y 2000, en la cual la libertad informática aparece como expresión positiva del derecho a la intimidad. Y la última fase, que se inicia en el 2000 y que se extiende hasta hoy, de reconocimiento pleno de la protección de datos personales como derecho fundamental autónomo. *El derecho a la protección de datos personales en la doctrina del Tribunal constitucional,* eds. Thomson Reuters y Aranzadi, Cizur Menor, 2013, págs. 87-111

[20] Troncoso Reigada, A., T., *La protección de datos personales. En busca del equilibrio*, ed. Tirant lo Blanch, Valencia, 2010, pág. 69.

enero de 1981, para la tutela de las personas con respecto al tratamiento automatizado de datos de carácter personal; y la LOPD en la Directiva 95/46/CE del Parlamento europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a su libre circulación[21].

La LOPD es básicamente una continuación de la LORTAD, reproduce la mayoría de sus preceptos y los de la Directiva 95/46/CE. Pretende ser una norma general de protección de datos pero contiene un gran número de excepciones en lo referido a su ámbito de aplicación y además está afectada por lo previsto en otras legislaciones más específicas, como son la de estadística, el régimen electoral general, el de personal de las Fuerzas Armadas, Registro Civil, Registro Central de Penados y Rebeldes, o la legislación que regula las imágenes y los sonidos obtenidos mediante videocámaras por las Fuerzas y Cuerpos de Seguridad[22].

El Tribunal constitucional español se ha encargado de la construcción del derecho a la autodeterminación informativa en un grupo de sentencias dictadas desde 1993 hasta el año 2000. En la primera, la STC 254/1993, de 20 de julio, lo formuló y denominó de forma imprecisa como libertad informática para después ir poco a poco perfilándolo en sucesivos pronunciamientos. Será en la STC 292/2000, de 30 de noviembre, en la que se que describa con más nitidez el contenido del derecho dotándolo de plena autonomía con respecto al derecho a la intimidad. Y es que ambos comparten el objetivo de ofrecer una eficaz tutela constitucional de la vida privada personal y familiar, y difieren abiertamente en lo relativo a su función, objeto y contenido[23].

En primer lugar, por lo que respecta a la función, mientras el artículo 18.1 de la CE brinda protección frente a cualquier invasión que pueda realizarse en el ámbito de la vida privada y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad (por todas STC 144/1999, de 22 de julio, FJ 8.º), el derecho a la protección de datos se orienta a garantizar a su titular el control sobre los datos personales y su uso y destino, «con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derechos del afectado» (STC 292/2000, de 30 de noviembre, FJ 6.º). Por consiguiente frente al derecho a la intimidad

[21] Troncoso Reigada, A., T., *La protección de datos personales. En busca del equilibrio, op. cit.*, pág. 82.

[22] Troncoso Reigada, A., *La protección de datos personales. En busca del equilibrio*, *op. cit.,* pág. 92.

[23] Garriga Domínguez, A., *Tratamiento de datos personales y derechos fundamentales*, ed. Dykinson, Madrid, 2009, págs. 35-36. Conde Ortiz, C., *La protección de datos personales. Un derecho autónomo con base en los conceptos de intimidad y privacidad,* ed. Dykinson, Madrid, 2005, págs. 40-45.

que reconoce a cualquier persona «el poder de resguardar su vida privada de una publicidad no querida», el derecho a la protección de datos garantiza el poder de disposición sobre los mismos (STC 292/2000, de 30 de noviembre, FJ 6.º). En este punto incide Villaverde Menéndez, para quien estos dos derechos se distinguen por los objetivos que persiguen. El artículo 18.4 CE tutela la confidencialidad de la información referida a una persona y se diferencia del artículo 18.1 CE en que éste ampara el buen uso de la misma una vez ésta se ha revelado a un tercero. Por eso, el derecho fundamental a la protección de datos no es, en sentido estricto, un derecho al secreto o la confidencialidad de los datos sino al control sobre su publicidad, en definitiva, un derecho esencialmente de prestación cuya atención se centra en los datos que permiten identificar a una persona[24].

En segundo lugar, por lo que se refiere al objeto, para el alto Tribunal el derecho a la autodeterminación informativa «no se reduce solo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales». Entre ellos se incluyen no solo «los relativos a la vida privada o íntima de la persona, sino también aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo» (STC 292/2000, de 30 de noviembre, FJ 6.º). También «alcanza a aquellos datos personales públicos, que por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado» (STC 292/2000, de 30 de noviembre, FJ 6.º).

Por último, a diferencia del derecho a la intimidad, «que confiere a la persona el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima de la persona y la prohibición de hacer uso de lo así conocido» (SSTC 73/1982, FJ 5.º, 110/1984, FJ 3.º, 89/1987, FJ 3.º, 231/1988, FJ 3.º, 197/1991, FJ 3.º y en general las SSTC 134/1999, 144/1999 y 115/2000, de 10 de mayo), el derecho a la protección de datos abarcará diversos poderes cuyo ejercicio impone a terceros deberes jurídicos: «el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, a ser informado sobre el destino y uso de esos datos y

[24] Villaverde Menéndez, I., «La jurisprudencia del Tribunal Constitucional sobre la protección de datos personales», *La protección de datos de carácter personal en los centros de trabajo* (Director y Coordinador: Antoni Farriols i Solá), ed. Cinca, Madrid, 2006, pág. 58.

a acceder, rectificar y cancelar dichos datos» (STC 292/2000, de 30 de noviembre, FJ 6.º).

Ahora bien, si el derecho a la autodeterminación informativa garantiza a su titular un poder de control sobre sus datos personales, su uso y destino, su ejercicio presupondrá que el afectado conozca qué datos personales «nada vale si el afectado desconoce qué datos son los que se poseen por terceros, quiénes los poseen, y con qué fin». El Pleno del Tribunal ha señalado, en este sentido, como elemento caracterizador de la definición constitucional del artículo 18.4 CE, de su núcleo esencial, el derecho del afectado a ser informado de quién posee los datos personales y con qué fin y el derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin» a su tenencia y empleo (STC 292/2000, de 30 de noviembre, FJ 7.º).

En el ámbito europeo, el 12 de marzo de 2014, el Parlamento ha dado luz verde al proyecto de reforma del Reglamento Europeo de Protección de Datos. Esta norma tiene como objetivos, entre otros; adaptar la protección de datos a las nuevas demandas del mundo digital (las disposiciones actuales fueron aprobadas cuando únicamente el 1% de los europeos utilizaba Internet); evitar las divergencias existentes en su aplicación por parte de los diferentes Estados miembros con la finalidad de conseguir que el derecho fundamental a la autodeterminación informativa se aplique de manera uniforme en todos los ámbitos de las actividades de la Unión; aumentar la confianza del consumidor en los servicios en línea facilitando una mejor información con respecto a los derechos y a la protección de datos, mediante la incorporación del derecho de rectificación, al olvido y a la supresión, derecho a la portabilidad de datos y de oposición; e impulsar el mercado único digital reduciendo la fragmentación actual.

2.2. Las imágenes como datos de carácter personal y su tratamiento

La instalación de los medios audiovisuales de control en el centro de trabajo supone no sólo un riesgo de pérdida de libertad del trabajador, por el poder de supervisión constante a que se ve sometido en el entorno laboral, sino también, por la posibilidad a través de la conservación de las imágenes y de los datos almacenados obtenidos, de reconstruir perfiles individuales y de utilizarlos potencialmente con fines discriminatorios.

Las imágenes grabadas por las videocámaras tienen la consideración de datos de carácter personal y, en consecuencia, entran dentro del ámbito de aplicación de la LOPD. El estudio de su régimen jurídico legal constituye junto con el

análisis de la jurisprudencia vertida sobre la materia y las opiniones doctrinales más relevantes el objeto principal de este trabajo.

La Directiva 95/46/CE y el artículo 3.a) de la LOPD definen dato personal como «toda información sobre una persona física identificada o identificable»; y persona identificable, como «toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social»[25]. Y el artículo 5.1.f) del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD (en adelante RLOPD), establece que son datos de carácter personal: «Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas[26] o identificables[27]».

En consecuencia, no cabe duda de que las imágenes son datos de carácter personal siempre que permitan la identificación de las personas que aparecen en ellas no afectándoles la LOPD en caso contrario. Es conveniente tener presente que aquí estamos hablando de grabaciones que se toman en el lugar de trabajo, por tanto, lo lógico será pensar que las personas filmadas sean en su mayoría fácilmente reconocibles por tratarse fundamentalmente de los empleados de la empresa.

La segunda cuestión que conviene dilucidar consiste en determinar si la captación y/o almacenamiento de imágenes de los trabajadores en el centro laboral efectuadas a través de videocámaras se rige por la LOPD. El art. 3 de esta norma en la letra c) lo deja muy claro, describe el «tratamiento de datos» como

[25] La misma regulación puede verse en el art. 2 del Reglamento CE n.º 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos.

[26] Según el Grupo del artículo 29: «de modo general, se puede considerar «identificada» a una persona física cuando, dentro de un grupo de personas, se la «distingue» de todos los demás miembros del grupo. Por consiguiente, la persona física es «identificable» cuando, aunque no se la haya identificado todavía, sea posible hacerlo».

[27] Por «persona identificable se entiende «aquella cuya identidad no es conocida (no está identificada), pero es susceptible de llegar a serlo (es identificable). Los datos relativos a estas personas no son directamente atribuibles a una persona determinada, al no aparecer identificada o al no existir una vinculación entre datos y persona; sin embargo, la vinculación de tales datos a la persona a la que se refieren es posible por diversos procedimientos, por lo general técnicos, en principio fácilmente realizables». ROMEO CASABONA, C. M.ª , «Persona identificada o identificable, el afectado o interesado y el procedimiento de disociación en la protección de datos de carácter personal», *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal,* eds. Civitas-Thomson-Reuters, Cizur Menor, 2010, pág. 228.

las «operaciones y procedimientos técnicos, de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias» y la Agencia Española de Protección de Datos (en adelante AEPD), a través de la Instrucción 1/2006, de 8 de noviembre, en sus artículos 1.1[28] y 2[29] lo reitera.

La emisión en tiempo real de las imágenes sin ser almacenadas no representa una recogida de datos personales en sentido estricto. La AEPD ha manifestado al amparo de lo dispuesto en los artículos 3 y 7.2 de la Instrucción 1/2006, que el empleo de sistemas de videovigilancia con fines de seguridad sin grabación de imágenes constituye un tratamiento de datos que obliga a informar del mismo[30] pero no genera ningún fichero. No es posible hablar de una recogida de datos al no haber quedado éstos registrados[31].

La LOPD supera la diferenciación que todavía acoge hoy la LOV, entre tratamiento automatizado y no automatizado de imágenes y sonidos. La legislación anterior, la LORTAD, se aplicaba únicamente a los «ficheros automatizados de los sectores público y privado y a toda modalidad de uso posterior, incluso no automatizado, de datos de carácter personal registrados en soporte físico susceptible de tratamiento automatizado». Sin embargo la LOPD también incluye en su regulación a los datos de carácter personal registrados en soporte físico que sean susceptibles de tratamiento y a toda modalidad de uso posterior de los mismos por los sectores público y privado.

---

[28] Instrucción 1/2006 de 8 de noviembre, de la Agencia Española de Protección de Datos. Artículo 1.1: «La presente instrucción se aplica al tratamiento de datos personales de imágenes de personas físicas identificadas o identificables, con fines de vigilancia a través de cámaras y videocámaras.

[29] Instrucción 1/2006 de 8 de noviembre de la Agencia Española de Protección de Datos. Artículo 2. 1: «Sólo será posible el tratamiento de los datos objeto de la presente instrucción cuando se encuentre amparado por lo dispuesto en el artículo 6.1 y 2 y el artículo 11.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. 2. Sin perjuicio de lo establecido en el apartado anterior la instalación de cámaras y videocámaras deberá respetar en todo caso los requisitos exigidos por la legislación vigente en la materia».

