El impacto del RGPD en el ámbito del control laboral y la era de la innovación

Raúl Rojas Rosco

Socio Labour Compliance en ECIJA

Daniel López Carballo

Socio IT, Privacy and Data Protection en ECIJA

Resumen: *Los tratamientos de datos en el ámbito laboral son acometidos a través de disposiciones legislativas o de convenios colectivos donde se establece normas para 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. Dichas normas incluirán medidas adecuadas y específicas para preservar la dignidad humana de los interesados así como sus intereses legítimos y sus derechos fundamentales, prestando especial atención a la transparencia del tratamiento, a la transferencia de los datos personales dentro de un grupo empresarial o de una unión de empresas dedicadas a una actividad económica conjunta y a los sistemas de supervisión en el lugar de trabajo.*

Palabras clave: Tratamiento de datos personales de los trabajadores. Reglamento General de Protección de Datos. Control sobre el uso de sistemas informáticos. Sistemas de registro biométricos. Sistemas de videovigilancia. Sistemas de videovigilancia oculta o secreta. Geolocalización.

Abstract: *The processing of data in the workplace is addressed through legislative provisions or collective agreements which establish provisions to ensure the protection of the rights and freedoms with regard to the processing of personal data of workers in the field of labour, in particular for the purpose of recruitment of staff, implementation of the labour contract, including the fulfilment of the obligations established by law or by the collective agreements, management, planning and organization of work, equality and diversity in the workplace,*

health and safety at work, protection of the property of employees or customers, as well as for the purpose of the exercise and enjoyment, individual or collective, of the rights and benefits related to work, and the effects of the termination of the employment relationship, and that these provisions shall include appropriate and specific measures to preserve the human dignity of the interested parties as well as their legitimate interests and their fundamental rights, paying particular attention to transparency of the processing, to the transfer of personal data within a business group or a group of companies dedicated to a joint economic activity and monitoring systems in the workplace.

Keywords: Processing of personal data of workers, General Data Protection Regulation, control over the use of computer systems, biometric registration systems, video surveillance systems, hidden or secret video surveillance systems, geolocation.

I. Introducción

Como punto de partida para el presente análisis, podemos tomar la cita «big brother is watching you» de la afamada distopía escrita en 1949 por George Orwell, en la que se describe una sociedad del futuro donde está presente el control absoluto y la vigilancia masiva de sus ciudadanos y donde simplemente el pensamiento de incumplir una norma suponía ya un incumplimiento en sí mismo.

Afortunadamente en nuestra sociedad todavía no hemos llegado a este extremo, si bien es cierto que las posibilidades de vigilancia y control que plantea la implantación de las nuevas tecnologías, especialmente en el entorno laboral, se antojan prácticamente ilimitadas. Pero, este control empresarial, ¿tiene límites? ¿el empresario puede vigilar todos y cada uno de los actos del trabajador durante su jornada de trabajo? ¿y fuera de ella?

En el presente artículo se intentará responder a estas y otras cuestiones a la luz de los últimos criterios jurisprudenciales existentes al respecto, no sólo desde el punto de vista del cumplimiento normativo laboral, sino también, y especialmente, desde la protección de los datos de carácter personal de los empleados. Se partirá de un análisis de la situación actual e intentaremos atisbar el futuro inmediato que nos puede deparar esta irrupción de las nuevas tecnologías en el ámbito del control laboral, sus posibles límites e implicaciones en materia de derechos fundamentales.

En este sentido, no podemos obviar que tanto las empresas como los empleados cuentan con más y mejores recursos tecnológicos para el desarrollo de su trabajo, permitiendo, a su vez, una mayor flexibilización en las relaciones jurídicas derivadas de la prestación laboral (trabajo a distancia en la nube, acceso a internet generalizado, uso de dispositivos móviles, smartphones, cuentas de correo electrónico, redes sociales corporativas, etc.), y, con ello, una mayor y más eficiente productividad laboral.

Así las cosas, la implementación de dichas tecnologías, junto con el necesario avance de los diferentes modelos empresariales, conllevan un avance en la forma en que los datos son recabados y posteriormente tratados por las empresas. Un avance, imparable que, por ejemplo, hace que el empresario trate más información sobre sus empleados de la que trataba años antes. Información que puede ser explotada con diferentes finalidades, desde la mejora de las condiciones de trabajo, intensificar o mejorar la relación con sus clientes, u optimizar los recursos existentes en su ámbito.

Criterio avalado por el Grupo de Trabajo del art. 29 que en su Dictamen 8/2001 recogía que, «la recopilación, almacenamiento y uso de información sobre los trabajadores por medios electrónicos, y las diversas herramientas de uso común en buena parte de las empresas, tales como el correo electrónico o el acceso a Internet, implican en muchas ocasiones el tratamiento de datos personales de los trabajadores. A ello se unen otras nuevas modalidades de control del trabajador, que llegan de la mano de la imagen y el sonido, entre las que destacan los sistemas de videovigilancia a los que se debe aplicar la normativa sobre protección de datos».

