LA VIDEOVIGILANCIA EMPRESARIAL EN LA INDUSTRIA 4.0: LA SALVAGUARDA DE LA INTIMIDAD INFORMÁTICA DEL TRABAJADOR[1]

CORPORATE VIDEO SURVEILLANCE IN INDUSTRY 4.0: SAFEGUARDING THE COMPUTER PRIVACY OF THE WORKER

JOSÉ ANTONIO GONZÁLEZ MARTÍNEZ

Profesor Derecho del Trabajo y de la Seguridad Social (Contratado Doctor acreditado). Universidad de Alicante (EURLE)

Revista Aranzadi Doctrinal 10 • Noviembre 2021 • Págs. 73 a 96

Fecha de recepción: 14-7-2021

Fecha de aceptación: 31-8-2021

Resumen: La utilización de medios técnicos para la vigilancia, y su auge con la cuarta revolución industrial, repercute sobre los derechos fundamentales sobre las personas, lo que obliga a establecer las debidas garantías para preservar los mismos. La utilización de la videovigilancia en el ámbito empresarial, presumiendo la legitimidad de su finalidad, no puede llevarse a cabo al margen de la normativa vigente, sin cumplir una serie de requisitos, ni respetar una serie de principios, y sin tener en cuenta los derechos específicos del trabajador.

Abstract: The use of technical means for surveillance, and its rise with the fourth industrial revolution, has repercussions on the fundamental rights of people, which makes it necessary to establish the due guarantees to preserve them. The use of video surveillance in the business environment, presuming the legitimacy of its purpose, cannot be carried out outside of current regulations, without complying with a series of requirements, nor respecting a series of principles, and without taking into account specific rights of the worker. And since the laws cannot be so

1. Trabajo realizado en el marco de una estancia de investigación en la UPCT, como investigador visitante, desde el 19/10/2020 hasta el 19/02/2021, bajo la dirección del investigador anfitrión Dr. Djamil Tony Kahale Carrillo.

José Antonio González Martínez

Y como las leyes no pueden ser tan precisas y anteponerse a esta realidad tan cambiante, es la jurisprudencia de los grandes tribunales la que va indicando que tratamientos son admisibles y las condiciones para su realización, y por tanto la práctica empresarial debe ir al compás marcado por los pronunciamientos de los mismos.

Palabras clave: Industria 4.0, protección de datos personales, videovigilancia empresarial.

precise and prevail over this ever-changing reality, it is the jurisprudence of the large courts that indicates which treatments are admissible and the conditions for their implementation, and therefore business practice must go to the marked compass by their pronouncements.

Keywords: Industry 4.0, personal data protection, business video surveillance.

SUMARIO

I. EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES Y SU TRATAMIENTO

1. IMPACTO DE LA DIGITALIZACIÓN, CON LA CUARTA REVOLUCIÓN INDUSTRIAL, EN EL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS

La industria 4.0 surge como una nueva revolución industrial que consiste en incorporar las nuevas tecnologías a la industria, y esta transformación digital supone todo un desafío para la industria española y produce una variedad de cambios en el mundo del trabajo[2].

2. KAHALE CARRILLO, D. T.: "La industria 4.0: los retos para el empleo español", en *Los actuales cambios sociales y laborales: nuevos retos para el mundo del trabajo*, Suiza, Peter Lang, 2017, p. 75.

El intenso desarrollo actual de las tecnologías de la información, con la industria 4.0[3], presenta aspectos de incertidumbre y riesgo, siendo distintos los derechos fundamentales que pueden verse amenazados o vulnerados por un uso indebido de las mismas: esta revolución industrial facilita, por el gran volumen de información que se maneja, ilimitadas posibilidades para recoger datos personales, tratarlos, conservarlos y transmitirlos[4].

En el juego de intereses en el control de la información como fuente de poder, irrumpe la digitalización para hacer de los datos una pieza clave, no solamente en la actuación diaria de las empresas, sino básica para el conjunto de la sociedad. El tratamiento de datos permite competir mejor, producir más eficientemente, adaptarse mejor a la demanda y a los cambios derivados del proceso tecnológico[5].

Por tanto, ante esta cuarta revolución industrial, se hace notar una especial sensibilidad hacia este derecho fundamental a la protección de datos personales, y es bastante posible que sean dos las razones que vayan estimulando e impulsen la instauración de medidas para la protección y garantía de los datos personales: el riesgo de sanción y la propia imagen de calidad[6], siendo la difusión mediática e institucional las que ejercen una importante labor de apoyo.

Pero cabe plantearse si debemos rendirnos ante el carácter inevitable de la tecnología de la industria 4.0, como si todo lo tecnológicamente posible fuera jurídicamente legítimo, porque la tecnología debe de convivir con el respeto a los derechos fundamentales de la persona, y no ser entendida como una dictadura tecnológica.

2. EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES Y LOS PRINCIPIOS RELATIVOS A SU TRATAMIENTO

La imagen, así como la voz de una persona es un dato personal, al igual que lo será cualquier información que permita determinar, directa o indirectamente, su identidad, como, por ejemplo, una matrícula de vehículo o una dirección IP; y su tratamiento derivado de la captación y, en su caso, grabación, ha de ajustarse a lo dispuesto en el RGPD[7].

---

3. Sobre la materia, véase el interesante estudio de KAHALE CARRILLO, D. T. y OTROS: *El impacto de la industria 4.0 en el trabajo. Una visión interdisciplinar*, Aranzadi, Pamplona, 2020.

4. Véase, TRONCOSO REIGADA, A., "Introducción y presentación", en *Repertorio de Legislación y Jurisprudencia sobre Protección de Datos*, Civitas, Madrid, 2004, p. 22.

5. PÉREZ DEL PRADO, D., "Representación de los trabajadores y protección de datos de carácter personal como fuente de poder", en *Documentación Laboral, núm. 119, año 2020, Vol. I. Protección de datos y relaciones laborales*, 2020, p. 59.

6. GONZÁLEZ MARTÍNEZ, J. A., "Tratamiento de la información por las entidades financieras y la protección de datos: ¿se respeta la privacidad?", en *Revista española de Protección de Datos*, número especial 7 (julio 2009-junio 2010), Madrid, p. 183.

7. Informe Jurídico 0319/2017 AEPD.

La captación y el tratamiento de imágenes con fines de videovigilancia es una práctica cada vez más extendida en nuestra sociedad. La videovigilancia permite la captación, y en su caso la grabación, en forma de imágenes, no sólo de bienes o instalaciones, sino también de personas; y si la captación y el tratamiento de imágenes registradas por videocámaras pertenece a una persona, en la medida que identifique o pueda identificar a la misma (persona identificada o identificable), ello constituye un dato de carácter personal a efectos de la aplicación de la norma (la imagen es un dato personal)[8].

El derecho a la protección de datos ampara a los afectados frente al tratamiento de los mismos: se define este tratamiento como cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción[9].

Los datos personales deben ser tratados respetando una serie de principios[10]:

a) Principios de licitud, lealtad y transparencia: deben ser tratados de manera lícita, leal y transparente en relación con el interesado[11];

b) Principio de proporcionalidad: en virtud del cual, los datos personales serán recogidos con fines determinados, explícitos y legítimos y no serán tratados ulteriormente de manera incompatible con dichos fines, de manera que los datos que sean objeto de tratamiento a través de la videovigilancia serán tratados para la finalidad que ha motivado la instalación de esta y que está vinculada a garantizar la seguridad de personas, bienes e instalaciones[12];

---

8. Conforme al art. 4.1 RGPD, se considera dato personal toda información relativa a una persona física identificada o identificable. Y se considerará identificable 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: a modo de ejemplo, se consideran datos personales información sobre nombre y apellidos, número de identificación, datos de localización, nacimiento, matrimonio, domicilio, infancia, sobre la vida académica, profesional o laboral, hábitos de vida y consumo, creencias religiosas e ideológicas, etc.