[30] En el Informe 0070/2010 de la AEPD, se cita la sentencia de 15 de junio de 2001 de la Audiencia Nacional en donde se señala la relevancia del derecho de información:»se trata de un derecho importantísimo porque es el que permite llevar a cabo el ejercicio de otros derechos, y así lo valora el texto positivo al pormenorizar su contenido y establecer la exigencia de que el mismo sea expreso, preciso e inequívoco».

[31] Arzoz Santisteban, X., *Videovigilancia, seguridad ciudadana y derechos fundamentales*, ed. Aranzadi, Cizur Menor, 2010, pág. 141.

2.3. El derecho de información y el consentimiento del trabajador afectado por la videovigilancia

La Instrucción 1/2006 de la AEPD en su artículo 3 establece que «Los responsables que cuenten con sistemas de videovigilancia deberán cumplir con el deber de información previsto en el artículo 5 de La Ley Orgánica 15/1999, de 13 de diciembre. A tal fin deberán: Colocar, en las zonas videovigiladas, al menos un distintivo informativo ubicado en lugar suficientemente visible, tanto en espacios abiertos como cerrados y b) Tener a disposición de los/las interesados/as impresos en los que se detalle la información prevista en el artículo 5.1 de la Ley Orgánica 15/1999. El contenido y el diseño del distintivo informativo[32] se ajustará a lo previsto en el Anexo de esta Instrucción».

Según dispone el artículo 6.1 de la LOPD, el consentimiento para el tratamiento de datos deberá ser inequívoco «salvo que la ley disponga otra cosa». Este principio general, sin embargo, pierde ese carácter y queda relegado a una mera condición de licitud porque en el número 2 de este mismo precepto —artículo 6 de la LOPD— se contiene una larga lista supuestos en los que el consentimiento no es necesario. Uno de ellos —el que aquí ahora nos interesa por el tema de objeto de estudio— es el previsto en el inciso segundo: «cuando el tratamiento de los datos se refiere a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y es necesario para su mantenimiento y cumplimiento».

La norma presume que el consentimiento dado por el trabajador para la formalización del vínculo jurídico contractual permite también la recogida y tratamiento de los datos recabados[33], por tanto, es posible la captación de las imágenes sin ningún otro pronunciamiento expreso. El legislador, consciente de la necesidad que tiene el empresario de manejar información sobre sus tra-

[32] La AEPD no dispone de ningún criterio acerca de cuáles deben ser las dimensiones mínimas del cartel informativo de la videovigilancia, únicamente que ha de ser acorde con el espacio en que se vaya a colocar. Respecto de la ubicación no es necesario que se sitúe debajo de la cámara sino que será suficiente, de acuerdo con el artículo 3a) de la Instrucción 1/2006 de la AEPD, hacerlo en un lugar suficientemente visible tanto en espacios abiertos como cerrados. Si se trata de un edificio sometido a videovigilancia será aconsejable su emplazamiento a la entrada del mismo. No es necesario hacer constar que las cámaras registran al mismo tiempo imágenes y sonidos (*Informe jurídico. Cartel informativo 0084/2007 de la AEPD*).

[33] García-Núñez Serrano, F., «La regulación sobre protección de datos personales y su incidencia en el ámbito laboral», *Aranzadi Social*, n.º 5, 2000, pág. 1112. Sagardoy Bengoechea, J. A., *Los Derechos fundamentales y el Contrato de trabajo*, ed. Civitas, col. Cuadernos, Madrid, 2000, pág. 77.

bajadores para la correcta organización productiva y económica de su negocio ha omitido este requisito[34].

El principio de «autodeterminación informativa» no impide, en consecuencia, el tratamiento de los datos del trabajador por el empresario cuyo conocimiento es preciso para el establecimiento y mantenimiento de la relación laboral. No obstante, como observa Sagardoy Bengoechea, «una cosa es que en determinadas circunstancias el empresario quede eximido de requerir el consentimiento del trabajador, y otra muy distinta es que este último desconozca la existencia de un fichero en donde figuran sus datos y el tratamiento que se está haciendo de los mismos»[35], entre otras razones porque afectado tiene derecho a acceder y modificar los datos, si son erróneos o inexactos.

En consecuencia, si aplicamos el régimen general del tratamiento de datos a la videovigilancia en el ámbito laboral, podemos afirmar que el empleador no necesita el consentimiento expreso del trabajador para instalar cámaras en la empresa o proceder al tratamiento de las imágenes que han sido obtenidas con finalidades de seguridad o de control laboral, pero sí se requerirá su consentimiento, sin embargo, si las operaciones descritas tienen otros objetivos o destinos. Si, por ejemplo, se efectúan grabaciones en el interior de una empresa y posteriormente se difunden para hacer publicidad de la misma, en ese caso, sí se precisaría el consentimiento inequívoco del afectado, como dispone el artículo 6.1 de la LOPD. La AEPD en la resolución R/330/2000, de diciembre de 2000 (PS/00088/2000), se ha pronunciado con claridad sobre esta cuestión.

Una empresa periodística procedió a la instalación de cámaras que recogían la actividad de los trabajadores en los locales de la redacción. Volcaban las grabaciones de forma instantánea en Internet, 24 horas al día, 7 días a la semana, con la intención de reflejar la actividad del periódico y así mejorar por tanto la información ofrecida por esa vía. En sus alegaciones la empresa manifestó que la colocación de *webcams* no podía considerarse como tratamiento de datos de carácter personal porque no concurría el requisito de identificabilidad. Al captar las cámaras panorámicas globales de la redacción, las imágenes de las personas aparecían borrosas y además cada 15 segundos se destruía lo grabado, por lo que no había ni tratamiento ni almacenamiento posterior ni, en consecuencia, tampoco era preciso un fichero de datos. Asimismo la parte denunciada adujo, invocando la doctrina constitucional, que las imágenes al haber sido recogidas en el ámbito

[34] Cardona Rubert, M.ª B., «Tratamiento automatizado de datos de carácter personal», *Revista del Trabajo y Seguridad Social*, n.º 16,1994, pág. 97.

[35] Sagardoy Bengoechea, J. A.: *Los Derechos fundamentales y el Contrato de trabajo*, *op. cit.*, pág. 78.

laboral no afectaban a la intimidad personal y familiar de los trabajadores y que en todo caso, contaba con su consentimiento tácito porque la instalación se había realizado a la vista de ellos y se había comunicado al Comité de empresa[36].

La Resolución, confirmada por la sentencia de la Audiencia Nacional de fecha 24 de enero de 2003, apreció una vulneración del deber de consentimiento consagrado en el artículo 6 de la LOPD, al haberse grabado y difundido imágenes y datos de los trabajadores en la red, sin contar con su autorización (a la luz de la legislación en materia de protección de datos, resulta insuficiente el hecho de informar en el Comité de empresa) y sin que tampoco concurriera ninguna causa de exclusión de las reguladas en el apartado 2.º del mencionado precepto. Las imágenes difundidas con el propósito exclusivamente de hacer publicidad no parecían necesarias ni para el mantenimiento ni tampoco para el cumplimiento de la actividad laboral. Por ello, la conducta de la empresa fue tipificada como infracción grave de las previstas en el artículo 44.3.d) de la LOPD.

Si bien el consentimiento del trabajador[37] no es necesario para que se pueda grabar su imagen sí es imprescindible no obstante que el empresario le informe sobre el uso que va a hacerse de sus datos, siendo el contrato el medio idóneo para ello[38]. El artículo 5 de la LOPD describe los extremos sobre los que se debe informar al afectado de forma expresa, precisa e inequívoca: a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información; b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que le planteen; c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos; d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición; e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

---

[36] Desdentado Bonete, A. y Muñoz Ruiz, A. B., *Control informático, Videovigilancia y Protección de Datos en el Trabajo*, ed. Lex Nova, Valladolid, 2012, pág. 63. Goñi Sein, J. L., *La videovigilancia empresarial y la protección de datos personales*, ed. Aranzadi, Cizur Menor, 2007, págs. 87-89.

[37] En el derecho laboral francés el Código de trabajo exige en los artículos L1221-9 y L1222-4 que los empresarios informen de manera individualizada a los trabajadores de la empresa de la presencia de cámaras de videovigilancia. Las videocámaras no deben filmar a los empleados sobre su puesto de trabajo salvo en circunstancias particulares en que sea necesario que las cámara enfoquen el puesto de trabajo, por ejemplo cuando los empleados manipulan bienes de valor o dinero, en estos casos la cámaras grabarán a la caja o la mercancía y no al cajero o las personas que los custodian.

[38] Desdentado Bonete, A. y Muñoz Ruiz, A. B., *Control Informático, Videovigilancia y Protección de Datos en el Trabajo*, *op. cit.*, pág. 107.

El artículo 18 del RLOPD especifica que esta obligación de información se llevará a cabo a través de un medio que permita acreditar su cumplimiento y se mantendrá mientras persista el tratamiento de los datos del afectado por parte del responsable del fichero. Para el almacenamiento de los soportes se podrán utilizar medios informáticos o telemáticos, en particular, se acudirá al escaneado de la documentación en soporte papel, siempre y cuando se garantice que en dicha automatización no ha mediado alteración alguna de los originales.

La jurisprudencia ordinaria se ha pronunciado sobre la trascendencia de este deber para garantizar el derecho fundamental a la protección de datos. La Audiencia Nacional ha señalado en la sentencia de 15 de junio de 2001 que «se trata de un derecho importantísimo porque es el que permite llevar a cabo el ejercicio de otros derechos, y así lo valora el texto positivo al pormenorizar su contenido y establecer la exigencia de que el mismo sea expreso, preciso e inequívoco». Los propios empresarios serán, de manera directa o bien de forma indirecta a través de sus representantes, quienes se encarguen de satisfacer esta obligación. En cualquier caso, lo relevante es que los empleados tengan con carácter previo información de la presencia de los aparatos de control.

La omisión de esta obligación por parte de los empleadores ha sido sancionada en numerosas ocasiones por la AEPD. En la Resolución 681/2004, de 10 de diciembre, encontramos un ejemplo de ello. Se denunció ante la Agencia la colocación de una cámara de vigilancia en un museo sin haber solicitado el consentimiento de los trabajadores y sin justificar el motivo de la instalación. El responsable de la acción informó que los sistemas de videovigilancia habían sido emplazados para controlar a los empleados que a su vez se encargaban de supervisar las instalaciones del museo. Para su defensa jurídica acudió, primero, a la STC 186/2000, de 10 de julio, y seguidamente, a los criterios de necesidad y proporcionalidad. Negó que hubieran sido lesionados los derechos a la intimidad y a la propia imagen de los trabajadores grabados, porque únicamente les habían filmado de espalda y como consecuencia de ello no era posible su identificación.

La AEPD, sin embargo, rechazando el razonamiento de parte, consideró que las imágenes captadas por la empresa, en la que se suponen que los empleados están expuestos a una identificación inequívoca, eran datos de carácter personal. Asimismo entendió que la simple información de la presencia de videocámaras sin advertir de cuál era su finalidad, es decir sin comunicarles a los afectados que las imágenes podían utilizarse para control laboral era insuficiente. La excepción recogida en el artículo 5.3 de la LOPD eximiendo de la obligación de información si del contenido de ésta se deduce claramente la naturaleza de los datos que se solicitan o las circunstancias en las que se recaba tampoco tenía aquí cabida.

En consecuencia, la conducta del empresario fue objeto sanción al constituir una infracción leve tipificada en el artículo 42.2.d) de la LOPD.