Y es que el avance de la tecnología ha conllevado la necesaria actualización de conceptos jurídicos tales como la propia definición de datos personales. Nuestra actual Ley Orgánica 15/1999, de 13 de diciembre de protección de datos de carácter personal (LOPD), introducía el concepto

como cualquier información concerniente a personas físicas identificadas o identificables. Y es en este punto en el que la información que obtenemos del empleado, no sólo es mayor, sino que es tratada de diferentes formas. Sírvase como ejemplo la utilización de sistemas de geolocalización, el uso de wearables, o el avance imparable tecnológico. Conceptos íntimamente unidos a las nuevas formas de comunicación con los clientes o usuarios o el asentamiento de la multicanalidad, conllevan que la información generada por el propio empleado, o aquella a la que éste tiene acceso, se haya maximizado en los últimos tiempos.

Las posibilidades de vigilancia y control que plantea la implantación de las nuevas tecnologías, especialmente en el entorno laboral, se antojan prácticamente ilimitadas

Un concepto y normativa que ha sido actualizado, tras la aprobación del Reglamento (UE) 2016/679 del Parlamento Europeo y el 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 (RGPD), actualmente en vigor y cuya plena aplicación será el 25 de mayo del presente año.

Esta nueva norma europea, de aplicación directa en todos los Estados de la Unión Europea, viene a actualizar, conforme a los cambios que comentábamos y el avance tecnológico, la reglas sobre el tratamiento de los datos personales, una suerte de reconocimiento de mayoría de edad de las empresas para llevar a cabo dichos tratamientos. Así las cosas, pasamos de un sistema muy tutelado, en el que el responsable debía notificar los tratamientos a la Autoridad de Control, a un sistema que se basa en el conocimiento de la propia empresa, en el análisis de los riesgos asociados a los tratamientos, en la incorporación de conceptos como la privacidad desde el diseño y por defecto, que vienen a empoderar este derecho fundamental reconocido constitucionalmente.

Y es que, el auge tecnológico ha conllevado a que determinada información que a priori no entraba dentro de las definiciones previas de datos personal, hoy, puedan englobarse. Datos como la dirección IP, o procesos de identificación de personas derivados de la aplicación de técnicas de tratamientos masivos de datos, hacen que, junto con la ampliación conceptual, sea cada vez más difícil la Anonimización completa de los datos y por tanto la no aplicabilidad de la nueva normativa europea.

Igualmente, hemos comprobado cómo, el nuevo marco europeo, incluye determinados datos que hasta la fecha sólo veíamos recogidos en informes de las autoridades de control o del propio Grupo de Trabajo del art. 29, como el dato biométrico, una realidad en nuestra vida cotidiana (*e.g.* sistema de desbloqueo de teléfonos móviles mediante la huella dactilar), que en este marco se eleva su nivel de protección considerándolo como categoría especial de datos, con las limitaciones que analizaremos. Estableciendo el Considerando 52 que, «deben autorizarse excepciones a la prohibición de tratar categorías especiales de datos personales cuando lo establezca el Derecho de la Unión o de los Estados miembros y siempre que se den las garantías apropiadas, a fin de proteger datos personales y otros derechos fundamentales, cuando sea en interés público, en particular el tratamiento de datos personales en el ámbito de la legislación laboral, la legislación sobre protección social, incluidas las pensiones y con fines de seguridad, supervisión y alerta sanitaria, la prevención o control de enfermedades transmisibles y otras amenazas graves para la salud». Excepciones que bien a recoger el art. 9 del RGPD, cuando «el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado».

Así, el Considerando 155 del RGPD reconoce que «el Derecho de los Estados miembros o los convenios colectivos, incluidos los "convenios de empresa", pueden establecer normas específicas relativas al tratamiento de datos personales de los trabajadores en el ámbito laboral, en particular en relación con las condiciones en las que los datos personales en el contexto laboral pueden ser

objeto de tratamiento sobre la base del consentimiento del trabajador, los fines de la contratación, la ejecución del contrato laboral, incluido el cumplimiento de las obligaciones establecidas por la ley o por convenio colectivo, la gestión, planificación y organización del trabajo, la igualdad y seguridad en el lugar de trabajo, la salud y seguridad en el trabajo, así como a los fines del ejercicio y disfrute, sea individual o colectivo, de derechos y prestaciones relacionados con el empleo y a efectos de la rescisión de la relación laboral».

En todo caso, el propio art. 88 hace expresa mención a los tratamientos de datos en el ámbito laboral, estableciendo que, los Estados miembros podrán, a través de disposiciones legislativas o de convenios colectivos, establecer 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, 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. Y que dichas normas incluirán medidas adecuadas y específicas para preservar la dignidad humana de los interesados así como sus intereses legítimos y sus derechos fundamentales, prestando especial atención a la transparencia del tratamiento, a la transferencia de los datos personales dentro de un grupo empresarial o de una unión de empresas dedicadas a una actividad económica conjunta y a los sistemas de supervisión en el lugar de trabajo.