9. Conforme al art. 4.2 RGPD.

10. Art. 5 RGPD. El empleador no puede conocer cualquier tipo de dato personal del trabajador, porque el principio de minimización de datos exige que los datos personales sean adecuados, pertinentes y limitados a lo necesario según los fines para los que son tratados.

11. El tratamiento de los datos debe tener su apoyo sobre una base legal, respetar los derechos, garantías y requisitos establecidos, y con facilidad para entenderlos con lenguaje sencillo y claro.

12. Conforme al Considerando 4 RGPD: "El tratamiento de datos personales debe estar concebido para servir a la humanidad. El derecho a la protección de los datos personales no es un derecho absoluto, sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad".

c) Principio de minimización de datos: de forma que los datos objeto de tratamiento sean adecuados, pertinentes y limitados en relación con los fines para los que son tratados; y solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios[13].

d) Principio de exactitud: los datos personales serán exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan.

e) Principio de limitación del plazo de conservación: los datos deben ser mantenidos de forma que se permita la identificación de los interesados durante el tiempo imprescindible (no más tiempo del necesario) para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos.

f) Principio de integridad y confidencialidad: los datos deben ser tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas.

g) Principio de responsabilidad proactiva: el responsable del tratamiento será responsable del cumplimiento de estos principios y capaz de demostrarlo[14].

La legislación de protección de datos es de aplicación al tratamiento de datos efectuado por un empleador respecto de los trabajadores, sin perjuicio de que el art. 88 RGPD permita que, mediante disposiciones legislativas o convenios colectivos, se establezcan normas más específicas para garantizar la protección de los derechos y libertades en relación con el tratamiento de datos personales de los trabajadores en el ámbito laboral[15].

13. Considerando 39 RGPD.

14. En el ámbito laboral debe prestarse especial atención a la transferencia de los datos personales dentro del grupo empresarial. Según el Informe Jurídico 0494/2008 de la AEPD, la existencia de un grupo de empresas no afecta para que cada una de las sociedades integradas en el mismo no mantenga diferenciada y plena su personalidad jurídica; a todos los efectos jurídicos, la circunstancia de que una sociedad esté participada por otra, no afecta al hecho de que ambas sean distintas personas, de modo que la comunicación de datos se produce entre dos personas distintas, sin que exista una previsión legal que flexibilice los requisitos para la legitimidad de dicha cesión (cada empresa que integra el grupo es responsable del fichero de datos de sus empleados).

15. En particular a efectos de contratación de personal, ejecución del contrato laboral, incluido el cumplimiento de las obligaciones establecidas por la ley o por el convenio colectivo, gestión, planificación y organización del trabajo, igualdad y diversidad en el lugar de trabajo, salud y seguridad en el trabajo, protección de los bienes de empleados o clientes, así como a efectos del ejercicio y disfrute, individual o colectivo, de los derechos y prestaciones relacionados con el empleo y a efectos de la extinción de la relación laboral.

La grabación de la imagen de una persona sea o no trabajador de la empresa, es un dato de carácter personal, a criterio de la Agencia Española de Protección de Datos (en adelante, AEPD), según su Resolución R/00035/2006 de 27 de febrero de 2006. La captación y grabación de imágenes con fines de vigilancia y control, se encuentra plenamente sometida a lo dispuesto en la LOPD, máxime cuando los afectados resultan perfectamente identificables, dentro del ámbito donde se realiza la captación de imágenes[16].

El Grupo de Trabajo del artículo 29, órgano consultivo independiente de la UE sobre protección de los datos y privacidad, creado en virtud del artículo 29 de la Directiva 95/46/CE[17], en su Dictamen 4/2004, adoptado en fecha 11/02/2004, relativo al tratamiento de datos personales mediante vigilancia por videocámara, establece los criterios para evaluar la legalidad y conveniencia de instalar sistemas de captación de imágenes en zonas públicas. El citado Grupo considera que los datos constituidos por imagen y sonido son personales, aunque las imágenes se utilicen en el marco de un sistema de circuito cerrado y no estén asociados a los datos personales del interesado, incluso, si no se refieren a personas cuyos rostros hayan sido filmados, e independientemente del método utilizado para el tratamiento, la técnica, el tipo de equipo, las características de la captación de imágenes y las herramientas de comunicación utilizadas.

El tratamiento de datos personales no puede realizarse por una razón de oportunidad, por la fácil obtención de estos o por si acaso en el futuro pudieran ser de utilidad, sino que exige que el responsable del tratamiento cuente con una base jurídica que le legitime para ello.

Con las capacidades que ofrecen los análisis de vídeo, es posible que un empresario observe las expresiones faciales del trabajador por medios automatizados, identifique desviaciones con respecto a los patrones de movimiento predefinidos (por ejemplo, una fábrica), etc. Esto sería desproporcionado a efectos de los derechos y libertades de los trabajadores y, por tanto, ilegal en general. El tratamiento también puede implicar la elaboración de perfiles y, posiblemente, la toma de decisiones automatizada. Por tanto, los empresarios deben abstenerse de utilizar tecnologías de reconocimiento facial. Puede haber algunas excepciones marginales a esta regla, pero tales escenarios no pueden utilizarse para invocar una legitimación general del uso de esta tecnología[18].

---

16. Conforme al Informe Jurídico 0533/2006 AEPD.

17. El Comité Europeo de Protección de Datos (CEPD), organismo independiente responsable de asegurar la consistente aplicación del RGPD, ha sucedido al GT29.

18. Dictamen 2/2017 sobre el tratamiento de datos en el trabajo, del GT29.

II. LA EJECUCIÓN DEL CONTRATO DE TRABAJO COMO BASE JURÍDICA PARA EL TRATAMIENTO DE DATOS PERSONALES: CARÁCTER EXCEPCIONAL DEL CONSENTIMIENTO DEL TRABAJADOR

1. LA LICITUD DEL TRATAMIENTO DE DATOS DEL TRABAJADOR ANTE LA EJECUCIÓN DEL CONTRATO

Si bien la celebración del contrato de trabajo otorga al empresario un poder de dirección para ordenar el normal funcionamiento de la empresa, y surge así un poder de control como complemento indispensable al de dirección, el margen de actuación del empresario no puede ser ilimitado; sin duda, la introducción de las nuevas tecnologías en la empresa tiene en su influencia sobre el poder de dirección su punto "más vistoso"[19].

El TCO pone de relieve la necesidad de que las resoluciones judiciales, preserven el necesario equilibrio entre las obligaciones dimanantes del contrato de trabajo para el trabajador y el ámbito (modulado por el contrato, pero en todo caso subsistente) de su libertad constitucional[20]. Dada la posición preeminente de los derechos fundamentales en nuestro ordenamiento, esa modulación sólo se producirá en la medida estrictamente imprescindible para el correcto y ordenado desenvolvimiento de la actividad productiva[21], lo que entraña la necesidad de proceder a una ponderación adecuada, que respete la correcta definición y valoración constitucional del derecho fundamental aquí en juego y de las obligaciones laborales que pueden modularlo.

Por un lado no debemos olvidar la naturaleza constitucional de este derecho fundamental a la protección de datos, que a diferencia del derecho a la intimidad del art. 18.1 CE, con quien comparte el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar, atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos cuya concreta regulación debe establecer la Ley, aquella que conforme al art. 18.4 CE debe limitar el uso de la informática, bien desarrollando el derecho fundamental a la protección de datos (art. 81.1 CE), bien regulando su ejercicio (art. 53.1 CE)[22].