A pesar de la sanción impuesta, la AEPD avaló la legitimidad de las cámaras de vigilancia en este asunto, apoyándose para ello en el precedente de la STC 186/2000, de 10 de julio. Según el razonamiento de este organismo público, el artículo 20.3 del ET habilita al empresario para tratar los datos de sus trabajadores sin su consentimiento, siempre que la medida adoptada no supere el juicio de proporcionalidad a que hace referencia el Tribunal constitucional. Y si el alto Tribunal había entendido que la medida asumida por la empresa en un caso similar al aquí enjuiciado había superado el juicio de proporcionalidad, también, por tanto, la actuación del empresario en este supuesto debía encontrarse amparada legalmente por el Estatuto de los trabajadores.

Otro de los casos que por su relación con el tema pueden traerse aquí a colación, aunque se trate de un ámbito diferente al empresarial, es el relativo a una Administración Pública, que instaló un sistema de videovigilancia en los locales de una Gerencia Municipal para supervisar los horarios de sus empleados. Las imágenes y sonidos quedaban registrados informáticamente, y no se hacía constar en carteles informativos el citado tratamiento. La parte denunciada finalizado el período probatorio, en el trámite de audiencia, acudió a la doctrina constitucional, para argumentar que la instalación de esos dispositivos se produjo con el fin de controlar y verificar el cumplimiento de los horarios de los trabajadores, potestad que forma parte de las facultades que se le otorgan al empresario. La AEPD falló en su resolución R/00451/2005 de fecha 20 de julio (procedimiento AAPP/00029/2004) que la Ley Orgánica de Protección de Datos no exime al empleador de la obligación de informar cuando el tratamiento de datos se encuentra habilitado por una norma, produciéndose, por ello, la vulneración del artículo 5 de la LOPD, relativo al deber de información y tipificado en el artículo 44.2.d) de la misma norma como una infracción leve. En todo caso al no existir para los empleados públicos en la Ley 7/2007, de 12 de abril, de su estatuto básico, una norma correlativa al artículo 20.3 del Estatuto de los Trabajadores tampoco podía ser objeto de control la actividad laboral de los mismos.

Por último, no podemos olvidarnos de citar aquí las palabras del Tribunal Constitucional -no se hace mención aquí a las contenidas en la STC 29/2013, de 11 de febrero que por su relevancia será objeto de un epígrafe aparte- refiriéndose a la importancia del deber de información de los trabajadores cuando se procede a la recogida de sus datos personales expuestas principalmente en la STC 292/2000, de 30 de noviembre:

«De suerte que sin la garantía que supone el derecho a una información apropiada mediante el cumplimiento de determinados requisitos legales (artículo 5

de la LOPD) quedaría sin duda frustrado el derecho del interesado a controlar y disponer de sus datos personales, pues es claro que le impedirían ejercer otras facultades que se integran en el contenido del derecho fundamental a que estamos haciendo referencia…» (FJ 6.º).

2.4. El Principio de calidad de los datos. la prohibición de usos incompatibles

Este principio aparece previsto en los artículos 4.1 de la Instrucción 1/2006 de la AEPD, 4.1 de la LOPD y 8 del RLOPD. En ellos se establecen las características que han de reunir los datos, en este caso las imágenes, para ser recogidas y proceder a su tratamiento: adecuadas, pertinentes y no excesivas en relación con el ámbito y finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

Por un lado, en la recogida con carácter general no son admisibles los fines genéricos que permiten cualquier propósito aunque se ajusten a derecho, sino que tienen que ser determinados y su concreción ha de producirse en los siguientes momentos: cuando tiene lugar la declaración e inscripción del fichero, mientras se le da la información al interesado o durante el ejercicio del derecho de acceso[39]. El responsable del fichero asume la obligación de asegurarle al afectado que las imágenes se emplearán para cumplir con el tratamiento y con los objetivos que previamente fueron descritos y posteriormente se le notificaron de la manera más detallada posible.

Por otro lado, es preciso señalar que la finalidad con la que se almacenan las imágenes ha de ser legítima, es decir conforme a la Constitución y a la ley para que se puedan recoger y tratar. En el caso de los ficheros privados es difícil precisar qué se entiende por finalidad legítima —habrá que indagar el objeto social de la entidad— debido a que el responsable privado disfruta de libertad ideológica y de empresa para su establecimiento. Tanto la finalidad de control laboral como la de seguridad son siempre conformes a derecho. Cuando se trata de ficheros públicos, la licitud se ajusta a la competencia del órgano administrativo[40].

Los requisitos de adecuación, pertinencia y prohibición de exceso operan como límites a la captación y almacenamiento de los datos. Por tanto, las imágenes que no cumplan con esta triple condición serán canceladas inmediatamente.

---

[39] Troncoso Reigada, A., *La protección de datos personales. En busca del equilibrio*, *op. cit.*, pág. 398.

[40] Troncoso Reigada, A., *La protección de datos personales. En busca del equilibrio*, *op. cit.*, pág. 396.

En primer lugar, se exige la adecuación, las cámaras han de ser el único medio al que el empresario puede acudir para lograr la vigilancia de su empresa por no disponer de otro instrumento menos restrictivo con los derechos fundamentales para cumplir con este objetivo[41]. El GTA en su Dictamen 4/2004 ha señalado, refiriéndose a los vídeos, que solo se «pueden utilizar estos sistemas cuando otras medidas de prevención, protección y seguridad, de naturaleza física o lógica, que no requieran captación de imágenes (por ejemplo la utilización de puertas blindadas para combatir el vandalismo, la instalación de puertas automáticas y dispositivos de seguridad, sistemas combinados de alarma, etc.) resulten claramente insuficientes o inaplicables en relación con los fines legítimos mencionados anteriormente»[42].

En segundo lugar, se requiere la pertinencia, es preciso seleccionar los sistemas de videovigilancia menos invasivos con los derechos a la intimidad y a la protección de datos de los trabajadores y público en general. Deberá optarse, por ejemplo, por cámaras que únicamente permitan la visualización y no la grabación de las imágenes, que sean fijas en lugar de móviles, que cuenten con circuitos cerrados de televisión y no con tecnología basada en IP o con sistemas de grabación digital conectados a la red, etc.

Y por último, la prohibición de exceso, esto es, ha de descartarse la ubicación de cámaras por toda la empresa, debiéndose limitar la grabación exclusivamente a aquellos lugares en que sea estrictamente necesario y durante el tiempo mínimo indispensable para satisfacer el interés legítimo del empresario[43].

El artículo 4.3 de la Instrucción AEPD y la LOV imponen asimismo unas determinadas prohibiciones: Las cámaras y videocámaras instaladas en espacios privados no podrán obtener imágenes de espacios públicos salvo que resulte imprescindible para la finalidad de vigilancia que se pretende o resulte imposible evitarlo por razón de la ubicación de aquéllas. La observación de espacios públicos está reservada de forma exclusiva a las Fuerzas y Cuerpos de Seguridad del Estado con las competencias que su Ley reguladora les otorga. Cuando se colocan cámaras en las empresas habrá que tener en cuenta si en las entradas o desde las

[41] Goñi Sein, J. L., *La videovigilancia empresarial y la protección de datos personales*, *op. cit.*, pág. 120.

[42] El GTA es el Grupo europeo de Comisarios sobre protección de datos personales, creado al amparo del artículo 29 de la Directiva 95/46/CE, del Parlamento europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales. Está integrado por representantes de las autoridades de protección de datos de los Estados miembros.

[43] Goñi Sein, J. L., *La videovigilancia empresarial y la protección de datos personales*, *op. cit.*, págs. 123-124.

ventanas se puede captar la vía pública o si la prestación laboral se lleva a cabo en espacios abiertos y no privados. La LOV no permite obtener imágenes de propiedades privadas ajenas a la empresa, interiores de viviendas o locales, fincas colindantes, accesos a otras fincas, etc.

Otra importantísima restricción, que procede también del principio de calidad de datos, es que las imágenes no pueden utilizarse para finalidades incompatibles con las que justificaron su recogida, tal y como dispone el artículo 4.2 de la LOPD. Este principio previsto en la derogada LORTAD establecía que a los datos de carácter personal no se les podían dar usos diferentes a aquéllos para los que habían sido recogidos. La LOPD modifica la redacción del precepto sustituyendo «usos diferentes» por «fines incompatibles». Según la doctrina este cambio ha originado interpretaciones diversas y ha provocado una importante quiebra del principio finalista, que se traduce principalmente en una pérdida de garantías para los afectados al permitirse que las imágenes se pudieran adscribir a destinos diversos a los que motivaron el tratamiento[44].

Ni la AEPD ni tampoco la LOPD definieron con carácter general el término incompatible sino que entendieron que lo mejor era hacerlo en cada caso concreto analizando las particulares circunstancias del mismo. Los Tribunales por su parte han realizado una interpretación estricta del término como sinónimo de distinto. En concreto, la Audiencia nacional, en una sentencia de 8 de febrero de 2002, ha descartado acudir a su sentido literal afirmando lo siguiente: «según el Diccionario de la Real Academia incompatibilidad significa repugnancia que tiene una cosa para unirse con otra, o de dos o más personas entre sí», por tanto, «una interpretación literal ampararía el uso de los datos para cualquier fin abriendo una gama indefinida e ilimitada de finalidades, pues es muy difícil imaginar usos que produzcan la repugnancia que evoca la incompatibilidad, por lo que semejante interpretación conduce al absurdo y como tal ha de rechazarse». Ampliar la posibilidad de utilización de los datos, sostiene la AEPD, supondría dejar sin sentido al artículo 6.2 de la LOPD que exige el consentimiento del afectado cuando los datos personales son empleados con otras utilidades. Se trata en consecuencia de una prohibición lógica que obedece, como Bellavista sostiene, a que «el uso multifuncional de datos aumenta no solo el riesgo de la multiplicación ilimitada de los efectos perjudiciales causados por los datos inexactos o incompletos, sino también el de la descontextualización y, por tanto, el de la distorsión de la información»[45].

[44] Goñi Sein, J. L., *La videovigilancia empresarial y la protección de datos personales*, *op. cit.*, pág. 173.

[45] Goñi Sein, J. L., *La videovigilancia empresarial y la protección de datos personales*, *op. cit.*, pág. 173.

La AEPD también en sus resoluciones ha interpretado que finalidades incompatibles es sinónimo de distintas: «Si los datos de acuerdo con el artículo 4.1 de la LOPD solo pueden ser objeto de tratamiento cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido», cuando se les da un uso diferente se está haciendo caso omiso a la prohibición del artículo 4.2 de la LOPD.

En esta misma línea, la OIT, en el Repertorio de Recomendaciones Prácticas de 1996, manifestó que «los datos personales reunidos en función de disposiciones técnicas o de organización que tengan por objeto garantizar la seguridad y el buen funcionamiento de los sistemas automatizados de información no deberían servir para controlar el comportamiento de los trabajadores» (punto 5.4). Y también el GTA referido al ámbito laboral en su Dictamen 4/2004, de 11 de febrero, sostuvo que: «Las imágenes recogidas exclusivamente para proteger la propiedad o detectar, evitar y controlar infracciones graves no deberán utilizarse para acusar a un empleado de una falta disciplinaria menor».