Esta revolución digital, a la que hacíamos referencia, está posibilitando innovadoras fórmulas de colaboración y de desarrollo productivo, pero también nuevas formas de control empresarial sobre el trabajo desempeñado por sus empleados (control sobre el uso de medios tecnológicos puestos a su disposición, geolocalización, videovigilancia, sistemas de registro o login mediante huella digital, entre otros). Por lo tanto, el desafío de los próximos años, en nuestra opinión, estará centrado principalmente en determinar cuáles serán los límites de esa vigilancia que pueda ejercer el empresario ante incumplimientos laborales de los trabajadores, puesto que de ello dependerá en definitiva la licitud de la actividad de control empresarial.

El desafío de los próximos años estará centrado principalmente en determinar cuáles serán los límites de la vigilancia que pueda ejercer el empresario ante incumplimientos laborales de los trabajadores

Ha sido la jurisprudencia del Tribunal Supremo (TS) y del Tribunal Constitucional (TC), la que se ha ido ocupando de delimitar el poder de dirección y control del empresario, regulado en el art. 20 del Estatuto de los Trabajadores (ET). Dicho control, según esta doctrina judicial que iremos citando a lo largo del artículo, se ha de llevar a cabo siempre con la consideración debida a la dignidad del trabajador y respetando derechos constitucionales de los empleados tan básicos como el del honor, la intimidad, la propia imagen o el del secreto de las comunicaciones.

En el mismo sentido, el Tribunal Superior de Justicia de Navarra, en su Sentencia 263/10, establece que este tipo de medidas de control deberán ser justificadas e idóneas para las finalidades de verificación, por parte de la empresa, de posibles irregularidades laborales; necesarias, es decir, que no supongan un tratamiento de datos de manera general o masiva, instalando cámaras en toda la superficie sin un criterio de elección de ángulo; y equilibradas, debiendo descartarse cualquier posible lesión a la intimidad personal del afectado, dando cumplimiento a lo establecido en el art. 18.1 de nuestra Constitución.

Sin embargo, y de acuerdo con la doctrina constitucional, el ejercicio de estos derechos fundamentales, en el seno de una relación laboral de ajenidad y dependencia contrato, no es absoluto, sino que se encuentra modulado o limitado por las mencionadas facultades de organización, dirección y control empresarial, así como por los legítimos derechos constitucionales de libertad de empresa (*ex* arts. 33 y 38 CE) en un equilibrio necesario de derechos de ambas partes, de acuerdo con el principio de proporcionalidad. Un equilibrio que encuentra mayor

relevancia, teniendo en cuenta, que nos encontramos con otros derechos fundamentales de los empleados, reconocidos en nuestra Carta Magna, como es el derecho al honor, la intimidad personal y familiar y a la protección de sus datos personales, entre otros (*ex* art. 18 CE). A mayor abundamiento, tal y como establece el art. 20.3 ET, el empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana y teniendo en cuenta la capacidad real de los trabajadores disminuidos, en su caso.

En materia de control empresarial, y posible limitación de derechos fundamentales, este principio de equilibrio de derechos constitucionales viene exigido de un lado por una necesaria información previa de dicho control, y de otro, por la superación del denominado «juicio de proporcionalidad», acuñado por el Tribunal Constitucional (STC 96/2012, de 7 de mayo, FJ 10; o SSTC 14/2003, de 28 de enero, FJ9; 89/2006, de 27 de marzo, FJ3) y seguido tanto por el Tribunal Supremo como por la jurisprudencia de suplicación.

Para superar este test de proporcionalidad será necesario el cumplimiento de cuatro condiciones para apreciar si el sistema de vigilancia implantado y el control efectuado es pertinente, adecuado y no excesivo para la satisfacción de los objetivos e intereses empresariales: (i) si tal medida es susceptible de conseguir el objetivo propuesto de controlar la actividad laboral y/o incumplimientos del trabajador (juicio de idoneidad); (ii) si la medida 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); (iii) si la medida 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); y finalmente si la medida está justificada, es decir, si existen razones objetivas y motivadas que legitimen la decisión de control empresarial (juicio de justificación).

La fórmula o sistema concreto que se elija para la verificación de la actividad laboral de los trabajadores determinará, a su vez, la afectación y el grado de invasión de uno o varios derechos fundamentales, ante lo cual se deberá realizar previamente, como establece el Tribunal Constitucional, el test de proporcionalidad de dichos sistemas o medidas de control, y posteriormente el establecimiento e implantación de unos protocolos concretos que garanticen un control lícito con respeto de esos posibles derechos fundamentales que pudieran ser afectados.