Por otro lado, la definición del contenido del derecho fundamental a la protección de datos se realiza a través de la resolución de recursos de inconstitucionalidad, y consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un

19. SEMPERE NAVARRO, A. V. y SAN MARTÍN MAZZUCONI, C., *Nuevas Tecnologías y Relaciones Laborales*, Aranzadi, Pamplona, 2002, p. 42.

20. STC 6/1988, de 21 de enero (RTC 1988, 6) (ECLI:ES:TC:1988:6).

21. STC 99/1994, de 11 de abril (RTC 1994, 99) (ECLI:ES:TC:1994:99).

22. STC 292/2000, de 30 de noviembre (RTC 2000, 292) (FJ 7), ECLI:ES:TC:2000:292.

tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso[23].

La celebración de un contrato de trabajo no implica la privación para una de las partes, el trabajador, de los derechos que la Constitución le reconoce como ciudadano, así como también que la libertad de empresa (art. 38 CE) no legitima que los trabajadores hayan de soportar limitaciones injustificadas de sus derechos fundamentales y libertades públicas[24]. El ejercicio de las facultades organizativas del empleador no puede traducirse en la producción de resultados inconstitucionales, lesivos de los derechos fundamentales del trabajador, ni en la sanción del ejercicio legítimo de tales derechos por parte de aquél, de manera que no neutraliza el panorama indiciario la genérica invocación de facultades legales o convencionales[25].

Por ello, cuando se prueba indiciariamente que una decisión empresarial puede enmascarar una lesión de derechos fundamentales incumbe al empresario acreditar que su decisión obedece a motivos razonables y ajenos a todo propósito atentatorio del derecho de que se trate y que es preciso garantizar en tales supuestos que los derechos fundamentales del trabajador no sean desconocidos por el empresario bajo la cobertura formal del ejercicio por parte de éste de los derechos y facultades reconocidos por las normas laborales[26].

Partiendo de este principio de no anulación de los derechos fundamentales, no puede desconocerse tampoco que la inserción en la organización ajena modula aquellos derechos, en la medida estrictamente imprescindible para que el correcto y ordenado desenvolvimiento de la actividad productiva reflejo, a su vez, de derechos que han recibido consagración en el texto de nuestra norma fundamental (arts. 38 y 33 CE) y que, como en todo caso de colisión de derechos fundamentales o bienes constitucionalmente protegidos, deben apreciarse los intereses en presencia, mediante una adecuada ponderación de las circunstancias concurrentes[27].

2. EL INTERÉS LEGÍTIMO DEL EMPRESARIO FRENTE AL CONSENTIMIENTO DEL TRABAJADOR

Las tecnologías modernas permiten que los trabajadores puedan ser objeto de seguimiento a lo largo del tiempo, en los lugares de trabajo y en sus hogares,

23. STC 292/2000, de 30 de noviembre (FJ 7), ECLI:ES:TC:2000:292. Reconoce así un derecho específico de protección de datos personales, frente al riesgo que suponen los tratamientos de los datos personales con las nuevas tecnologías.

24. STC 196/2004, de 15 noviembre (RTC 2004, 196) (FJ 3), ECLI:ES:TC:2004:196.

25. STC 41/2006, de 13 febrero (RTC 2006, 41) (FJ 4), ECLI:ES:TC:2006:41.

26. STC 342/2006, de 11 diciembre (RTC 2006, 342) (FJ 4), ECLI:ES:TC:2006:342.

27. SSTC 186/2000, de 10 julio (RTC 2000, 186), ECLI:ES:TC:2000:186; 98/2000, de 10 abril, ECLI:ES:TC:2000:98.

a través de muchos dispositivos diferentes, como teléfonos inteligentes, ordenadores de mesa, tabletas, vehículos y tecnología ponible. Si el tratamiento no tiene límites y no es transparente, existe un alto riesgo de que el interés legítimo de los empresarios en la mejora de la eficiencia y protección de los activos de la empresa se convierta en un control injustificado e intrusivo[28].

Aunque el uso de estas tecnologías puede ser útil para detectar o prevenir la pérdida de propiedad intelectual y material de la empresa, mejorando la productividad de los trabajadores y protegiendo los datos personales de los que se encarga el responsable del tratamiento, también plantea importantes retos en materia de privacidad y protección de datos: hay que equilibrar el interés legítimo del empresario de proteger su empresa y la expectativa razonable de privacidad del trabajador.

La digitalización trae consigo un aumento exponencial de la cantidad y variedad de la información disponible, si como de las posibilidades de su tratamiento, Esto implica una alteración del esquema de poder de las partes concernidas, lo que es especialmente significativo en los sistemas de relaciones laborales, ya que el tratamiento de datos personales no solamente es una cuestión de ponderación de derechos e intereses en juego, sino de equilibrio adecuado de poderes entre el empresario (y su legítimo interés) y los derechos y libertades fundamentales del trabajador[29].

Es muy poco probable que el consentimiento constituya una base jurídica para el tratamiento de datos en el trabajo, a no ser que los trabajadores puedan negarse sin consecuencias adversas, ya que el trabajador en muy pocas ocasiones está en condiciones de dar, denegar o revocar el consentimiento libremente. Salvo en situaciones excepcionales, los empresarios tendrán que basarse en otro fundamento jurídico distinto del consentimiento, como la necesidad de tratar los datos para su interés legítimo. Sin embargo, un interés legítimo en sí mismo no es suficiente para primar sobre los derechos y libertades de los trabajadores.

Ahora bien, aunque no se requiere el consentimiento expreso del trabajador, si se exige que sea informado (persiste el deber de información), y en este sentido, la nueva doctrina establece que lo importante es que la instalación no sea oculta, debe ser conocida por los trabajadores, basta con que la empresa indique que

---

28. Dictamen 2/2017 sobre el tratamiento de datos en el trabajo, del GT29.

29. PÉREZ DEL PRADO, D., "Representación de los trabajadores y protección de datos de carácter personal como fuente de poder", en *Documentación Laboral, núm. 119, año 2020, Vol. I. Protección de datos y relaciones laborales*, 2020, p. 57. Como ejemplo de equilibrio entre partes, véase el asunto de Köpke/Alemania, [2010] ECHR 1725, (*http://www.bailii.org/eu/cases/ECHR/2010/1725.html*), en el que un trabajador ve extinguida su relación laboral como resultado de una operación de videovigilancia discreta llevada a cabo por el empresario y una agencia de detectives privados. Aunque en este caso el Tribunal concluyó que las autoridades nacionales habían logrado un equilibrio justo entre los intereses legítimos del empresario (protección de sus derechos de propiedad), el derecho del trabajador al respeto de la vida privada y el interés público en la administración de justicia también observó que los distintos intereses afectados podrían valorarse de manera diferente en el futuro como resultado del desarrollo tecnológico.

cuenta con un sistema de videovigilancia por razones de seguridad (para evitar robos y delitos), aunque no se les hubiese informado expresamente de la finalidad de control de la actividad laboral.

Es lícita la medida siempre que el trabajador conozca la existencia, ubicación e instalación por motivos de seguridad, aunque la empresa no indique el destino que les puede dar a las grabaciones, ni que las puede utilizar en su contra. Lo importante es determinar si el dato obtenido se ha utilizado para la finalidad de control de la relación laboral o para una finalidad ajena al cumplimiento del contrato, porque sólo si la finalidad del tratamiento de datos no guarda relación directa con el mantenimiento, desarrollo o control de la relación contractual el empresario estaría obligado a solicitar el consentimiento de los trabajadores afectados.