En la doctrina sin embargo encontramos opiniones discrepantes con relación a la utilización de imágenes de los trabajadores que han sido obtenidas por cámaras instaladas exclusivamente, por ejemplo, por razones de seguridad para fines distintos. Desdentado Bonete y Muñoz Ruiz consideran que la prohibición de «usos incompatibles» prevista en el artículo 4.2 de la LOPD no debería operar en el ámbito laboral. Estos autores sostienen que al no ser necesario el consentimiento de los trabajadores para la instalación de las cámaras el uso que se le va a dar a las imágenes resultará completamente irrelevante. A su juicio lo importante es únicamente que el trabajador tenga noticia de que está siendo objeto de un control visual electrónico. Los ejemplos que enumeran para demostrar esta irrelevancia son muy ilustrativos. Se trata de supuestos hipotéticos en los que las cámaras son colocadas en una entidad financiera o en un gran establecimiento comercial con un objetivo concreto: proteger el bien jurídico de la propiedad. Si un trabajador de uno de estos establecimientos roba o hurta un producto no se plantearía ningún problema porque las imágenes podrían ser utilizadas como medio de prueba al quedar incluidas dentro de la finalidad para la que fue instalada la videovigilancia; pero si en lugar de perpetrar estos delitos el mismo trabajador cometiese una agresión sexual en la empresa, aunque la grabación ya no fuese útil para proteger la propiedad de aquélla, lo lógico sería que pudiera ser empleada como medio de prueba para demostrar la comisión de un delito sexual[46]. Esta interpretación ha sido adoptada en alguna ocasión por la jurispru-

[46] Desdentado Bonete, A. y Muñoz Ruiz, A. B., *Control Informático, Videovigilancia y Protección de Datos en el Trabajo*, *op. cit.*, pág. 70.

dencia. El Tribunal Superior de Justicia de Andalucía en una sentencia 9 de enero de 2006 admitió como medio de prueba válido en un juicio de despido, la grabación efectuada de dos trabajadores consumiendo un polvo por vía nasal durante la jornada laboral. Quedó probado que la instalación del sistema de videocámaras se había producido por razones ajenas a la relación laboral, más concretamente, para controlar el desarrollo de los sucesivos sorteos o juegos que se iban ejecutando en el bingo, sin embargo, el Juzgador admitió la utilización de las imágenes para el despido de los trabajadores, es decir, con un propósito completamente diferente al declarado[47].

En la doctrina Goñi Sein mantiene una posición contraria a la defendida por los autores anteriores. A su juicio, del principio de usos incompatibles se deriva la prohibición de aplicar a los trabajadores sanciones disciplinarias por incumplimientos contractuales descubiertos casualmente mediante el empleo de cámaras colocadas con finalidades organizativas, productivas o de seguridad; razones todas ellas ajenas al control de la actividad laboral. Sin embargo es cierto también que el autor matiza esta afirmación diciendo que parece razonable permitir el empleo de los datos con fines disciplinarios, cuando la información que se obtiene de forma casual se refiere a hechos especialmente graves que pudieran ser tipificados como ilícitos penales[48]. Estaríamos en esta ocasión ante un conflicto de derechos que deberá resolverse haciendo prevalecer el bien jurídico más importante. Si para investigar o comprobar la autoría de un delito contra la vida, integridad física o libertad sexual es preciso sacrificar el derecho a la protección de datos la actuación estaría plenamente justificada por ser proporcionada.

El responsable del fichero y de su tratamiento deberá hacer constar expresamente la finalidad del mismo en el momento que lo declara ante la AEPD. Únicamente, de acuerdo con la Instrucción 1/2006, no se requerirá la inscripción del fichero ni la descripción de su uso o utilidad cuando las imágenes no sean almacenadas, esto es, en aquellos casos en que son captadas y reproducidas en tiempo real. Sin embargo, exista o no la obligación de declarar la existencia del fichero, tendrá que definirse con carácter previo la finalidad, explícita y legítima de la captación o en su caso del tratamiento que justifiquen y amparen aquél. La AEPD no dispone, en contra de lo que en ocasiones se cree, de una potestad para «autorizar» la instalación de cámaras sino que se limita a inscribir el fichero cuando lo declara el responsable. La colocación de las cámaras de vigilancia, a

[47] Thibault Aranda, J., *El control multimedia de la actividad laboral*, ed. Tirant lo Blanch, Valencia, 2004, pág. 44.

[48] Goñi Sein, J. L., *La videovigilancia empresarial y la protección de datos personales*, *op. cit.*, pág. 179.

diferencia de lo que sucede en otros países de nuestro entorno, no está sujeta en el derecho español a autorización administrativa alguna. En el derecho francés, por ejemplo, los dispositivos de vídeo deberán ser autorizados por la Prefectura y declarados ante el CNIL (Comisión Nacional de Informática y de Libertades públicas) cuando la instalación de las cámaras se efectúa en lugares no abiertos al público, mientras que si se trata de espacios abiertos al público será el CNIL el órgano competente[49].

2.5. La STC 29/2013, de 11 de febrero

La legalidad de la videovigilancia laboral ha sido enjuiciada tradicionalmente desde la perspectiva del derecho a la intimidad de los trabajadores y en muy pocas ocasiones desde la del derecho a la autodeterminación informativa[50]. Se ajustaba a derecho la captación y grabación de imágenes en el puesto de trabajo siempre que se tratase de una medida conforme al principio de proporcionalidad. En la práctica, sin embargo, lo que sucede es que en muchas ocasiones la captación y almacenamiento de imágenes se vuelve ilegal porque lo que se vulnera es el derecho a la protección de datos y no el derecho a la intimidad de los trabajadores. Seguramente esto tiene que ver con la todavía reciente naturaleza autónoma del derecho a la protección de datos con respecto al derecho a la intimidad.

La STC 29/2013, de 11 de febrero, del Tribunal Constitucional viene a cubrir por fin las expectativas de un sector doctrinal que propugna desde hace tiempo el tratamiento de los asuntos de videovigilancia desde la perspectiva del derecho a la autodeterminación informativa. De ahí que por su relevancia dediquemos un epígrafe específico a su análisis en este trabajo.

El relato de los hechos es el siguiente, ante la sospecha de irregularidades en el cumplimiento de la jornada laboral por parte de un empleado de la Universidad de Sevilla, el director de recursos humanos de este organismo decidió comprobar los horarios de entrada y salida del trabajador. Para ello acudió a unas grabaciones efectuadas por un sistema de vídeo que había sido instalado en el recinto universitario con la autorización de la AEPD para controlar el acceso a los diferentes campus y centros del mismo.

---

[49] http://www.cnil.fr/fileadmin/documents/approfondir/dossier/Videosurveillance/CNIL_Video_au_travail.pdf.

[50] Goñi Sein, J. L.,»Videovigilancia y nuevas formas de control del empleador. La perspectiva de la protección de datos», *op. cit.*, pág. 156.

La Universidad pudo constatar que mientras en las hojas de control de asistencia de la unidad administrativa, el trabajador había consignado y firmado cada día como momento de entrada las 8:00 horas y, de salida, las 15:00 horas, resultaba que, en realidad, había permanecido en las dependencias de su unidad en horarios muy diferentes a los señalados en los controles de firma, acreditándose en una gran parte de los días laborables (cerca de una treintena, según concretan los hechos probados de las resoluciones recurridas) una demora variable en la hora de llegada al trabajo de entre treinta minutos y varias horas. Como consecuencia de ello, tras el visionado de las cintas se le impusieron por parte de la Universidad al empleado, tres sanciones de suspensión de empleo y sueldo de tres meses cada una originadas por la comisión de varias faltas muy graves. Faltas reiteradas e injustificadas de puntualidad en la entrada al trabajo durante diez o más días en un mes; transgresión de la buena fe contractual y abuso de confianza, consistente en hacer constar en las hojas de control de asistencia una hora de inicio de la jornada laboral que no se correspondía con la real; y ausencias en el trabajo durante más de tres días en un mes.

El trabajador impugnó dichas sanciones primero ante el Juzgado de lo Social n.º 3 de Sevilla que denegó su pretensión y posteriormente ante la Sala de lo Social del Tribunal Superior de Justicia de Andalucía que también desestimó el recurso. Ambas resoluciones se situaron en la línea jurisprudencial defendida por el propio Tribunal Constitucional en la sentencia 186/2000, de 10 de julio: tras la ponderación de los intereses en juego y una vez verificado el cumplimiento del principio de proporcionalidad se justificaba por el Constitucional un control oculto y se consideraban válidas a efectos probatorios las imágenes captadas por unas cámaras que se habían colocado por la empresa, sin conocimiento de los trabajadores ni de sus representantes, con el fin de comprobar unas concretas actuaciones irregulares.

El alto Tribunal en la sentencia que estamos analizando, la STC 29/2013, examinó exclusivamente el asunto desde el plano del derecho a la protección de datos olvidándose por completo del derecho a la intimidad como se preocupó de dejar claro al inicio del fundamento jurídico 4º: «Es preciso aclarar que, pese a existir una cita plural (apartados primero y cuarto del artículo 18 de la CE), la demanda se contrae exclusivamente a lo dispuesto en el número cuatro de dicha previsión constitucional, ya que estima que el tratamiento de las imágenes obtenidas del trabajador vulneró «su derecho fundamental a la autotutela informativa». A juicio del máximo intérprete constitucional el objeto central del asunto consistía en averiguar si se había producido una vulneración del artículo 18.4 de la CE como consecuencia de la utilización de unas grabaciones con una finalidad diferente para la cual las cámaras habían sido instaladas, teniendo en cuen-

ta que en ningún momento la Universidad había advertido a los trabajadores de que las imágenes podían ser utilizadas para controlar su actividad laboral.

El Ministerio fiscal se opuso al otorgamiento del amparo demandado por el trabajador. Sostuvo que el empleo de las imágenes grabadas para vigilar su actividad había sido una actuación idónea, necesaria y rigurosamente proporcionada, y, por tanto, constitucionalmente irreprochable. El Constitucional contradijo esta aseveración; consideró que la falta de información a los empleados de que las grabaciones obtenidas por las videocámaras podían ser empleadas para controlar la actividad laboral afectaba a una de las garantías nucleares del derecho fundamental a la autodeterminación informativa e incluso insinuó que en sentencias anteriores en las que el este órgano excepcionalmente había declarado lícitas las instalaciones ocultas, el fallo hubiera sido diferente si los recurrentes fundamentaran su impugnación en el artículo 18.4 de la CE y no en el artículo 18.1 de este mismo texto legal.

El fundamento jurídico séptimo, en donde se contiene la *ratio decidendi* de la sentencia, el Tribunal definió el núcleo esencial del artículo 18.4 de la CE remitiéndose para ello a la STC 292/2000, de 30 de noviembre. La obligación de información que en este caso le correspondía a la Universidad frente al trabajador advirtiéndole de que las grabaciones de las videocámaras se podían emplear con la finalidad de inspección laboral era necesaria, es más incluso lo sería, según el Órgano juzgador, en aquellos supuestos en los que existiera una habilitación legal para recabar los datos sin necesidad de consentimiento pues «una cosa» era «la necesidad o no de autorización del afectado y otra, diferente, el deber de informarle sobre su poseedor y el propósito del tratamiento». En este asunto, sin embargo, siguió diciendo el Tribunal, ni existía habilitación legal expresa que permitiera la omisión del derecho a la información ni tampoco podía fundamentarse este derecho en el interés empresarial de vigilar la actividad laboral a través de sistemas sorpresivos o no informados de tratamiento de datos. No fue suficiente que existieran distintivos colocados en diferentes puertas de acceso a la Universidad anunciando la instalación de las cámaras y la captación de imágenes en el recinto universitario, ni que se hubiera notificado la creación del fichero a la AEPD, ni tan siquiera que se hubiera probado que entre las diecinueve autorizaciones con que contaba la Universidad hispalense para hacer uso de los soportes informáticos o ficheros grabados por sus videocámaras, figurara una dirigida al control de acceso de las personas de la comunidad universitaria.

La información previa y expresa, precisa, clara e inequívoca en la que debían concretarse las características y el alcance del tratamiento de los datos que iba a realizarse; esto es, en qué casos las grabaciones podían ser examinadas, durante cuánto tiempo, con qué propósitos -haciendo constar expresamente que podían

utilizarse para la imposición de sanciones disciplinarias por incumplimientos del contrato de trabajo- y el destino que se les iba a dar a las imágenes no se produjo. A mayor abundamiento —como añadió el Alto Tribunal— tampoco hubo evidencia alguna de cuál era la finalidad del tratamiento de los datos, o uno de sus posibles objetos, pues los aparatos de vigilancia no estaban situados dentro de las concretas dependencias en donde se desarrollaba la prestación laboral sino en los vestíbulos y zonas de paso públicas.