Mismo criterio recogido en la Sentencia del Tribunal de Justicia de la Unión Europea de 30 de mayo de 2013, en la que el Tribunal, aporta aclaraciones en relación con 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 la libre circulación de estos datos, entre otros, que los datos deben ser recogidos con fines determinados, explícitos y legítimos, así como adecuados, pertinentes y no excesivos conforme a los fines comentados.

El control empresarial, y posible limitación de derechos fundamentales, habrá de valorarse a la luz del principio de equilibrio de derechos constitucionales

A mayor abundamiento, ya la Agencia Española de Protección de Datos, en su Guía sobre la protección de datos en las relaciones laborales, al referirse a la facultad de control laboral del empresario, recordaba que, el uso de tecnologías de la información multiplica las posibilidades de control empresarial, y 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, su derecho a la protección de datos y su vida privada.

En relación con la información previa, la propia Agencia Española de Protección de Datos establece que, «es necesario recordar lo que ya se dijo sobre la existencia de un hábito social generalizado de tolerancia con ciertos usos personales moderados de los medios informáticos y de comunicación facilitados por la empresa a los trabajadores. Esa tolerancia crea una expectativa también general de confidencialidad en esos usos; expectativa que no puede

ser desconocida, aunque tampoco convertirse en un impedimento permanente del control empresarial, porque, aunque el trabajador tiene derecho al respeto a su intimidad, no puede imponer ese respeto cuando utiliza un medio proporcionado por la empresa en contra de las instrucciones establecidas por ésta para su uso y al margen de los controles previstos para esa utilización y para garantizar la permanencia del servicio. Por ello, lo que debe hacer la empresa de acuerdo con las exigencias de buena fe es establecer previamente las reglas de uso de esos medios —con aplicación de prohibiciones absolutas o parciales— e informar a los trabajadores de que va existir control y de los medios que han de aplicarse en orden a comprobar la corrección de los usos, así como de las medidas que han de adoptarse en su caso para garantizar la efectiva utilización laboral del medio cuando sea preciso, sin perjuicio de la posible aplicación de otras medidas de carácter preventivo, como la exclusión de determinadas conexiones. De esta manera, si el medio se utiliza para usos privados en contra de estas prohibiciones y con conocimiento de los controles y medidas aplicables, no podrá entenderse que, al realizarse el control, se ha vulnerado "una expectativa razonable de intimidad" en los términos que establecen las sentencias del Tribunal Europeo de Derechos Humanos de 25 de junio de 1997 (caso Halford) y 3 de abril de 2007 (caso Copland) para valorar la existencia de una lesión del art. 8 del Convenio Europeo para la protección de los derechos humanos. (Sentencia de la Sala de lo Social del Tribunal Supremo de 26 de septiembre de 2007)».

La falta de información previa y de la proporcionalidad de la medida de control determinará la ilicitud de la actuación empresarial y la nulidad de las pruebas que se obtengan derivadas de dichas actuaciones, así como, en su caso, de la medida disciplinaria adoptada con base en dichas pruebas (Doctrina del fruto del árbol envenenado).

Veamos algunos de los sistemas de control basados en las nuevas tecnologías más utilizadas, sus peculiaridades e implicaciones en la esfera de los derechos fundamentales de los trabajadores.

II. Control sobre el uso de sistemas informáticos

Los empleados, en la prestación diaria de su trabajo, utilizan distintas herramientas y sistemas informáticos, habitualmente propiedad de la empresa, que pueden ser susceptibles de control y vigilancia empresarial (ordenador, dispositivos móviles, smartphones, internet, intranet, sistemas telefónicos, correo electrónico, acceso a las instalaciones o a equipos informáticos, entre otros).

El Tribunal Supremo, desde su ya clásica Sentencia de fecha 26 de septiembre de 2007 y en otras muchas posteriores (entre otras la STS 6/10/2011), ha establecido cuáles son los límites en el ejercicio de las facultades de control empresarial del uso por parte de los trabajadores de los medios tecnológicos propiedad de la empresa puestos a su disposición, creando la figura jurisprudencial de la «expectativa razonable de intimidad» en dicho uso.

Para evitar que el empleado genere esta expectativa de privacidad sobre la utilización de los equipos informáticos, archivos, comunicaciones mediante correo electrónico corporativo y/o acceso a internet o redes sociales de la empresa, y por tanto pueda determinar la nulidad de la medida de control por vulneración del derecho a la intimidad, la jurisprudencia mencionada exige, o bien que los dispositivos sean de uso común con canales abiertos de comunicación, o bien debe de existir una comunicación previa y expresa de las concretas reglas de uso de los medios puestos a disposición del trabajador, mediante prohibiciones parciales o totales de su uso privado o ajenos a fines profesionales.