Ante sospechas fundadas, no es necesario el consentimiento previo de los trabajadores afectados, ya que el mismo se entiende implícito en la aceptación del contrato de trabajo, si bien el empresario debe informar al trabajador sobre la adopción de los sistemas de videovigilancia. Así, un primer pronunciamiento del caso López Ribalda se dio con la STEDH de 9 de enero de 2018) no admite la videovigilancia encubierta cuando se basa en una sospecha general contra todo el personal, pues viola el derecho a la intimidad la vigilancia por cámaras ocultas de todos los trabajadores en cajas registradoras, durante semanas, sin límite de tiempo y durante todas las horas del trabajo, por lo que no superaban el test de proporcionalidad (se estima que la instalación de cámaras de videovigilancia vulnera el derecho a la vida privada de los empleados, tanto porque suponía un incumplimiento del deber de información a los trabajadores, como por tratarse de una medida de control empresarial no proporcional a los efectos pretendidos).

Sin embargo, la Sala General del TEDH alcanza ahora una conclusión distinta en un segundo pronunciamiento el 17 de octubre de 2019, dejando sin efecto su sentencia previa: el hecho de que se haya informado previamente a los trabajadores de la instalación de los sistemas de videovigilancia se erige en un factor más para valorar la proporcionalidad de la medida de control implantada, pero no es un requisito absoluto para determinar que la medida es ajustada a derecho (el requisito de información previa a los empleados sobre la instalación de cámaras ocultas no es indispensable para concluir que la medida de control empresarial respeta el derecho a la vida privada de los trabajadores).

La resolución establece que, a la hora de usar cámaras en el entorno laboral, la regla general, que no absoluta, será que el deber de información es necesario. Ahora bien, dicha pauta cederá en aquellos supuestos en los que se aprecie la existencia de una sospecha razonable sobre un incumplimiento laboral (circunstancia que deberá ser acreditada por parte de la empresa) que avale la implantación de un sistema de videovigilancia empresarial y, además, que la actuación empresarial supere el triple juicio de idoneidad, necesidad y proporcionalidad. Así, a juicio del TEDH, la inobservancia del deber de información a los trabajadores carecería de

relevancia constitucional si existe una justificación que permita la adopción de la medida de control susceptible de conseguir el objetivo propuesto (idoneidad), si además es necesaria en el sentido de que no exista otro medio más moderado para la consecución de dicho objetivo (necesidad) y si, finalmente, de la misma se pueden derivar más beneficios para el interés general que perjuicios sobre otros bienes o valores en conflicto (proporcionalidad). Se reproduce la doctrina constitucional de las SSTC de 10 de julio de 2000 o de 8 de abril de 2016, en el sentido de que la ausencia de cumplimiento del requisito de información previa a los trabajadores (regla general) se ve eximido cuando la medida de control implantada resultase una medida idónea, necesaria y proporcional al fin perseguido.

III. LA PROTECCIÓN ANTE MEDIDAS RESTRICTIVAS DE DERECHOS FUNDAMENTALES: OBSERVANCIA DEL PRINCIPIO DE PROPORCIONALIDAD DE LA INTROMISIÓN EMPRESARIAL

1. LA VIDEOVIGILANCIA, COMO PODER DE CONTROL EMPRESARIAL, Y EL RESPETO A LOS DERECHOS FUNDAMENTALES

La utilización de instalaciones de videovigilancia para captar, grabar o reproducir imágenes de personas constituye una práctica que puede afectar a los derechos fundamentales y en particular al derecho fundamental a la protección de datos, siendo una temática que provoca muchas disputas entre las partes afectadas. Según datos de la Memoria del año 2019 de la Agencia Española de Protección de Datos (en adelante, AEPD), los servicios de Internet (13%), la videovigilancia (12%), y los ficheros de morosidad (12%), son las áreas de actividad con mayor número de reclamaciones planteadas ante la AEPD; y le siguen: reclamación de deudas (9%); publicidad, excepto spam (7%); administración pública (7%); comercios, transporte y hostelería (4%); entidades financieras, acreedoras (4%); sanidad (4%); telecomunicaciones (4%); y otros (24%). Las áreas de actividad con mayor número de procedimientos sancionadores son: la videovigilancia (31%); los servicios de internet (17%); la publicidad a través de e-mail o teléfono móvil (9%); las telecomunicaciones (6%); la administración pública (4%); las asociaciones, federaciones y clubes (4%); la contratación fraudulenta (4%); los ficheros de morosidad (3%); los comercios, transporte y hostelería (3%); los suministros de gas, electricidad y agua (2%).

Y esta videovigilancia, no sólo se vincula a la captación y tratamiento de imágenes con fines de garantizar la seguridad de personas, bienes e instalaciones, que en la actualidad es la finalidad más común (en acceso a edificios y salas de juego, entidades financieras, vía pública, entornos escolares y menores, espacios públicos de uso privado, control de tráfico, o espectáculos deportivos, entre otros), sino también puede usarse con otros fines como la investigación, la monitorización de una UVI, o el control empresarial de la prestación laboral.

La utilización de medios de control digitales en el ámbito empresarial no puede ser enmarcado sólo en el contexto de la seguridad y la protección de datos de personas y bienes, sino también en un excelente medio de control de la actividad laboral de los trabajadores, o una nueva forma de gobernar las relaciones laborales[30].

Del control presencial, con la acción de vigilancia directa por personal específico en la empresa, se pasó, en el origen de la digitalización, al control tecnológico, a los dispositivos de grabación de imágenes y sonidos, con un ahorro de costes importante para la misma frente a la supervisión humana, y que se basaban en los tradicionales circuitos cerrados de televisión y que sólo estaban en las grandes empresas, como las entidades financieras, punteras en la aplicación e implantación de los nuevos avances tecnológicos. Un claro ejemplo del tratamiento automatizado de datos se da en la actividad bancaria, concretamente en la práctica denominada "scoring"[31], que es un procedimiento de concesión de operaciones de riesgo mediante sistemas informáticos, a través del cual y en función de la información introducida autoriza o deniega la operación solicitada[32]. Posteriormente dichos sistemas fueron sustituidos por soluciones de videovigilancia basadas en IP, con la posibilidad de controlar el sistema desde cualquier puesto conectado a la red, incluso desde internet, la integración de otros sistemas de control y la posibilidad de recuperación y de tratamiento de imágenes grabadas[33].

Con la introducción de los sistemas de videovigilancia en el ámbito laboral, la privacidad queda atenuada dando la sensación de que el empresario termina por adueñarse del comportamiento de las personas en el lugar de trabajo. Y estos métodos de vigilancia engendran un desequilibrio entre las partes en tanto que suponen para el empresario una concentración mayor de poder, sacan al trabajador de su anonimato. El ojo mecánico contribuye de esta manera a la gobernabilidad, al control social de los trabajadores, ampliando la esfera de poder del empresario[34].

Hemos señalado que el concepto de dato personal incluye las imágenes cuando se refieran a personas identificadas o identificables, que los principios vigentes en materia de protección de datos personales deben aplicarse al uso

30. GOÑI SEIN, J. L., *La Videovigilancia Empresarial y la Protección de Datos Personales*, Civitas, Madrid, 2007, p. 16.

31. GONZÁLEZ MARTÍNEZ, J. A. y ORTEGA GIMÉNEZ, A.: "El sector financiero y la protección de datos: el precio de nuestra intimidad", en *Actualidad Juridica Aranzadi*, número 822, 9 de junio (2011), Cizur Menor (Navarra), p. 5: Se trata de una práctica basada en unas herramientas informáticas que incorporan una serie de factores de riesgo, cuya adecuada combinación entre sí ofrecen como resultado una puntuación de la calidad crediticia de la operación a realizar con el cliente.

32. GONZÁLEZ MARTÍNEZ, J. A., "Tratamiento de la información por las entidades financieras y la protección de datos: ¿se respeta la privacidad?", cit., p. 183.