En consecuencia por todo lo expuesto, y debido a que las cámaras de vídeo colocadas en el recinto universitario reprodujeron la imagen del recurrente y se emplearon las grabaciones para controlar su jornada de trabajo, la Universidad de Sevilla, responsable del tratamiento de datos, a juicio de la instancia máxima, vulneró el artículo 18.4 de la CE. Por tanto, las sanciones impuestas con base en esta única prueba lesiva del derecho fundamental a la protección de datos fueron declaradas nulas.

La sentencia fue objeto de diversos comentarios por parte de la doctrina. Para algunos autores resulta difícil comprender por qué la utilización por el empresario de medidas de videovigilancia en condiciones como las descritas en este pronunciamiento no constituye una intromisión ilegítima en el derecho a la intimidad personal y a la propia imagen, es decir, no son reprobables *ex* artículo 18.1 de la CE (SSTC 98/2000, de 10 de abril y 186/2000, de 10 de julio) y, sí en cambio, lo son desde la perspectiva del artículo 18.4 de la Norma suprema. Y de igual modo, por qué la obligación de informar previamente al trabajador es una cuestión de mera legalidad ordinaria en el caso del derecho a la intimidad (STC 186/2000, de 10 de julio) y, en cambio, forma parte del contenido esencial de la llamada libertad informática.

No puede olvidarse en este asunto que la instalación de las cámaras de seguridad estaba autorizada y debidamente advertida mediante los oportunos carteles anunciadores. El recurrente en amparo conocía por tanto de su existencia. El deber de información previa y detallada que se contiene en la LOPD sobre el uso y destino de los datos personales sirve principalmente al objeto de que el interesado preste o no su consentimiento. Consentimiento que no se precisa en aquellos supuestos en que existe una previa autorización administrativa o la correspondiente habilitación legal para captar y grabar las imágenes. Si el empresario puede instalar el sistema -aun sin contar con la autorización del trabajador- debido a la potestad de vigilancia que le otorga el artículo 20.3 del ET, lo lógico sería que el incumplimiento de esta obligación de información por parte de la Universidad aunque debe castigarse administrativamente, como establece la LOPD, no ha de elevarse a la categoría de conducta vulneradora del artículo 18.4 de la CE sobre todo si tenemos en cuenta que la sanción que impone la ley

es calificada como leve (artículo 44.2.d) LOPD). La interpretación efectuada por la sentencia no se compadece con la jurisprudencia laboral española y la de países como Alemania o Francia, que avala aunque sea de modo excepcional, la instalación de cámaras ocultas de videovigilancia para vigilara a trabajadores sobre los que existe sospecha de que han cometido un delito o cualquier ilícito grave cuyas consecuencias tengan que ser asumidas por el empresario[51].

Según el Constitucional, en el asunto examinado en la STC 29/2013, de 11 de febrero, no fue necesario valorar si el órgano judicial había ponderado previa y adecuadamente si el uso que se le había dado a las imágenes captadas por las cámaras de seguridad había respetado el derecho a la intimidad de los trabajadores con arreglo al citado y descrito test de proporcionalidad, sino que, a su juicio, para declarar la existencia de una lesión del artículo 18.4 de la CE bastaría con comprobar simplemente que el empresario no había cumplido con el deber de información previa a que obliga con carácter general el artículo 5.1 de la LOPD. De este modo, prescindió por completo de la ponderación entre el derecho fundamental en juego, el derecho a la protección de datos, y las eventuales limitaciones al mismo justificadas en el cumplimiento de las obligaciones laborales y las correlativas facultades empresariales de vigilancia y control. De alguna manera como ha sido señalado por parte de la doctrina, esta sentencia contradice la línea argumental del propio Tribunal Constitucional contenida en su jurisprudencia pero en particular en la STC 186/2000, de 10 de julio, tantas veces aquí citada. En ella aun reconociendo la existencia de un ámbito reservado,

[51] La máxima instancia judicial laboral alemana, el *Bundesarbeitsgericht*, recientemente en una sentencia de 21 de mayo de 2012, consideró lícita la instalación de cámaras ocultas en un lugar de trabajo de acceso público, contradiciendo así a un sector doctrinal que interpretaba que en ningún caso debían ser admitida este tipo de videovigilancia por contradecir el § 6b 2 de la BDSG (Bundesdatunschutzgesetz o Ley federal de protección de datos), en donde se establece con carácter general la obligación de señalización de estos medios de control en los lugares de acceso público. El Tribunal, por el contrario, entendió que la legalidad de la videovigilancia no puede hacerse depender del cumplimiento de este requisito. Si la medida secreta no fuera permitida en ningún supuesto esto supondría colocar al empresario en el juicio de ponderación de intereses en una posición de desventaja. El emplazamiento de cámaras ocultas es en muchas ocasiones el único instrumento efectivo a disposición del empleador para esclarecer una conducta delictiva. Si éstas se prohibieran de manera absoluta, a juicio del Tribunal, no podría el empresario proteger sus derechos. Sus instrumentos de vigilancia se verían seriamente reducidos independientemente de la gravedad de afectación de sus intereses, entre los que se podría encontrar el esclarecimiento de hechos delictivos. Todos estos aspectos no se tomarían en consideración si la videovigilancia secreta fuera prohibida. Lo lógico será efectuar un juicio de ponderación para determinar si la videovigilancia oculta en el concreto supuesto se considera proporcionada y en consecuencia si la colocación de las cámaras está justificada. PRACKA J. y BYERS, P., «Die Zulässigkeit der Videoüberwachung am Arbeitsplatz», *Betriebs Berater Heft*, n.º 13/2013, pág. 762.

manifestación del derecho fundamental a la intimidad y a la dignidad, no sometido a la fiscalización y conocimiento de terceros, declaró el Tribunal que, este derecho como cualquier otro no es ilimitado y que puede ceder frente a derechos de terceros siempre que se trate de un interés legítimo y la medida sea proporcionada a la finalidad perseguida. La instalación por parte de la empresa de un circuito cerrado de televisión para controlar diversos puestos de trabajo era una medida justificada e idónea para la finalidad pretendida al ser necesaria para el correcto funcionamiento de la actividad laboral.

Lo oportuno hubiera sido quizás que el Alto Tribunal emitiera un juicio acerca de si el órgano judicial había valorado previa y adecuadamente, si el empleo que se le había dado a las imágenes captadas por las cámaras de seguridad, había respetado los derechos a la intimidad y a la protección de datos de los trabajadores con arreglo al test de proporcionalidad y no declarar la existencia de una lesión del artículo 18.4 de la CE, porque simplemente se comprobó que el empresario no cumplió con el deber previo de información que impone con carácter general el artículo 5.1 de la LOPD. El examen del asunto desde la perspectiva exclusivamente del artículo 18.4 de la CE olvidándose por completo del derecho a la intimidad a que el trabajador sancionado, por otro lado, había hecho referencia expresa en la demanda, no tiene mucho sentido. A mayor abundamiento, si con el artículo 18.1 de la CE es necesario acudir al juicio de ponderación para apreciar si se ha conculcado o no el derecho que en él se regula, no parece razonable desde un punto de vista lógico reducir el juicio de vulneración del derecho a la autodeterminación informativa, a que se le hubiera comunicado o no a los trabajadores el destino que se les iba a dar a las imágenes sin tener en cuenta ninguna otra consideración[52].

El asunto no terminó únicamente con la sentencia del Constitucional, el recurrente en amparo presentó una denuncia ante la AEPD que finalizó con la Resolución 0987/2008, de 1 de septiembre, en la que se declaró que la Universidad había incumplido el artículo 5 de la LOPD, al no satisfacer el derecho de información de los afectados cuando se produjo la recogida de los datos personales. El Constitucional invocó esta resolución de la Agencia para afirmar que aunque no podía condicionar su juicio de constitucionalidad resultaba indicativa de la ilegalidad de la medida. La Resolución 0987/2008, a pesar de todo, fue anulada por la sentencia de la Audiencia Nacional, Sala de lo Contencioso-

[52] Casino Rubio, M., «Cámaras de seguridad y control de las obligaciones laborales (a propósito de la STC 29/2013, de 11 de febrero», en http://www.abogacia.es/2013/03/20/camaras-de-seguridad-y-control-de-las-obligaciones-laborales-a-proposito-de-la-stc-292013-de-11-de-febrero/.

Administrativo, de 15 de octubre de 2009, al apreciar la prescripción de la infracción y el recurso de casación solicitando el amparo fue rechazado por la Sentencia del Tribunal Supremo, Sala 3.ª de 16 de octubre de 2012[53].

2.6. El principio de seguridad de los datos

Otro ineludible principio de la LOPD es el de seguridad de los datos previsto en el artículo 9 y que resulta lógicamente aplicable a las imágenes a las que nos estamos refiriendo a lo largo de todo este trabajo. Su pérdida casual, las sustracciones voluntarias y las modificaciones y manipulaciones indebidas representan una conculcación del principio de calidad que impone la conservación de la información respetando su exactitud, autenticidad e integridad[54]. La LOPD, a diferencia de la Directiva 95/46/CE y de la legislación de otros países, ha relacionado el principio de seguridad con la toma de acciones concretas, señalando en su artículo 9.1 que «el responsable del fichero, o en su caso, el encargado del tratamiento, debe adoptar medidas tanto técnicas como organizativas necesarias que garanticen la seguridad de los datos y eviten su alteración, pérdida, tratamiento o acceso no autorizado habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico natural». Las amenazas son aquellas situaciones en las que una persona pretende acceder fraudulentamente al material grabado, para obtenerlo, falsificarlo o manipularlo. Por el contrario, los riegos son aquellas prácticas incorrectas por parte de los usuarios del material almacenado que pueden poner en peligro su seguridad[55]. Además no solo se deberá prestar atención a los ficheros en los que las imágenes se guardan sino también a los centros de tratamiento, los locales, los documentos, los dispositivos de almacenamiento, los equipos, los sistemas y los programas[56] que con ellas se utilizan.

El incumplimiento por parte del responsable o del encargado de alguna de estas normas puede provocar una declaración de infracción por quebrantamiento del principio de seguridad. No se registrarán imágenes en ficheros que no reúnan

[53] Marín López, J. J., «La utilización de los datos personales en el marco de un procedimiento disciplinario laboral: La STC 29/2013, de 11 de febrero, y el derecho a la información sobre tratamiento de datos personales», *Noticias Breves*, septiembre 2013, pág. 3.

[54] Troncoso Reigada, A., *La protección de datos personales. En busca del equilibrio*, *op. cit.*, pág. 475.

[55] *Seguridad y Protección de datos personales*, eds. Thomson y Civitas, Madrid, 2009, pág. 107.

[56] Santos García, D., *Nociones generales de la Ley Orgánica de protección de datos y su Reglamento*, ed. Tecnos, 2.ª edición, Madrid, 2012, pág. 88.

las condiciones de seguridad que por vía reglamentaria se exigen y que se contienen en el Reglamento de desarrollo de la LOPD.

Las medidas destinadas a proteger los datos personales en general pueden clasificarse en tres grupos: organizativas, en las que se incluyen los procedimientos que dan cumplimiento al deber de hacer del responsable del fichero en situaciones en las que está obligado a un determinado comportamiento; jurídicas, que son los instrumentos que el derecho de protección de datos otorga a los afectados y deben establecer los responsables del fichero o encargados del tratamiento que dispongan de datos personales; y por último, técnicas, que se regulan tanto en el RLOPD en su título VIII como en la LOPD misma y que están referidas a los ficheros, es decir, que se deben incorporar a ellos para preservar la integridad de su contenido[57].