A esta comunicación previa se deberá acompañar:

- Información escrita sobre la existencia de la posibilidad de control empresarial sobre dicho uso.
- Reglas o normas concretas del uso de estos medios (con prohibiciones totales o parciales del uso extra-laboral).
- Medios de control que utilizará la empresa para tal fin (software de monitorización o de captura de pantallas, informes periciales informáticos, acceso a contenidos, entre otros).
- Adopción, en su caso, de medidas disciplinarias para los casos de incumplimiento.

Así, debe recordarse en septiembre de 2017, la Sentencia de la Gran Sala del Tribunal Europeo de Derechos Humanos, que fallaba a favor de un trabajador cuyo empleador espió sus mensajes privados en su cuenta profesional de correo electrónico. Fallo mediante el que se rectificaba otra sentencia de la Sala. La Corte europea dio la razón al trabajador porque los tribunales no verificaron si el demandante había sido advertido por su empleador de la posibilidad de que sus comunicaciones fueran vigiladas, ni de la naturaleza y el alcance de esa vigilancia.

III. Sistemas de registro biométricos

Por su parte, otro de los aspectos importantes a tener en cuenta en el uso de medios tecnológicos para el control laboral referido al acceso a las instalaciones de la empresa y el control horario, es la utilización de sistemas de registro o fichaje biométrico.

Estos sistemas, cada vez con mayor implantación en las empresas, captan determinados parámetros biométricos de la huella digital, el iris, voz o la morfología del rostro del empleado, con la finalidad de identificar al trabajador en su acceso a determinadas zonas de trabajo posibilitando con ello un registro de la hora concreta de entrada y salida. Cabe preguntarse, si estos sistemas afectan a derechos tan básicos como la intimidad o la propia integridad física o moral del trabajador. A mayor abundamiento debe recordarse que el art. 4 del RGPD define datos de carácter personal como «toda información sobre una persona física identificada o identificable ("el interesado"); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona», entendiéndose que, los datos biométricos, bajo esta definición, tendrían la consideración de datos de carácter personal.

A mayor abundamiento, el propio RGPD define los datos biométricos, como datos personales «obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos» (*ex* art. 4.14 RGPD).

Sobre esta cuestión ya han tenido oportunidad de pronunciarse tanto el Tribunal Supremo (STS 2/07/2007) y jurisprudencia de suplicación (STSJ Murcia 25/01/2010), como la Agencia de Protección de Datos (entre otros, Informe 0324/2009), estableciendo claramente la licitud de estos sistemas al tratarse de medidas adecuadas, pertinentes y no excesivas, estando limitadas a la mera identificación de los empleados para el cumplimiento del control horario. No existirá intromisión ilegítima en la intimidad de los empleados, siempre y cuando exista una advertencia e información previa tanto de su instalación como de los motivos de su implantación, haciendo especial mención de su uso para el control laboral. En estos casos, si bien se exigen información previa, no será necesario el consentimiento expreso del trabajador cuando «el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales» (*ex* art. 6.1 del RGPD) o en aquellos casos en los que «el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento» o, en algunos casos, cuando «el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales».

IV. Sistemas de videovigilancia

El marco jurídico laboral en el que se encuadra este supuesto de hecho es, de un lado, el ordenamiento jurídico laboral y la Constitución Española, y, de otro la normativa específica en materia de protección de datos personales en el marco del contrato de trabajo, y más concretamente, en lo que respecta a la captación de imágenes de los empleados.

Actualmente, la regulación normativa del control laboral por medios tecnológicos se sitúa, como

indicábamos, en al art. 20.3 del Estatuto de los Trabajadores (ET), el cual regula, con carácter general, la facultad del empresario de adoptar todas aquellas medidas de vigilancia y control «que estime más oportunas» para verificar el cumplimiento de las obligaciones laborales de sus trabajadores, «guardando en su adopción y aplicación la consideración debida a la dignidad de los trabajadores». La adopción de estas medidas de control, por lo tanto, estará justificada por el legítimo ejercicio de las facultades empresariales de dirección y control, pero siempre que dichas facultades sean ejercidas por el empresario sin vulnerar los derechos fundamentales de los trabajadores.

De acuerdo con el precitado artículo la licitud de la utilización de sistemas de videovigilancia para control laboral vendrá determinada, entre otras cuestiones, por la finalidad del concreto uso y tratamiento de las imágenes captadas a los empleados. Es decir, siempre que las imágenes se capten con la finalidad de supervisar el cumplimiento de las obligaciones laborales de los trabajadores, y no se vulneren sus derechos fundamentales, tales como la propia imagen, la dignidad o la intimidad, la medida de videovigilancia se considerará como regla general adecuada y no excesiva.