33. GOÑI SEIN, J. L., *La Videovigilancia Empresarial y la Protección de Datos Personales*, cit., p. 16.

34. RODRÍGUEZ ESCANCIANO, S., "Vigilancia y control en la relación de trabajo: la incidencia de las nuevas tecnologías", en *La protección de datos de carácter personal en los centros de trabajo*, Cinca, Madrid, 2006, p. 88.

de cámaras o videocámaras (u cualquier otro medio técnico análogo, que capte imágenes (y/o las registre); y todo ello no sólo con fines de preservar la seguridad, sino también con fines de control empresarial de los trabajadores.

La instalación de cámaras de videovigilancia sería una medida proporcional y justificada si se cumplen los siguientes requisitos: 1. Que se trate de una medida susceptible de conseguir el objetivo propuesto. 2. Que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia. 3. Que la misma sea ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto[35].

Además de la videovigilancia, como una de las manifestaciones más problemáticas, estas técnicas empresariales pueden manifestarse de diversos modos, como la geolocalización para el control de la ubicación física del trabajador, la monitorización del correo electrónico, o el control de los dispositivos digitales del trabajador puestos a disposición por el empleador, entre otras. Todos estos medios de control que las nuevas tecnologías permiten, además de un control directo sobre actividades de los trabajadores para verificar su comportamiento, permite otro indirecto derivado de la posibilidad de retener la información obtenida a sus resultas y, mediante técnicas de elaboración de datos, obtener y sistematizar informaciones nuevas relativas a la persona del trabajador, remontándose desde los actos más banales hasta sus más íntimos secretos[36].

Frente a esta facultad de dirección empresarial, se impone una vez más la necesidad de proceder a una adecuada ponderación de los bienes y derechos constitucionalmente protegidos, que dilucide si el eventual recorte que se produce a través de esos medios de vigilancia y control resulta justificado y proporcional en los términos recogidos por el Constitucional; para lo cual habrá que atender, no sólo al concreto medio utilizado sino también a otros elementos de juicio: si se ha autorizado o no la utilización de las TIC para fines extralaborales, si los sistemas de control son conocidos o han sido instalados subrepticiamente, o si existen razones de seguridad por el tipo de actividad que se desarrolla[37].

2. LA PROTECCIÓN DE DATOS PERSONALES A LOS OJOS DE LA NORMA

2.1. La LOPD como respuesta al mandato del art. 18.4 CE

Desde una dimensión europea, la Carta de los Derechos Fundamentales de la Unión Europea, hecha en Estrasburgo de 12 de diciembre de 2007[38], afirma la

35. Informe Jurídico 0319/2017 AEPD.

36. TASCÓN LÓPEZ, R., *El Tratamiento por la Empresa de Datos Personales de los Trabajadores. Análisis del estado de la cuestión*, Civitas, Madrid, 2005, p. 136.

37. ORTEGA GIMÉNEZ, A. y GONZÁLEZ MARTÍNEZ, J. A.: "Protección de datos, secreto de las comunicaciones, utilización del correo electrónico por los trabajadores y control empresarial", cit., p. 3.

38. DOUEC núm. 303, de 14 de diciembre (vigente desde el 1 de diciembre de 2009).

necesaria adaptación al progreso en el campo de los derechos fundamentales, y proclama en su Preámbulo que "para ello es necesario, dándoles mayor proyección mediante una Carta, reforzar la protección de los derechos fundamentales a tenor de la evolución de la sociedad, del progreso social y de los avances científicos y tecnológicos". Así, recoge en su art. 8.1, dentro del título relativo a las Libertades, el reconocimiento del derecho a la protección de datos de carácter personal, estableciendo que "Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan"[39].

En el sistema jurídico español, este derecho fundamental es el resultado de una paulatina construcción constitucional, legislativa y, sobre todo, jurisprudencial, que encuentra el oportuno refrendo en el citado art. 8 de la Carta. Liberado ya de su congénita servidumbre respecto de la protección de la intimidad, el derecho a la protección de datos se configura como un derecho fundamental autónomo[40].

Haciéndose eco del debate surgido en toda Europa, más o menos en torno a su promulgación, la CE de 1978 en su art. 18.4, efectúa una remisión a la Ley[41] para "limitar 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"[42]. Su regulación y desarrollo se especifica en la vigente Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales[43] (en adelante, LOPD), como la norma básica sobre la materia en nuestro país; y que se debe completar con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE[44] (en adelante, RGPD)[45].

La videovigilancia, conforme a la norma, persigue dos finalidades distintas, según estemos en un ámbito general o en un entorno específico empresarial, surgiendo así dos medidas de protección distintas pero complementarias,

---

39. Y en su art. 8.2 añade que "Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación".

40. OLIVER LALANA, A. D., "Autorregulación, normas jurídicas y tecnologías de la privacidad. El lado virtual del derecho a la protección de datos", en *XVII Encuentros sobre Informática y Derecho (2002-2003)*, Facultad de Derecho, Instituto de Informática Jurídica, Universidad Pontificia Comillas, Madrid, 2003, p. 85.

41. La Ley que limite el uso de la informática aludida por la CE tarda en llegar hasta la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD); y tras 8 años de vigencia de esta, se aprobó la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, antecesora de la actual.

42. Llama la atención que la única vez que la CE habla de la informática, lo haga para limitar su uso. Y conviene tener presente que la Constitución Portuguesa de 1976 y la CE 1978 fueron las primeras en Europa en hacer referencia específica a la protección de datos personales en sus textos constitucionales.

43. BOE núm. 294, de 6 de diciembre.

44. DOUEL núm. 119, de 4 de mayo (vigente desde el 24 de mayo de 2016).

45. Así pues, la LOPD, completada con el RGPD, da respuesta al mandato del art. 18.4 CE.

constituyendo ambas finalidades, bienes muy valiosos dignos de protección jurídica, si bien condicionados al cumplimiento de determinados requisitos.

Una protección genérica, establecida en el art. 22 LOPD, independientemente de si se da o no en un entorno laboral, y que tiene unos principios básicos:

a) Autoriza a las personas físicas o jurídicas, públicas o privadas, a gestionar el tratamiento de imágenes a través de sistemas de cámaras o videocámaras con el objetivo de "preservar la seguridad de las personas y bienes, así como de sus instalaciones".

b) No está sometido a la normativa de protección de datos, el tratamiento de imágenes en el ámbito exclusivamente personal o doméstico por una persona física que capte imágenes del interior de su domicilio privado.

c) No es posible la captación de imágenes de espacios públicos con fines de seguridad, salvo imágenes parciales o limitadas imprescindibles para garantizar la seguridad de bienes o instalaciones estratégicos o de infraestructuras vinculadas al transporte.

d) Las imágenes serán conservadas durante el plazo máximo de un mes desde su captación, salvo cuando hubieran de ser conservadas para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones, en cuyo caso, serán puestas en conocimiento de la autoridad competente en un plazo máximo de setenta y dos horas desde que se tuviera conocimiento de la existencia de la grabación.

e) En todo caso, se debe informar de la existencia del sistema de videovigilancia, deber que se entiende cumplido mediante la colocación de un dispositivo informativo en lugar suficientemente visible que indique, al menos, la existencia del tratamiento, la identidad del responsable de la instalación y la posibilidad de ejercitar los derechos que prevé la normativa de protección de datos.

Y una protección específica, prevista en el art. 89 LOPD, referida a la protección de la "intimidad informática del trabajador" frente al uso de dispositivos de videovigilancia y geolocalización en el marco de una relación laboral. Esta regulación se aplica a los trabajadores y empleados públicos, formando parte de la legislación laboral y de las bases del régimen estatutario de los funcionarios públicos, y tiene carácter mínimo respecto de la autonomía colectiva, que podrá establecer garantías adicionales de los derechos y libertades relacionados con el tratamiento de los datos personales de los trabajadores y la salvaguarda de derechos digitales en el ámbito laboral[46].