En principio, y salvo que la finalidad del fichero sea captar informaciones relativas a infracciones administrativas o penales o a datos especialmente protegidos, el nivel de seguridad que corresponde a las imágenes grabadas en el ámbito laboral es el básico. Si fortuita o casualmente se obtuviesen y almacenasen otras que precisen un nivel de seguridad mayor, deberían aplicarse a los soportes que las recogen una superior protección acorde con el tipo de información personal almacenada, salvo que tuvieran el carácter de incidentales o accesorias en relación con la finalidad —artículo 81.5.b) del RLOPD— en cuyo caso podría recurrirse a las medidas de nivel básico. Especial atención merecen los supuestos en que las grabaciones se efectúan mediante cámaras con control remoto a través de Internet —cámaras IP— pues para ellas se requieren garantías específicas a fin de evitar su acceso a través de la red de personas ajenas al responsable de los datos.

El deber de secreto además de ser un principio de protección de datos es también un derecho del titular de los mismos. Al responsable del fichero es a quien le corresponde la obligación de cumplir con el secreto profesional con relación a las imágenes que se almacenan en el fichero que ha creado. Sin embargo no se trata de una obligación individual sino colectiva que afecta a «quienes intervengan en cualquier fase del tratamiento», como establece el artículo 10 de la LOPD, y subsiste después de finalizar las relaciones con el titular del archivo o responsable del mismo alcanzando incluso al personal que ha dejado de trabajar en la empresa. La vulneración de este deber se tipifica en la LOPD como una infracción leve, grave o muy grave en función de los datos que se hayan desvela-

[57] Santos García, D., *Nociones generales de la Ley Orgánica de protección de datos y su Reglamento*, *op. cit.*, págs. 87 y 88.

do y es objeto de responsabilidad penal de acuerdo con el artículo 197.2 del Código penal.

La Audiencia nacional a través de una sentencia de 27 de mayo de 2010 se pronunció sobre el deber de custodia en un asunto en el que se producía la transmisión en tiempo real de imágenes del interior de una oficina a través de una página *web*. Cualquier usuario podía acceder a las mismas debido a la alta resolución de la cámara que permitía identificar a las personas sin que existiera ningún tipo de control y simplemente seleccionando la dirección de Internet en el navegador. Tanto la AEPD como la Audiencia nacional afirmaron que la empresa estaba obligada a adoptar las medidas técnicas organizativas necesarias previstas en la normativa y, en particular, las destinadas a impedir el acceso a los datos personales por parte de terceros no autorizados. Finalmente, la empresa fue condenada por incumplir sus obligaciones de seguridad al no obrar con la diligencia y el cuidado necesario en el tratamiento de las imágenes evitando el libre acceso del público a ellas.

2.7. La cesión de datos

La LOPD define la cesión o comunicación de datos en el artículo 3.i) como toda «revelación de datos realizada a persona distinta del interesado» es decir la efectuada a un tercero. Según el artículo 1.r) de su RLOPD, tiene esta consideración «la persona física o jurídica, pública o privada u órgano administrativo distinto del afectado o interesado, del responsable del tratamiento, del responsable del fichero, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del mismo». De ahí que existan dos supuestos de entrega de datos, en este caso de imágenes, que no pueden ser calificados como cesiones: uno, el ejercicio del derecho de acceso por el propio interesado o por la persona que ostente su representación legal o voluntaria y otro, el acceso a las imágenes por el responsable de su tratamiento y las personas autorizadas para ello bajo su autoridad en el ámbito mismo de la persona jurídica.

Dos son los rasgos característicos de esta operación de cesión: primero, la existencia de una voluntad de transmisión por parte del responsable de las imágenes. Esta intención de comunicar una determinada información diferencia a las cesiones del acceso a los datos por terceras personas no deseado por el responsable de los mismos y causado principalmente por el incumplimiento de las medidas de seguridad destinadas a garantizar la confidencialidad de esa información. El segundo rasgo distintivo de la cesión es que la transmisión se efectúe

por medio del tratamiento y que lo diferencia del incumplimiento del deber de secreto, en donde el acceso de un tercero a la información se produce en circunstancias bien diferentes.

Las transmisiones de imágenes están, en principio, sujetas al consentimiento de su titular. La LOPD dispone que éstas «sólo podrán ser comunicadas a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado». La prestación de dicho consentimiento exige que se informe sobre la finalidad del destino o sobre la actividad de la persona a quien se le pretenden comunicar las imágenes. Sorprendentemente en el RLOPD se ha sustituido la conjunción disyuntiva «o» que se contiene en la Ley por la copulativa «y», de modo que, si nos atenemos a la norma reglamentaria, no bastará con informar de una de las dos circunstancias sino que es preciso hacerlo de las dos.

El responsable del fichero o encargado puede solicitar el consentimiento para efectuar la cesión en dos momentos: o bien cuando recaba las imágenes para someterlas al tratamiento o bien posteriormente, en la primera comunicación, si no se hubiera informado al titular sobre la posibilidad de la cesión y tuviera ahora la intención de realizarla[58]. En algunos casos puede prescindirse de este consentimiento, en el artículo 11 de la LOPD se recoge una la larga lista de excepciones. Las que aquí más nos interesan, por su aplicación al ámbito de la videovigilancia laboral, son las siguientes: las relativas a la existencia de una habilitación legal; aquellos casos en que la cesión responde a una relación jurídica que para su desarrollo, cumplimiento y control sea necesario la conexión del tratamiento con ficheros de terceros; y las ocasiones en las cuales los destinatarios de la cesión sean el Ministerio Fiscal y los Jueces y Tribunales en el ejercicio de sus funciones.

El segundo de los supuestos citado —cuando la cesión responde a una relación jurídica— es el que tiene lugar con mayor frecuencia en el ámbito empresarial. Son habituales las entregas por el empresario de imágenes obtenidas por el control directo e indirecto de los trabajadores a terceros, sin embargo, el consentimiento que se presta para el desarrollo del contrato o su ejecución posterior no autoriza su comunicación salvo «cuando dicha cesión se muestre necesaria para el normal y recto desarrollo de la relación laboral».

Otra de las cuestiones que se plantea con motivo de la cesión de datos es el papel que desempeñan los representantes de los trabajadores que no son ni órganos internos de la empresa ni tampoco están integrados en su organización,

[58] SANTOS GARCÍA, D., *Nociones general de la Ley Orgánica de Protección de Datos y su Reglamento*, *op. cit.*, pág. 95.

tienen, por tanto, la consideración de terceros. El responsable del fichero o tratamiento no puede, por ello, entregar las imágenes a los representantes de los trabajadores si no se ajusta a los requisitos previstos en el artículo 11 de la LOPD para la realización de esta operación.

Normalmente las operaciones de captación y tratamiento no las lleva a cabo la empresa que contrata directamente con el trabajador sino que este servicio se encarga a una segunda empresa generalmente de seguridad. En estos casos, el rol a desempeñar por el nuevo ente es, ineludiblemente, el de «encargado de tratamiento» que le será otorgado tras la firma de un contrato escrito o de cualquier otra forma que permita acreditar su celebración y contenido de acuerdo con el artículo 12 de la LOPD. Ahora bien recibirá dicha denominación si la empresa de seguridad realiza la captación, almacenamiento y tratamiento de las imágenes, no si su labor se limita a instalar las cámaras y los sistemas. En estas actividades es muy importante que el contrato se formalice al inicio de la captación y/o tratamiento de las imágenes, de no hacerlo, estaríamos realizando una cesión que no tendría ningún amparo legal y, por ende, constituiría una infracción sancionable por la AEPD conforme a lo dispuesto en el artículo 44 de la LOPD.

Es preciso advertir el cambio normativo que en la materia ha supuesto la Ley 25/2009, de 27 de diciembre, conocida como Ley Ómnibus. Esta norma elimina la necesidad de que el tratamiento de los datos sea llevado a cabo por empresas de seguridad debidamente autorizadas por el Ministerio del Interior, de modo que tras su entrada en vigor estas operaciones pueden ser efectuadas directamente por ellas o contratar una segunda en la que no tiene que concurrir esa condición.

El RLOPD permite la subcontratación regulando su modo de realización y las relaciones entre el titular de la responsabilidad y el encargado material de su utilización en los artículos 20 a 22. Entre las exigencias recogidas en estos preceptos encontramos un deber *in vigilando* que impone al responsable una obligación de velar porque el encargado reúna las garantías necesarias para cumplir con las disposiciones reglamentarias.

La entrega de imágenes del encargado del tratamiento al responsable de ellas no supone cesión alguna puesto que estas operaciones aunque materialmente requieran un traspaso no son consideradas por la ley como cesiones y, por tanto, no se someten al régimen general de éstas, sino que están amparadas por el contrato mismo a tenor del artículo 12 de la LOPD. En cualquier caso, el encargado actuará siempre y en todo momento bajo las instrucciones del responsable y si se excediera en ellas o utilizase las imágenes conculcando el contrato responderá personalmente por ello.

2.8. Los derechos ARCO en la videovigilancia empresarial

Como es sabido, la LOPD reconoce a todos y cada uno de los ciudadanos una serie de derechos, conocidos bajo el acrónimo de ARCO, y que no son otros que los derechos de acceso, rectificación, cancelación y oposición con plena vigencia en el ámbito de la videovigilancia. Forman parte, como ha manifestado la jurisprudencia constitucional, del contenido esencial del derecho fundamental a la protección de datos personales y son, en definitiva, derechos subjetivos de carácter personal que deberán ser ejercitados directamente frente al responsable del fichero tanto si se trata de una persona pública como privada[59].

A. El derecho de acceso

El derecho de acceso es el mejor exponente de lo que se ha dado en llamar «habeas data» que no solo es un derecho autónomo sino también una garantía de instituto para el ejercicio de otros derechos fundamentales.

De acuerdo con el artículo 15 de la LOPD, el interesado, en este caso la persona que ha sido objeto de videovigilancia tendrá derecho a solicitar y obtener gratuitamente información sobre las imágenes sometidas a tratamiento, su origen, así como las comunicaciones realizadas o que se prevé hacer con ellas.

El Reglamento de desarrollo de la LOPD incluye dentro del contenido de este derecho la facultad del afectado de obtener información sobre la finalidad del tratamiento de imágenes concretas incluidas en un fichero o sobre la totalidad de las sometidas a tratamiento.

El responsable del fichero podrá excepcionalmente oponerse a que el titular acceda a las mismas. No estamos ante un derecho absoluto que indefectiblemente tenga que ser materializado por el empresario sino que, por el contrario, puede ser denegado cuando concurren determinadas circunstancias, por ejemplo, en aquellos casos en que sea necesario proteger derechos y libertades de terceros, en los supuestos en los que sea preciso asegurar la represión de conductas o infracciones muy graves en la empresa o aquellas situaciones en las que los esfuerzos para recuperar las imágenes resulten desproporcionados en materia de investigación, coste y recursos si se comparan con la brevedad del período de retención de las mismas.

La información exigida se obtendrá mediante la visualización en pantalla, escrito, copia o fotocopia remitida por correo, certificada o no, telecopia, correo electrónico o cualquier otro medio a la configuración o implantación material

[59] Artículo 23 del RLOPD.

del fichero. La AEPD en el informe jurídico 0193/2007 se pronunció sobre las dificultades que plantea el acceso a las imágenes de forma automática, afirmando que la LOPD «no exige ningún sistema concreto para el reconocimiento de imágenes como datos de carácter personal, quedando por tanto, la elección del sistema al arbitrio del consultante. Este criterio es el mantenido por el Tribunal constitucional, que con relación a la actuación de la Administración pública, permite deducir que quien trata los datos, es responsable de cumplir con todo aquello que la ley determina».

El derecho de acceso del trabajador deberá ejercitarse en intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo, en cuyo caso podrá efectuarse con anterioridad. Debido a la «usual brevedad del período de retención de las imágenes», las posibilidades de acceso a las mismas son reducidas. No obstante, es un derecho que –como señala el GTA– debe ser protegido cuando tenga lugar una petición y resulte fácil la recuperación de las correspondientes grabaciones. Los trabajadores tienen derecho a acceder al fichero para comprobar si se ha respetado el fin para el cual fueron captadas aunque la LOPD en su artículo 15.3, establece un límite al ejercicio del derecho: no podrá hacerse uso de él más de una vez al año salvo que el interesado acredite interés legítimo de una manera muy clara y el responsable del fichero así lo considere.