En materia de control mediante sistemas de videovigilancia, la doctrina del Tribunal Constitucional (STC 292/00, entre otras), ratificada recientemente por la STC 29/2013, de 11 de febrero, con invocación de los derechos fundamentales de los arts. 18.1 CE (honor, intimidad y propia imagen) y, especialmente, el 18.4 CE (limitación del uso de la informática para garantizar el honor y la intimidad), ha venido exigiendo, igualmente que en los casos anteriores, la existencia de una información previa a los trabajadores para que dicho control sea lícito, y por ende, las pruebas derivadas de las grabaciones efectuadas.

La doctrina del TC exige la existencia de una información previa a los trabajadores para que este control sea lícito, y por ende, las pruebas derivadas de las grabaciones efectuadas

Debe recordarse, en caso de implementar este tipo de sistemas de control laboral, que el empresario deberá adoptar determinadas garantías, a título enunciativo, el art. 7 de la Ley Orgánica 1/1982, de 5 de mayo, sobre protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, y el art. 4.2.e ET (en la relación de trabajo, los trabajadores tienen derecho (…) al respeto de su intimidad y a la consideración debida a su dignidad, comprendida la protección frente al acoso por razón de origen racial o étnico, religión o convicciones, discapacidad, edad u orientación sexual, y frente al acoso sexual y al acoso por razón de sexo).

Así las cosas, dado que la imagen de los empleados captada por medios técnicos es considerada un dato de carácter personal, a los efectos de citada normativa europea en materia de protección de datos y teniendo en cuenta que la utilidad sería el control del cumplimiento de las obligaciones laborales contenidas en el contrato de trabajo y el trabajador es parte de dicho contrato de trabajo, si bien no sería necesario su previo consentimiento para que sean grabados, sí que existirá la obligación por parte de la empresa de informarles, de acuerdo con el derecho fundamental a la intimidad y la limitación del uso de la informática (art. 18.4 CE), así como el propio RGPD. En este sentido, el art. 13 del RGPD establece la información que deberá facilitarse cuando los datos personales se obtengan del interesado, en este caso por arte de la empresa, especificándose, a título enunciativo más no limitativo, la identidad y los datos de contacto del responsable y, en su caso, de su representante, los datos de contacto del delegado de protección de datos, en su caso, los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento, o el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo, entre otros aspectos.

En lo que respecta a la obligación de información, la Agencia Española de Protección de Datos, a través de su Instrucción 1/2006, de 8 de noviembre, establece la obligación de «colocar, en las zonas videovigiladas, al menos un distintivo informativo ubicado en lugar suficientemente visible, tanto en espacios abiertos como cerrados», y «tener a disposición de los/las interesados impresos en los que se detalle la información prevista en el art. 5.1 de la Ley Orgánica 15/1999»

(«información genérica»), aspecto que deberá ser actualizado en relación con el precitado derecho de información recogido en el RGPD.

En este sentido, la jurisprudencia constitucional tradicional, y en concreto la Sentencia del Tribunal Constitucional 29/2013, de 11 de febrero, establecía que el mero cumplimiento de estas exigencias que establecía la AEPD, es decir, el ofrecimiento de esa «información genérica» no implicaba necesariamente el cumplimiento del deber de información a los trabajadores por parte del empresario con respecto a la captación de sus imágenes en el entorno laboral. Según señalaba el Tribunal Constitucional en esa línea jurisprudencial, el deber de información exigía que fuera más específica, es decir, se debe proporcionar al empleado una «información previa y expresa, precisa, clara e inequívoca a los trabajadores de la finalidad laboral a que esa captación podría ser dirigida», debiendo, por tanto, «concretar las características y el alcance del tratamiento de datos que iba a realizarse, esto es, en qué casos las grabaciones podrían 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» («información específica»).

Sin embargo, dicha línea jurisprudencial cambia con la sentencia del Tribunal Constitucional de 3 de marzo de 2016 (STC 39/16), ratificada posteriormente por el Tribunal Supremo en sendas sentencias, introduciendo, como corrección de la doctrina anterior, importantes cambios en lo que respecta a este deber de información y su concreto alcance, relajando las exigencias de una información más específica y con mayor rigor, tal y como que se venía requiriendo hasta este momento.

En la propia STC 39/16 se hace expresa mención a su especial trascendencia en el marco constitucional dado que «las especificidades propias del caso permiten a este Tribunal perfilar o aclarar su doctrina en relación con el uso de cámaras de videovigilancia en la empresa», siendo la finalidad de la misma «aclarar el alcance de la información a facilitar a los trabajadores sobre la finalidad del uso de la videovigilancia en la empresa: si es suficiente la información general o, por el contrario, debe existir una información específica (tal como se había pronunciado la STC 29/2013, de 11 de febrero)».

El supuesto de hecho enjuiciado por el Tribunal Constitucional parte de la instalación de una cámara de videovigilancia en un establecimiento comercial de la conocida empresa, ante las sospechas de que en la tienda se estaban produciendo numerosas irregularidades contables en la caja de la tienda. La cámara se instaló sin una previa comunicación a los trabajadores, si bien cumplió con las obligaciones del art. 3 de la Instrucción 1/2006, en lo referente a la instalación de un distintivo informativo, y la puesta a disposición de una cláusula informativa que cumplía con los requisitos del deber de información.