Las condiciones para el tratamiento de datos con fines de videovigilancia se establecen en el art. 22 LOPD, el cual hace una remisión expresa a los supuestos

46. De conformidad con el art. 91 LOPD.

de tratamiento en los que el empleador obtiene datos personales a través de sistemas de cámaras o videocámaras, remitiendo directamente para estos fines a lo establecido en el art. 89 de la misma Ley. Así pues, debemos conjugar ambos artículos 22 y 89 con el objetivo de garantizar el tratamiento de datos personales de los sistemas de video vigilancia y control laboral.

El empresario puede tratar las imágenes obtenidas a través de sistemas de cámaras o videocámaras para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respectivamente, en el artículo 20.3 ET y en la legislación de función pública (y a tales efectos, ha de estarse a su marco legal). Si bien las imágenes grabadas en un soporte físico constituyen un dato de carácter personal que queda bajo el paraguas del art. 18.4 CE[47], el empresario no necesita el consentimiento expreso del trabajador para el tratamiento de las imágenes que han sido obtenidas a través de las cámaras instaladas en la empresa con la finalidad de seguridad o control laboral[48]. Ahora bien, dichos sistemas de videovigilancia deben utilizarse respetando su marco legal y con los límites inherentes al mismo. Sin embargo, la LOPD no determina cuándo la instalación de los dispositivos de videovigilancia es lícita y cuándo no, simplemente señala que "los empleadores deben informar con carácter previo, y de forma expresa, clara y concisa, a los trabajadores y, en su caso, a sus representantes, acerca de esta medida"[49].

No obstante, y sin perjuicio de las eventuales sanciones legales que pudieran derivar, para que el incumplimiento del deber de información por parte del empresario implique una vulneración del art. 18.4 CE exige valorar la observancia o no del principio de proporcionalidad. Deben ponderarse así en cada caso y a la vista de las circunstancias concurrentes los derechos y bienes constitucionales en conflicto; a saber, por un lado, el derecho a la protección de datos del trabajador y, por otro, el poder de dirección empresarial imprescindible para la buena marcha de la organización productiva. De este modo, se viene a dejar a salvo la constitucionalidad del control oculto cuando existen razonables sospechas de la comisión por parte del trabajador de graves irregularidades laborales[50].

No son pocas las resoluciones judiciales que atribuyen un tratamiento unitario a la actividad de control considerada de manera unívoca, sin diferenciar los distintos derechos fundamentales implicados en uno y otro caso. Efectivamente, no se aplica el principio de jerarquía de los derechos fundamentales sobre cualquier

47. STC 29/2013, de 11 febrero (RTC 2013, 29) (ECLI:ES:TC:2013:29).

48. STS 2 febrero 2017 (ECLI:ES:TS:2017:817).

49. Art. 89.1 LOPD. No se distingue si se trata de una instalación puntual de una cámara tras razonables sospechas de incumplimientos contractuales de los trabajadores o de un sistema permanente de videovigilancia.

50. STC 39/2016, de 3 marzo (RTC 2016, 39) (ECLI:ES:TC:2016:39). Se considera proporcionado la instalación de cámaras de video temporalmente instaladas en las cajas registradoras ante las razonables sospechas de la comisión de graves irregularidades por parte de un trabajador.

otro derecho por su lugar privilegiado en la carta magna, sino que el sistema de garantía debe basarse en el principio de proporcionalidad y equilibrio entre todos los derechos reconocidos constitucionalmente[51].

Estas prácticas restrictivas de derechos fundamentales, deben respetar de modo riguroso los principios anteriormente señalados, tanto en el momento de la adopción del sistema de videovigilancia empresarial: debe existir un interés legítimo que justifique la instalación de ellos dispositivos de control audiovisual (finalidad legítima); el recurso a la videovigilancia solo en el caso de *extrema ratio* (proporcionalidad); la recogida de datos no puede realizarse por medios fraudulentos, desleales o ilícitos (licitud); y se debe garantizar al trabajador el poder de disposición de sus propios datos de imagen y sonido (transparencia informativa).

Como durante la actividad de videovigilancia: adecuación y pertinencia de los datos. El aumento de la cantidad de datos generados en el entorno del lugar de trabajo con la industria 4.0, en combinación con las nuevas técnicas de análisis de datos y la comparación cruzada, también puede crear el riesgo de un tratamiento posterior ilegítimo (uso de sistemas instalados legítimamente para proteger las propiedades, pero para controlar después la disponibilidad, el desempeño y el trato de los trabajadores con los clientes).

Así, por ejemplo, existen espacios que por sus condiciones podría ser desproporcionado la utilización de la videovigiiancia, en vestuarios, taquillas y zonas de descanso de trabajadores: "en ningún caso se admitirá la instalación de sistemas de grabación de sonidos ni de videovigilancia en lugares destinados al descanso o esparcimiento de los trabajadores o los empleados públicos, tales como vestuarios, aseos, comedores y análogos"[52].

Y, por otro lado, tales prácticas deben tener en cuenta el respeto de los derechos específicos de los trabajadores. Se debe garantizar la protección de los derechos y libertades en relación con el tratamiento de datos personales de los trabajadores en el ámbito laboral, en particular a efectos de contratación de personal, ejecución del contrato laboral, incluido el cumplimiento de las obligaciones establecidas por la ley o por el convenio colectivo, gestión, planificación y organización del trabajo, igualdad y diversidad en el lugar de trabajo, salud y seguridad en el trabajo, protección de los bienes de empleados o clientes, así como a efectos del ejercicio y disfrute, individual o colectivo, de los derechos y prestaciones relacionados con el empleo y a efectos de la extinción de la relación laboral[53].

---

51. ORTEGA GIMÉNEZ, A. y GONZÁLEZ MARTÍNEZ, J. A.: "Protección de datos, secreto de las comunicaciones, utilización del correo electrónico por los trabajadores y control empresarial", en *Diario La Ley (Estudios Doctrinales)*, Año XXX, número 7188, 03 de junio (2009), Madrid, p. 4.

52. Art. 89.2 LOPD.

53. Art. 88.1 RGPD.

2.2. El raquitismo jurídico del ET sobre la videovigilancia empresarial

Ante esta progresiva sociedad digitalizada capaz de erosionar la esfera privada del trabajador, y partiendo de que el legislador siempre camina un paso por detrás de la realidad social que trata de normar, se une que nuestro ordenamiento jurídico laboral se caracteriza por la ausencia de reglas especiales aplicables a la actividad de control empresarial, quedando la previsión del art. 20.3 ET huérfana de toda referencia expresa al uso de estos sistemas. El raquitismo jurídico exhibido por el ET contrasta con la minuciosa y detallada regulación sobre la videovigilancia en el ámbito de la seguridad pública[54] contenida en la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las fuerzas y cuerpos de seguridad en lugares públicos[55].

El uso de cámaras y videocámaras con fines de control empresarial igualmente debe cumplir una serie de requisitos. Por un lado, el tratamiento de los datos se debe limitar a las finalidades previstas por el ET, esto es, para poder utilizar un sistema de esta naturaleza en el ámbito laboral, hace falta contar con la oportuna legitimación para ello, por lo que los empleadores pueden tratar las imágenes obtenidas a través de sistemas de cámaras o videocámaras para el ejercicio de las funciones de control de los trabajadores, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo. Así pues, el ET faculta al empresario para adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad y teniendo en cuenta, en su caso, la capacidad real de los trabajadores con discapacidad[56].