Según el artículo 25.1.a) RLOPD para el ejercicio del derecho de acceso (y para el resto de derechos ARCO), la solicitud deberá contener, entre otra información: nombre y apellidos del interesado así como fotocopia del DNI, pasaporte o documento que lo identifique válidamente.

El plazo para responder a la petición de acceso a los datos es, según el artículo 29.1 del RLOPD, un mes a contar desde la recepción de la solicitud. Transcurrido este tiempo si no se ha dictado resolución expresa se entenderá desestimada la pretensión. Este período coincide curiosamente con el tiempo máximo en el que las imágenes pueden estar almacenadas, una vez finalizado, serán bloqueadas de manera que la contestación sería la información sobre el citado bloqueo y no el contenido del derecho de acceso.

Relacionado con esta cuestión, resulta interesante el informe de la AEPD, 252/2007, relativo a una cámara que almacenaba únicamente imágenes durante 24 horas, a pesar de lo cual la Agencia afirmó que en este caso el acceso supondría comunicar que no hay información sobre esa persona:

«En consecuencia, el responsable deberá de atender la solicitud de acceso, y responderla en el plazo de un mes, indicando que se carecen de datos personales del afectado, debido a que las imágenes se borran cada 24 horas» (aquí se habla de borrado y no de bloqueo).

Existen determinados ámbitos como bancos, cajas de ahorro y demás entidades de crédito, en los que, en virtud de lo dispuesto en el artículo 120.1 del Reglamento de Seguridad Privada, no cabe el derecho de acceso por las personas que han sido videovigiladas:

«Los soportes destinados a la grabación de imágenes han de estar protegidos contra robo, y la entidad de ahorro o de crédito deberá conservar los soportes con las imágenes grabadas durante quince días al menos desde la fecha de la grabación, en que estarán exclusivamente a disposición de las autoridades judiciales y de las dependencias de las Fuerzas y Cuerpos de Seguridad, a las que facilitarán inmediatamente aquellas que se refieran a la comisión de hechos delictivos. El contenido de los soportes será estrictamente reservado y las imágenes grabadas únicamente podrán ser utilizadas como medio de identificación de los autores de delitos contra las personas y la propiedad, debiendo ser inutilizado el contenido de los soportes y las imágenes una vez transcurridos quince días desde la grabación, salvo que hubiesen dispuesto lo contrario las autoridades judiciales o las Fuerzas y Cuerpos de Seguridad competentes. El Ministerio del Interior podrá ordenar, conforme a lo que se disponga reglamentariamente, la adopción de las medidas de seguridad necesarias en establecimientos e instalaciones industriales, comerciales y de servicios, para prevenir la comisión de los actos delictivos que se puedan cometer contra ellos, cuando generen riesgos directos para terceros o sean especialmente vulnerables.»

B. Los derechos de rectificación y cancelación

La LOPD contempla los derechos de rectificación y cancelación que puede ejercer el interesado en el mismo precepto, el artículo 16.

El ejercicio del derecho de rectificación da lugar a la sustitución de los datos erróneos[60] por los correctos para adecuar el tratamiento a la situación real de la persona interesada. La cancelación, por el contrario, no busca una modificación sino una eliminación del dato.

El artículo 16.2 de la LOPD prevé dos supuestos en que los datos deberán ser rectificados o cancelados. Primero, cuando el tratamiento no se ajuste al principio de seguridad dispuesto en la LOPD. En este caso es la cancelación en la mayoría de los supuestos lo que tiene más sentido porque probablemente tanto la captación como el tratamiento de las imágenes se había realizado

[60] Según Santos García, D., datos erróneos son datos contrarios a los principios de la LOPD, y en concreto al principio de calidad de datos. *Nociones generales de la Ley Orgánica de Protección de datos y su Reglamento*, *op. cit.*, pág. 112

de manera ilegal. La LOPD exige que se cancelen las imágenes cuando hayan dejado de ser necesarias o pertinentes para el propósito para el que se habían recogido —artículo 4.5—. En este sentido, la Instrucción 1/2006 de la AEPD fija el mismo criterio y además establece como plazo máximo el de 1 mes para su destrucción.

El ejercicio del derecho de cancelación dará lugar al bloqueo de las imágenes conservándose únicamente las que estuvieran bajo la custodia de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento y durante el plazo de prescripción de éstas. No puede identificarse el término «cancelar» con el término «destruir», únicamente se exige que las imágenes se conserven debidamente «bloqueadas» con el fin de impedir su tratamiento pero esto no implica su desaparición física[61], finalizado el plazo legal sí deberá procederse a su supresión de los ficheros.

El segundo supuesto que describe el artículo 16.2 de la LOPD para el ejercicio de los derechos de cancelación y rectificación se produce cuando los datos o en este supuesto las imágenes sean inexactas o incompletas. Cualquiera de estas dos operaciones —de manera especial la de cancelación por tratarse de imágenes— deberá hacerse efectiva en un período máximo de diez días desde la recepción de la solicitud del afectado y si no es posible su satisfacción, porque las imágenes no existen, tendrá igualmente que responderse a la petición debiendo acreditarse de manera fehaciente que se ha informado al interesado sobre este extremo. Todo ello, claro está, siempre que no perviva una obligación legal de conservación y puesta a disposición de lo grabado ante las autoridades judiciales o policiales por haberse captado un ilícito penal. Su destrucción en estos casos solo procederá una vez que se hayan agotado los plazos legales de ejercicio de las diversas acciones.

Otro problema que aquí se plantea con las imágenes es el del almacenamiento: no estamos ante el bloqueo de un fichero de unos concretos datos sino que como se trata de grabaciones continuas pueden surgir problemas con su acopio y con las copias de seguridad que en teoría están bloqueadas. No parece estar muy claro el tiempo que pueden mantenerse las imágenes y sus respectivas copias de seguridad en ese estado.

La AEPD en el informe 672/2008 se pronunció acerca de si debe eliminarse mensualmente toda la información recogida a través de las cámaras, incluida también la que pudiera encontrarse en las copias de seguridad de las cintas:

«A este respecto debe señalarse que la cancelación de los datos no supone su eliminación automática, sino su bloqueo tal y como dispone el artículo 16.3 de

[61] Garriga Domínguez, A., *Nociones generales de la Ley Orgánica de protección de datos y su Reglamento, op. cit.,* pág. 134.

la LOPD al establecer que "La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión".

En consecuencia, el plazo de un mes que señala la Instrucción 1/2006 es el período máximo para la cancelación de las imágenes en los términos vistos, no para su eliminación que estará sujeta al transcurso de los plazos de prescripción de las responsabilidades. En cuanto a las imágenes contenidas en la copia, siendo la copia de respaldo conforme al artículo 5.2.e) del RLOPD «copia de los datos de un fichero automatizado en un soporte que permita su recuperación», se someterán a los mismos plazos del que proceden.

Tras la solicitud de cancelación y en los casos que el borrado de lo grabado no sea posible por razones técnicas o como consecuencia del procedimiento o soporte en que se encuentra se procederá a su bloqueo. La operación equivale a una inutilización de la imagen a todos los efectos aunque ésta continúe existiendo físicamente dentro del fichero de manera inactiva. Si las imágenes han sido recogidas de forma fraudulenta, desleal o ilícita, es decir, contraviniendo las condiciones establecidas por la LOPD, excepcionalmente el artículo 16.1 del RLOPD recoge un supuesto de bloqueo automático o de oficio.

El responsable del fichero, como ocurría con el derecho de acceso, podrá en determinados supuestos, denegar los derechos de rectificación y cancelación:

— Cuando quien solicite el ejercicio sea una persona distinta al titular de las imágenes y no haya quedado acreditado que actúa en representación de éste (art. 23 del RLOPD).
— En los casos que así lo prevea una ley o una norma de derecho comunitario de aplicación directa o cuando éstas impidan al responsable del tratamiento revelar a los afectados el tratamiento de las imágenes a que se refiere el acceso (art. 33 del RLOPD).
— Si las imágenes deben ser conservadas durante un determinado plazo en virtud de una norma específica que así lo prevea o las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado que justificaron el tratamiento de los datos (art. 33.1 del RLOPD).
— En aquellas situaciones en que se pudiese causar un perjuicio a intereses legítimos del afectado o de terceros (Norma Tercera, punto 5 del RLOPD).

C) Consecuencias del incumplimiento de la LOPD en este ámbito

Ante una vulneración de la normativa de protección de datos por parte de la empresa o empresario[62], el afectado, en este caso, el trabajador o su representante legal tienen la posibilidad como primera medida de presentarse ante la AEPD y denunciar el incumplimiento para poder acudir a un procedimiento de tutela de derechos en los siguientes supuestos: frente a la negativa a satisfacer un derecho ARCO, contra el mero silencio ante su ejercicio o para recurrir una respuesta que no se considera adecuada. En esos casos la AEPD aplicaría el régimen sancionador previsto en el artículo 44 de la LOPD.

La disposición final quincuagésima sexta de la Ley 2/2011, de 4 de marzo, de Economía Sostenible, ha reformado el régimen sancionador de la LOPD, dicha modificación además de introducir un mayor número de elementos de graduación de las sanciones ha elevado sus cuantías mínimas aunque sigue manteniendo la máxima, de 600.000 euros prevista en el artículo 45.

Las acciones que el perjudicado puede emprender no se agotan aquí sino que, de acuerdo con lo que establece el artículo 19 de la LOPD, se reconoce también un derecho de indemnización a quien haya sufrido daños en sus bienes o derechos por vulneración de la legislación. Si la lesión procede de una persona privada, la responsabilidad tiene que exigirse ante la jurisdicción civil ordinaria, mientras que si aquélla es imputable a una persona jurídica pública, la indemnización se reclamará aplicando el régimen de responsabilidad de las Administraciones públicas. El lesionado acudirá, en primer término, por vía administrativa, ante la AEPD que resolverá en el plazo máximo de seis meses, y solo cuando su pretensión es denegada por desestimación o por silencio negativo se dirigirá a la jurisdicción contencioso-administrativa.

Asimismo y dependiendo del caso concreto, la conducta denunciada podría ser objeto de responsabilidad penal, tipificada en los artículos 197 y siguientes del Código Penal, o bien dar lugar al ejercicio de una acción preferente y sumaria de amparo de los derechos fundamentales de la Ley Orgánica 1/1982 por tratarse de una intromisión ilegítima. Finalmente también sería posible acudir a un proceso de tutela de derechos fundamentales del artículo 176 y siguientes

[62] Si el empresario elige un sistema de videovigilancia con circuito cerrado, será él únicamente responsable ante la AEPD en su condición de titular del fichero. Si optase por un circuito abierto con contratación de una empresa de seguridad privada será esta última la responsable. Ordeñana Gezuraga, I., «La videovigilancia en el ámbito laboral. Especial incidencia en su utilización como pruebe en el proceso penal», *Videovigilancia. Ámbito de aplicación y derechos fundamentales afectados. En particular la protección de los datos personales*, ed. Tirant lo Blanch, Valencia, 2011, pág. 64.

de la Ley 36/2011, de 10 de octubre, reguladora de la jurisdicción social (en adelante LJS) siempre y cuando se hubiera conculcado el derecho a la libertad sindical. De haberse producido esta vulneración ello supondría el cese automático de la actividad y de los actos contrarios al ordenamiento y al mismo tiempo el otorgamiento al trabajador de una indemnización por daños morales, derivada de la intromisión ilegítima o del desconocimiento del derecho de acuerdo con el artículo 183 de la LJS.

Por último y para concluir, al trabajador le cabría también la posibilidad de solicitar la resolución del contrato *ex* artículo 50 del ET, con el pago de los daños morales, lo que acarrearía una doble indemnización por parte del empresario. Una, por la resolución misma del contrato y otra, derivada de las consecuencias lesivas del quebrantamiento del derecho fundamental aunque esta última acción requiere que los hechos revistan cierta gravedad no bastando cualquier vulneración del derecho a la protección de datos.