Una vez evidenciado el incumplimiento laboral, consistente en la apropiación por parte de la empleada de dinero de la caja, la empresa le comunicó su despido disciplinario, aportando como evidencia de dicho incumplimiento las imágenes captadas por el sistema de video-vigilancia. La trabajadora presentó demanda impugnando el despido por la que solicitaba la declaración de nulidad del mismo, por atentar contra su derecho al honor, intimidad y dignidad, y subsidiariamente la declaración de improcedencia, desestimadas ambas pretensiones tanto en primera instancia como en sede de suplicación.

El Tribunal Constitucional, limitándose en este caso a la revisión del cumplimiento de los arts. 18.1 y 18.4 de la Constitución Española, con respecto al derecho fundamental a la intimidad y la protección de datos de carácter personal, consideró que el contenido y diseño del distintivo informativo era perfectamente visible por los trabajadores que prestaban servicios en el establecimiento y por lo tanto que se ajustaba a lo previsto por la norma, teniendo por cumplida la obligación de información, en este caso, genérica, impuesta por la normativa de protección de datos personales. En este sentido, el dato relevante para el Tribunal es que la cámara se encontraba situada en el lugar donde se desarrollaba la prestación laboral, enfocando directamente a la caja, y que, además, la empresa había colocado el distintivo informativo en el escaparate del establecimiento, y por lo tanto en un lugar perfectamente visible.

Por lo tanto, se pasa de exigir una información específica de la finalidad de la grabación, a una

información general de acuerdo con las exigencias de la Agencia Española de Protección de Datos, si bien se sigue exigiendo el cumplimiento del principio de proporcionalidad de la medida.

A partir de su sentencia de 3 de marzo de 2016, el TC pasa de exigir una información específica de la finalidad de la grabación, a una información general de acuerdo con las exigencias de la AEPD

Es decir, no bastará con que la información sea adecuada y acorde con la normativa vigente en materia de protección de datos, sino que es necesario además que la medida de control supere el denominado «Juicio de Proporcionalidad» tal y como se veía exigiendo hasta el momento, es decir que la medida sea idónea, necesaria, proporcional y esté justificada. Para ello, se deberá examinar previamente si la medida de video-vigilancia adoptada ha sido susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, resultaba necesaria, en el sentido de que no existiese otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); si la misma es 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), y finalmente si la medida de control se ha realizado en base a una justificación objetiva y no obedece a mero capricho y discrecionalidad empresarial (juicio de justificación).

En cualquiera de los casos, esa ausencia de necesidad u obligación de ofrecer información específica por parte de la empresa cuando ésta pretenda utilizar las cámaras de vigilancia como herramienta de control laboral para potenciales sanciones y/o despidos se ha visto ratificada recientemente por el Tribunal Supremo en diversas sentencias (SSTS 31/01/2017 y 2/02/2017).

En este sentido, el Tribunal Supremo, si bien admite la suficiencia de una información general sobre la existencia de sistemas de video vigilancia por motivos o razones de seguridad a los efectos de un posterior control laboral, clarifica qué se ha de entender por dicho concepto de «razones de seguridad», en el que incluye expresamente el control de hechos ilícitos cometidos por los trabajadores (robos, hurtos, entre otros), pero del que excluye expresamente otros tipos de control laboral relativos, por ejemplo, a la efectividad del trabajo, tales como pueden ser el control horario o de la jornada.

Así, por ejemplo, en el supuesto de hecho analizado por la STS 31/01/17 enjuicia la validez de las pruebas de video vigilancia empleadas por la empresa para justificar el despido disciplinario de un trabajador por manipular tickets y hurtar productos propiedad de la empresa. Las pruebas de dichos ilícitos fueron obtenidas por las cámaras de vigilancia que estaban instaladas en el centro de trabajo por motivos de seguridad y de cuya existencia el empleado era conocedor, aunque no fue informado expresamente de la finalidad específica que podría darse a dichas imágenes.

Teniendo en cuenta lo anterior, y la doctrina constitucional mencionada, se concluye por el Alto Tribunal que, de un lado, no será necesario el consentimiento del empleado para la captación de su imagen en el puesto de trabajo siempre que se utilice con la finalidad de dar cumplimiento al propio contrato de trabajo, en aplicación de la normativa de protección de datos, y que, una vez superado el juicio de proporcionalidad (idoneidad, necesidad, proporcionalidad y justificación), en función de las circunstancias concurrentes en cada caso, seguirá siendo válida para fines disciplinarios la utilización de las imágenes obtenidas por el sistema de video vigilancia con la mera información de la existencia del mismo a través de, por ejemplo, los carteles o indicadores que exige la normativa de protección de datos, pero siempre que la instalación se justifique por «razones de seguridad». A tal efecto, se entenderá incluido en dicho concepto de «seguridad» el control laboral que se realice sobre hechos ilícitos imputables a empleados, como puede ser robos, hurtos o manipulación de tickets de caja, excluyendo sin embargo otro tipo de control laboral «que sea ajeno a la seguridad, esto es el de la efectividad en el trabajo, las ausencias del puesto de trabajo, las conversaciones con compañeros, etc.».