La previsión legal del art. 20.3 ET, se completa con otras previsiones singularmente previstas. Así el art. 20 bis ET autoriza al empleador a realizar el tratamiento de las imágenes obtenidas a través de dispositivos de videovigilancia con la limitación del respeto al derecho a la intimidad. El art. 18 ET establece una excepción a la inicial discrecionalidad en la elección del medio de control, al señalar que solo pueden realizarse registros sobre la persona del trabajador, en sus taquillas y efectos particulares, cuando sean necesarios para la protección del patrimonio empresarial y del de los demás trabajadores de la empresa, dentro del centro de trabajo y en horas de trabajo; y en su realización se debe respetar al máximo la dignidad e intimidad del trabajador y contar con la asistencia de un representante legal de los trabajadores o, en su ausencia del centro de trabajo, de otro trabajador de la empresa, siempre que ello fuera posible. El art. 20.2 ET indica que las facultades empresariales de vigilancia y control deben ejercerse de buena fe, es decir, de forma correcta y leal, adecuándose a

54. GOÑI SEIN, J. L., *La Videovigilancia Empresarial y la Protección de Datos Personales*, cit., p. 21.

55. BOE de 5 de agosto de 1997.

56. Art. 20.3 ET.

las específicas causas que las justifican. Y el art. 64.5.f) ET indica que la representación legal de los trabajadores debe emitir informe previo a la implantación o revisión por el empresario de todos los sistemas de control dirigidos a evaluar el cumplimiento de la prestación laboral o verificar el incumplimiento de las obligaciones laborales.

Observamos pues como el ET atribuye a la empresa facultades específicas para controlar el desarrollo de la prestación laboral, y el ejercicio de estas comporta en la mayoría de las ocasiones tratamientos de datos personales. Si en el desarrollo de la función empresarial de control se utilizan las nuevas tecnologías de la información de la industria 4.0, las posibilidades de repercusión en los derechos del trabajador se multiplican, lo cual obliga a tener en cuenta el respeto a los derechos fundamentales de los trabajadores, a adoptar medidas de control que sean proporcionales y respeten su dignidad (la dignidad humana se encuentra presente en todos los derechos fundamentales).

Para la AEPD, la aplicación del artículo 20.3 ET no legitima por sí solo el tratamiento de las imágenes, si bien este será posible, aún sin contar con el consentimiento del afectado en caso de que el trabajador haya sido debidamente informado de la existencia de esta medida, debiendo además ser claro que, los datos no podrán ser utilizados para fines distintos.

El control laboral como causa legitimadora para el tratamiento de datos personales no implica, *per se*, que quepa todo tratamiento de datos amparado en dicha finalidad. Y en el aspecto que nos ocupa relativo a la videovigilancia, el tratamiento de todas las imágenes que ocupan la jornada laboral de un trabajador, como mecanismo de seguimiento continuo y permanente de su actividad pudiera resultar excesivo al suponer una verdadera monitorización de los trabajadores, y sin que se ofrezca una causa concreta, temporalmente limitada y ponderada, como podría suceder si existiera un problema concreto con un trabajador determinado relativo al cumplimiento de sus deberes laborales[57].

3. PODER DE CONTROL EMPRESARIAL CON SISTEMAS DE VIDEOVIGILANCIA: ADECUADA PONDERACIÓN DE LAS CIRCUNSTANCIAS CONCURRENTES

La escasez de normativa legal sobre la materia, unida al rapidísimo crecimiento y desarrollo de nuevas formas de control amparadas en las tecnologías de la información y de la comunicación, han provocado que sean los Tribunales quienes estén llamados a realizar la adecuación entre estos nuevos sistemas y los derechos fundamentales, con lo cual la criticable imprecisión legislativa obliga a una labor creadora, cuasi legislativa de los tribunales[58].

---

57. Según Informe Jurídico 0475/2014 AEPD.

58. TASCÓN LÓPEZ, R., *El Tratamiento por la Empresa de Datos Personales de los Trabajadores. Análisis del estado de la cuestión*, Civitas, Madrid, 2005, p. 138.

El problema que plantea el art. 20.3 ET es el de la determinación de cuando los mecanismos de control empresarial, para el cumplimiento de los deberes laborales por los trabajadores, suponen una vulneración de derechos fundamentales del trabajador, convirtiéndose en ilegítima la facultad de vigilancia del empleador.

Podemos decir que hay un antes y un después en la jurisprudencia constitucional con la STC 39/2016, pues hasta la misma lo decisivo era debatir sobre la validez o no de la prueba empresarial obtenida mediante sistemas de videovigilancia, pasando a un segundo plano los pormenores de la información suministrada por el empresario a los trabajadores o las características del sistema de videovigilancia.

De la doctrina del TCO se deriva, como ha puesto de relieve la doctrina científica, que: a) por una parte, los derechos fundamentales del trabajador deben adaptarse a los requerimientos de la organización productiva en que se integra; b) por otra parte, que también las facultades empresariales se encuentran limitadas por los derechos fundamentales del trabajador, que son prevalentes y constituyen un "límite infranqueable" no solo a sus facultades sancionadoras, sino también a las facultades de organización y de gestión del empresario, causales y discrecionales; y, c) que cuando se prueba indiciariamente que una decisión empresarial puede enmascarar una lesión de derechos fundamentales incumbe al empresario acreditar que su decisión obedece a motivos razonables y ajenos a todo propósito atentatorio del derecho de que se trate y que es preciso garantizar en tales supuestos que los derechos fundamentales del trabajador no sean desconocidos por el empresario bajo la cobertura formal del ejercicio por parte de éste de los derechos y facultades reconocidos por las normas laborales[59].

Por tanto, el control empresarial sobre la actividad productiva del trabajador debe ser estrictamente laboral, sin que pueda afectar a facetas ajenas a la actividad laboral, o en lugares de trabajo no idóneos (espacios personales en los que esté en juego la intimidad individual o colectiva de los trabajadores), respetando siempre el principio de proporcionalidad.

En cuanto a la proporcionalidad es un elemento fundamental en todos los ámbitos en los que se instalen sistemas de videovigilancia u otro tipo de controles, dado que son numerosos los supuestos en los que la vulneración del mencionado principio puede llegar a generar situaciones abusivas, tales como la instalación de sistemas de vigilancia en espacios comunes, o aseos del lugar de trabajo. Por todo ello se trata de evitar la vigilancia omnipresente, con el fin de impedir la vulnerabilidad de la persona[60].

Según doctrina reiterada del TCO, una exigencia común y constante para la constitucionalidad de cualquier medida restrictiva de derechos fundamentales,

---

59. STS de 8 de marzo de 2011.

60. Según Informe Jurídico 0495/2009 AEPD.

entre ellas las que supongan una injerencia en los derechos a la integridad física y a la intimidad, y más en particular de las medidas restrictivas de derechos fundamentales adoptadas en el curso de un proceso penal viene determinada por la estricta observancia del principio de proporcionalidad. En este sentido, para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres siguientes requisitos o condiciones: si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)[61].

Ahora bien, esta legitimación no es absoluta y exige que el empresario informe de dicho tratamiento a los trabajadores y a sus representantes (el requisito informativo expreso es insalvable). No es suficiente que el tratamiento de datos resulte en principio lícito, por estar amparado por la Ley (LOPD y ET)[62], o que pueda resultar eventualmente, en el caso concreto de que se trate, proporcionado al fin perseguido; el control empresarial por esa vía, antes bien, aunque podrá producirse, deberá asegurar también la debida información previa. No contrarresta esa conclusión que existieran distintivos anunciando la instalación de cámaras y captación de imágenes en el recinto universitario, ni que se hubiera notificado la creación del fichero a la Agencia Española de Protección de Datos; era necesaria además la información previa y expresa, precisa, clara e inequívoca a los trabajadores de la finalidad de control de la actividad laboral a la que esa captación podía ser dirigida. Una información que debía concretar las características y el alcance del tratamiento de datos que iba a realizarse, esto es, en qué casos las grabaciones podían ser examinadas, durante cuánto tiempo y con qué propósitos, explicitando muy particularmente que podían utilizarse para la imposición de sanciones disciplinarias por incumplimientos del contrato de trabajo[63].