3. CONCLUSIONES

La videovigilancia se ha convertido en la actualidad en un instrumento eficaz para garantizar la seguridad y prevenir el delito así como para fiscalizar en el ámbito laboral la prestación de trabajo. El artículo 20.3 del Estatuto de los trabajadores atribuye al empresario la facultad de adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales. Las cámaras de vídeo proporcionan al empleador una amplia e incontrovertible información a los efectos de acreditar en juicio los posibles incumplimientos laborales y actuaciones ilícitas.

La inexistente regulación sobre la videovigilancia empresarial en nuestro ordenamiento jurídico contrasta con su uso cada vez más frecuente en este ámbito y con la atención prestada por las legislaciones de los países de nuestro entorno, en las cuales, o bien se establece su prohibición absoluta cuando se implanta con finalidad de control laboral, como en sucede en Italia o en Portugal, o bien como ocurre en Francia o Alemania es preciso la observancia de una serie de requisitos o garantías procedimentales como la transparencia, proporcionalidad y consulta previa a los representantes de los trabajadores.

La LOPD 15/1999 (que recoge los principios básicos de la Directiva 95/46/CE) y su Reglamento de desarrollo junto con la Instrucción 1/2006, de la AEPD, constituyen las normas básicas que regulan esta materia en el derecho español. Las imágenes grabadas por las videocámaras en las que aparecen personas físicas identificadas o identificables, son datos de carácter personal, tal y como estable-

cen las diferentes normas legales citadas; y las operaciones y procedimientos técnicos, de carácter automatizado o no, que permiten la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de imágenes tienen la consideración de tratamiento de datos.

El empleador ha de advertir al trabajador de la presencia de cámaras en la empresa cumpliendo con la obligación legal de señalización de las mismas, sin embargo, ni su instalación ni tampoco el tratamiento de las imágenes precisan del consentimiento del trabajador si se hace con fines de seguridad y control laboral. En cambio sí sería necesario si estas operaciones se adscriben a otros fines, como puede ser, por ejemplo, el publicitario.

En aquellos casos en que las imágenes obtenidas en el ámbito laboral han sido almacenadas, es imprescindible que el empresario comunique a los empleados la creación del fichero y su destino. El artículo 5 de la LOPD describe los extremos sobre los que el empleador ha de informar de forma expresa, precisa e inequívoca: a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información; b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que le planteen; c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos; d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición; e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante. El artículo 18 del RLOPD especifica que la satisfacción de esta obligación se llevará a cabo a través de un medio que permita acreditar su cumplimiento y se mantendrá mientras persista el tratamiento de los datos por parte del responsable del fichero. Para el almacenamiento de los soportes se podrán utilizar medios informáticos o telemáticos, en particular, se acudirá al escaneado de la documentación en soporte papel, siempre y cuando se garantice que en dicha automatización no ha mediado alteración alguna de los originales.

Las imágenes, para ser recogidas y proceder a su tratamiento, han de ser adecuadas, pertinentes y no excesivas en relación con el ámbito y finalidades determinadas, explícitas y legítimas para las que se hubieran captado, a tenor de la normativa de protección de datos. Para su almacenamiento no son admisibles con carácter general los fines genéricos aunque se ajusten a derecho sino que tienen que ser determinados y su concreción ha de producirse en los siguientes momentos: cuando tiene lugar la declaración e inscripción del fichero, mientras se le da la información al interesado o en último caso, durante el ejercicio del derecho de acceso.

Los requisitos de adecuación, pertinencia y prohibición de exceso operan como límites en los procesos de captación y almacenamiento de las imágenes.

En primer lugar, por lo que se refiere a la adecuación, las cámaras han de ser el único medio al que el empresario puede acudir para lograr la vigilancia de su empresa por no disponer de otro instrumento menos restrictivo con los derechos fundamentales para alcanzar este objetivo. Sólo serán empleadas las videocámaras cuando otras medidas de prevención, protección y seguridad, de naturaleza física o lógica, que no exijan captación de imágenes (por ejemplo la utilización de puertas blindadas para combatir el vandalismo, la instalación de puertas automáticas y dispositivos de seguridad, sistemas combinados de alarma, etc.) resulten claramente insuficientes o inaplicables. En segundo lugar, se exige la pertinencia, es preciso seleccionar los sistemas de videovigilancia menos invasivos con los derechos a la intimidad y a la protección de datos de los trabajadores y del público en general. Ha de optarse, así, por cámaras que sean fijas en lugar de móviles, que cuenten con circuitos cerrados de televisión y no con tecnología basada en IP o con sistemas de grabación digital conectados a la red, etc. Y por último, la prohibición de exceso, esto es, se ha de descartar el emplazamiento de cámaras por toda la empresa, limitándose la grabación exclusivamente a aquellos lugares que sea estrictamente necesario y durante el tiempo mínimo indispensable para satisfacer el interés legítimo del empresario.

El principio de calidad de datos, según el artículo 4.2 de la LOPD, impone otra importante restricción: las imágenes no pueden utilizarse para finalidades «incompatibles» con las que justificaron su recogida. La AEPD y la jurisprudencia han interpretado este término como sinónimo de «distintas» lo que en materia de videovigilancia podría provocar, como se ha apuntado por algunos autores de la doctrina, situaciones absurdas al impedir que estas imágenes pudieran acreditar ilícitos graves si ésta no fuera la finalidad declarada para la que había sido instalada. La STC 29/2013 versa sobre este concreto asunto. Las videocámaras habían sido ubicadas en el lugar de trabajo para garantizar la seguridad y se había hecho la correspondiente notificación de creación de los ficheros ante la AEPD. Las imágenes captadas por los sistemas de vigilancia, sin embargo, se emplearon con otra finalidad, para acreditar el incumplimiento de jornada de un trabajador al que se le impusieron varias sanciones por esta causa. El Constitucional consideró que la Universidad, responsable de las videocámaras y titular del fichero, había vulnerado el derecho a la protección de datos del recurrente en amparo, porque no había cumplido con el deber previsto en el artículo 5.1 de la LOPD, al no informar al trabajador de que las imágenes podían utilizarse para control laboral. Y así, mientras que para apreciar si se ha vulnerado o no el derecho a la intimidad en el ámbito de la videovigilancia se acude al complejo principio de proporcionalidad, examinando si la medida adoptada es adecuada para conseguir el objetivo propuesto (juicio de idoneidad); necesaria, en el sentido de

que no existan otras alternativas más moderadas para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, ponderada o equilibrada, por producir más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto), no parece suceder lo mismo con en el derecho a la autodeterminación informativa, el Tribunal en el asunto analizado por la STC 29/2013 consideró que la vulneración se produjo simplemente porque el empleador no había comunicado al trabajador que las imágenes grabadas por las cámaras podían emplearse para fiscalizar actividad laboral, en definitiva, por incumplir un deber que a tenor de la LOPD tiene la consideración de infracción leve (artículo 44.2.d) LOPD).

La LOPD define la cesión o comunicación de datos en el artículo 3.i) como toda «revelación de datos realizada a persona distinta del interesado» es decir la efectuada a un tercero. Dos son sus rasgos característicos: primero, la voluntad de transmisión por parte del responsable de las imágenes, que diferencia a las cesiones del acceso a los datos por terceros, provocado por el incumplimiento de las medidas de seguridad destinadas a garantizar la confidencialidad de esa información. Segundo, que la transmisión se efectúe por medio del tratamiento lo que distingue a esta operación del incumplimiento del deber de secreto, en donde el acceso de un tercero a la información se produce en circunstancias bien diferentes. El responsable del fichero asume la obligación de asegurarle al afectado que las imágenes se van a emplear para cumplir con el tratamiento y con los objetivos que previamente fueron descritos y posteriormente notificados.

La LOPD reconoce a todos y cada uno de los ciudadanos una serie de derechos, conocidos bajo el acrónimo de ARCO, y que no son otros que los derechos de acceso, rectificación, cancelación y oposición con plena vigencia algunos de ellos en el ámbito de la videovigilancia. Forman parte, como ha manifestado la jurisprudencia constitucional, del contenido esencial del derecho fundamental a la autodeterminación informativa y son, básicamente, derechos subjetivos de carácter personal que deberán hacerse valer ante el responsable del fichero tanto si se trata de una persona jurídica pública como privada.

La persona que ha sido objeto de observación por las cámaras tendrá derecho a solicitar y obtener gratuitamente información, según el artículo 15 de la LOPD, sobre las imágenes sometidas a tratamiento, su origen, así como las comunicaciones realizadas o que se prevé hacer de las mismas. Se ejercerá en intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo, en cuyo caso podrá efectuarse con anterioridad. No estamos, sin embargo, ante un derecho absoluto que indefectiblemente tenga que ser materializado por el empresario sino que excepcionalmente puede ser denegado cuando concurren determinadas circunstancias. En cualquier caso y debido a la «usual

brevedad del período de retención de las imágenes» las posibilidades de acceso del trabajador a las mismas son reducidas.

El artículo 16 LOPD contempla los derechos de rectificación y cancelación. El último de ellos que es el que tiene sentido en materia de videovigilancia, busca la eliminación del dato y se produce, primero, cuando el tratamiento no se ajusta al principio de seguridad dispuesto en la LOPD, porque o bien la captación o bien el tratamiento de las imágenes se habían realizado de manera ilegal. Y segundo, en aquellos casos que lo grabado sea inexacto o incompleto. La LOPD exige que se cancelen las imágenes cuando hayan dejado de ser necesarias o pertinentes para el propósito para el que se han recogido —artículo 4.5—. En este sentido, la Instrucción 1/2006 de la AEPD fija el mismo criterio y además establece como plazo máximo el de 1 mes para su cancelación.

Title:

WORKPLACE VIDEO SURVEILLANCE AND RIGHT TO THE PROTECTION OF PERSONAL DATA

Summary:

1. The new instruments of control in workplace: the video cameras. 2. Video surveillance and the right to the protection of information of personal character. 2.1. The right to the protection of information of personal character: differential characteristics opposite to the privacy right. 2.2. Images like information of personal character and its treatment. 2.3. Right to information and the assent of the worker affected by the video surveillance. 2.4. The principle of the quality of data. The prohibition of incompatible uses. 2.5. The principle of the security of data. 2.6. The Sentence 29/2013 of the Constitutional Court. 2.7. The cession of data. 2.8. The ARCO rights in the video surveillance in workplaces. a. The right to access. b. The rights to rectification and cancellation. c. Consequences of the infraction of the LOPD in this area. 3. Conclusions.

Resumen:

Este trabajo tiene por objeto el examen de los problemas que plantea la videovigilancia laboral desde la perspectiva del derecho a la protección de los datos. La Ley Orgánica 5/1999, de 13 diciembre y su Re-

glamento de desarrollo son aplicables a las imágenes obtenidas por los empresarios a través de videocámaras de sus trabajadores; pues bien, el análisis de estos textos normativos así como de la jurisprudencia dictada sobre la materia, en especial la STC 29/2013 de 11 de febrero, constituyen el contenido principal de este estudio.

Abstract:

This work focuses on workplace video surveillance and its implications from the viewpoint of the right to the protection of personal data. Organic Law 5/1999 and its development regulation applies to the images obtained by employers through use of video cameras. The analysis of these legal texts and of the jurisprudence, particularly of the Constitutional Court sentence of 11 February 2013, is the subject of this study.

Palabras clave:

Videovigilancia, Derecho a la protección de datos, Derecho a la autodeterminación informativa, Principio de calidad de datos, Principio de seguridad de los datos; Derechos de acceso, rectificación y cancelación de los datos.

Key words:

Video surveillance, right to the protection of personal data, right to informational self determination, data quality principle, data security principle, Right of access, rectification, cancellation and opposition to data.