Las SSTC 29/2013 de 11 de febrero (RTC 2013, 29) y la 39/2016 de 8 de abril, valoran situaciones distintas a la vez de un derecho fundamental, el de su intimidad, dando como resultado distintas soluciones. En la sentencia de 2013 (que es la primera resolución específica sobre uso de sistemas de videovigilancia con fines de control laboral), se declara expresamente que no se puede carecer del requisito informativo, pues la empresa impone una sanción sirviéndose de datos obtenidos

---

61. STC 207/1996, de 16 diciembre (RTC 1996, 207) (ECLI:ES:TC:1996:207).

62. El tratamiento de datos de las personas trabajadoras por parte del empleador es lícito, cuando sea necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de éste de medidas precontractuales (art. 6.1.b) RGPD). La empresa puede tratar los datos personales necesarios para el normal desarrollo del acuerdo de voluntades plasmado en el contrato, como el nombre y los apellidos del trabajador, su fecha de nacimiento, su sexo, su nacionalidad, o su discapacidad, entre otros.

63. STC 29/2013 de 11 febrero (ECLI:ES:TC:2013:29).

en el exterior del lugar de trabajo lo que no cumple ni siquiera una función de advertencia implícita y que tampoco va unida a la comunicación específica dirigida a los trabajadores. En la segunda sentencia, una cámara es situada exactamente sobre la caja una vez producidos hechos irregulares sirviendo en definitiva para comprobar lo que era objeto de sospecha y se deniega el amparo que la trabajadora solicita.

Con la STC 39/2016, se crea una nueva jurisprudencia constitucional a la establecida desde 2013, siendo más sencillo superar el juicio de contradicción, pues se amplían considerablemente las posibilidades empresariales de utilización de sistemas de videovigilancia sin lesión de derechos fundamentales a la intimidad (art. 18 CE), y a la autodeterminación informativa y derecho a la privacidad (art. 18.4 CE):

En paralelo, las resoluciones del TS tampoco muestran uniformidad basando la licitud en el juicio de proporcionalidad. Tras la citada sentencia, reiterada jurisprudencia del TS[64] recuerda que el empresario no necesita el consentimiento expreso del trabajador para el tratamiento de las imágenes que han sido obtenidas a través de las cámaras instaladas en la empresa con la finalidad de seguridad o control laboral, ya que se trata de una medida dirigida a controlar el cumplimiento de la relación laboral, y es conforme con el art. 20.3 ET. En el ámbito laboral el consentimiento del trabajador pasa, por tanto, como regla general a un segundo plano pues el consentimiento se entiende implícito en la relación negocial, siempre que el tratamiento de datos de carácter personal sea necesario para el mantenimiento y el cumplimiento del contrato firmado por las partes.

La constitucionalidad de cualquier medida restrictiva de derechos fundamentales viene determinada por la estricta observancia del principio de proporcionalidad, y para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres requisitos o condiciones siguientes: si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)[65]. Lo que entraña la necesidad de proceder a una ponderación adecuada que respete la definición y valoración constitucional de los derechos fundamentales y que atienda a las circunstancias concurrentes en cada caso concreto[66].

---

64. SSTS de 2 febrero (ECLI:ES:TS:2017:817 [RJ 2017, 1628]), de 1 febrero (ECLI:ES:TS:2017:811), y 31 enero 2017 (ECLI:ES:TS:2017:654); y 7 julio 2016 (ECLI:ES:TS:2016:4070).

65. STC 186/2000, de 10 de julio (ECLI:ES:TC:2000:186).

66. STC 151/2004, de 20 de septiembre (RTC 2004, 151) (ECLI:ES:TC:2004:151).

Superado dicha prueba de proporcionalidad, se pueden adoptar medidas de control, respetando siempre el derecho a la protección de datos cuando se produzca un tratamiento de datos personales. Abogamos por las medidas preventivas (más que la mera detección) para evitar el riesgo de la vulneración posterior de derechos fundamentales en la fase de control, prevención vinculada a la subsidiariedad, pues la medida potencialmente invasiva de derechos fundamentales debe ceder frente a medidas preventivas que eliminen el riesgo.

En este sentido el Dictamen 4/2004, señala respecto a la proporcionalidad del recurso a la vigilancia por videocámara, "...que el circuito cerrado de televisión y otros sistemas similares de vigilancia por videocámara sólo podrán utilizarse con carácter subsidiario, es decir: con fines que realmente justifiquen el recurso a tales sistemas. (...). Deberá evitarse, por ejemplo, que un organismo administrativo pueda instalar equipos de vigilancia por videocámara en relación con infracciones de menor importancia (por ejemplo, para reforzar la prohibición de fumar en los colegios y otros lugares públicos o la prohibición de tirar colillas y papeles al suelo en los lugares públicos). Dicho de otro modo, es necesario aplicar, caso por caso, el principio de idoneidad con respecto a los fines perseguidos, lo que implica una especie de obligación de minimización de los datos por parte del responsable del tratamiento".

IV. BIBLIOGRAFÍA

GONZÁLEZ MARTÍNEZ, J. A.: "Tratamiento de la información por las entidades financieras y la protección de datos: ¿se respeta la privacidad?", en *Revista española de Protección de Datos*, número especial 7 (julio 2009-junio 2010), Madrid.

GONZÁLEZ MARTÍNEZ, J. A. y ORTEGA GIMÉNEZ, A.: "El sector financiero y la protección de datos: el precio de nuestra intimidad", en *Actualidad Jurídica Aranzadi*, número 822, 9 de junio (2011), Cizur Menor (Navarra).

GOÑI SEIN, J. L.: La Videovigilancia Empresarial y la Protección de Datos Personales, Civitas, Madrid, 2007.

KAHALE CARRILLO, D. T.: "La industria 4.0: los retos para el empleo español", en *Los actuales cambios sociales y laborales: nuevos retos para el mundo del trabajo*, Suiza, Peter Lang, 2017.

KAHALE CARRILLO, D. T. y OTROS: El impacto de la industria 4.0 en el trabajo. Una visión interdisciplinar, Aranzadi, Pamplona, 2020.

OLIVER LALANA, A. D.: "Autorregulación, normas jurídicas y tecnologías de la privacidad. El lado virtual del derecho a la protección de datos", en *XVII Encuentros sobre Informática y Derecho (2002-2003)*, Facultad de Derecho, Instituto de Informática Jurídica, Universidad Pontificia Comillas, Madrid, 2003.

ORTEGA GIMÉNEZ, A. y GONZÁLEZ MARTÍNEZ, J. A.: "Protección de datos, secreto de las comunicaciones, utilización del correo electrónico por los trabajadores y control empresarial", en *Diario La Ley (Estudios Doctrinales)*, Año XXX, número 7188, 03 de junio (2009), Madrid.

PÉREZ DEL PRADO, D.: "Representación de los trabajadores y protección de datos de carácter personal como fuente de poder", en *Documentación Laboral, núm. 119, año 2020, Vol. I. Protección de datos y relaciones laborales*, 2020.

RODRÍGUEZ ESCANCIANO, S.: "Vigilancia y control en la relación de trabajo: la incidencia de las nuevas tecnologías", en *La protección de datos de carácter personal en los centros de trabajo*, Cinca, Madrid, 2006.

SEMPERE NAVARRO, A. V. y SAN MARTÍN MAZZUCONI, C.: *Nuevas Tecnologías y Relaciones Laborales*, Aranzadi, Pamplona, 2002.

TASCÓN LÓPEZ, R.: El Tratamiento por la Empresa de Datos Personales de los Trabajadores. Análisis del estado de la cuestión, Civitas, Madrid, 2005.

TRONCOSO REIGADA, A.: "Introducción y presentación", en *Repertorio de Legislación y Jurisprudencia sobre Protección de Datos*, Civitas, Madrid, 2004.