Dicha dispensa del consentimiento del empleado en materia normativa de protección de datos, se refiere a los datos necesarios para el mantenimiento y cumplimiento de la relación laboral, lo

que abarca, sin duda, las obligaciones derivadas del contrato de trabajo. Por ello un tratamiento de datos dirigido al control de la relación laboral debe entenderse amparado por la excepción citada, pues está dirigido al cumplimiento de la misma. Por el contrario, el consentimiento de los trabajadores afectados sí será necesario cuando el tratamiento de datos se utilice con finalidad ajena al cumplimiento del contrato.

Como se señalaba anteriormente, aunque no sea necesario el consentimiento en los casos referidos anteriormente, el deber de información seguirá existiendo, pues este deber permite al trabajador afectado ejercer los (derechos de acceso, rectificación, cancelación y oposición y conocer la dirección del responsable del tratamiento o, en su caso, del representante.

Por tanto y, en conclusión, cabe resumir los siguientes parámetros generales en materia de videovigilancia:

- El empresario no necesitará 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, entendiendo por «razones de seguridad» el control laboral que se realice sobre hechos ilícitos imputables a empleados, como puede ser robos, hurtos o manipulación de tickets de caja, excluyendo otro tipo de control laboral «que sea ajeno a la seguridad», tales como el control horario o de jornada, ausencias del puesto de trabajo, efectividad del trabajo, entre otros aspectos.
- Esta dispensa del consentimiento del trabajador se justifica siempre que el tratamiento de datos de carácter personal sea necesario para el mantenimiento y el cumplimiento del contrato firmado por las partes.
- Aunque no sea necesario el consentimiento en los casos señalados, el deber de información sigue existiendo de acuerdo con la normativa de protección de datos para que el afectado pueda ejercer los derechos que la normativa en materia de protección de datos le reconoce.
- El deber de información se cumple con la colocación en las zonas videovigiladas, al menos un distintivo informativo ubicado en lugar suficientemente visible, tanto en espacios abiertos como cerrados, de acuerdo con los requisitos establecidos por la AEPD, de tal manera que el trabajador pueda conocer que en la empresa se ha instalado un sistema de control por videovigilancia, sin que haya que especificar, más allá de la mera vigilancia, la finalidad exacta que se le ha asignado a ese control.
- Lo importante será determinar si el dato obtenido se ha utilizado para la finalidad de control de la relación laboral o para una finalidad ajena al cumplimiento del contrato, porque sólo si la finalidad del tratamiento de datos no guarda relación directa con el mantenimiento, desarrollo o control de la relación contractual el empresario estaría obligado a solicitar el consentimiento de los trabajadores afectados
- En materia de videovigilancia, se puede concluir que el test de proporcionalidad, en atención a la doctrina jurisprudencial citada, razonablemente se superaría siempre que la medida adoptada por la empresa se encontrase oportunamente justificada, en la medida en que se fundamenta en la existencia de sospechas fundadas o prevención de ilícitos laborales; la medida fuera ponderada, en tanto en cuanto la captación de imágenes se limite a zonas concretas de trabajo (ej.: la zona de caja) y no a zonas de paso o comunes; necesaria, en la medida en que únicamente con la captación de esas imágenes se puede probar los incumplimientos laborales; y finalmente, la medida se considerará la más idónea para acreditar las irregularidades cometidas por el empleado.

De conformidad con la normativa y jurisprudencia citada deberá tenerse en consideración por parte del empresario que el tratamiento de los datos (imagen) deberá limitarse a las finalidades previstas por el Estatuto de los Trabajadores, dicho tratamiento deberá ser proporcional y sólo implementarse cuando no exista otro sistemas más idóneo y menos invasivo con la privacidad de los empleados. La captación de las imágenes deberá limitarse a los espacios estrictamente necesarios, no pudiendo implementarse en espacios vetados a la utilización de este tipo de medios como vestuarios, baños, taquillas o zonas de descanso, igualmente, no podrán ser captadas conversaciones privadas entre los empleados.

El consentimiento de los trabajadores afectados sí será necesario cuando el tratamiento de datos se utilice con finalidad ajena al cumplimiento del contrato

En este sentido, se deberá tener en cuenta determinados parámetros adicionales, como la finalidad del sistema de grabación (seguridad y/o control laboral); la permanencia o puntualidad de las grabaciones; si se trata de una actuación preventiva o derivada de sospechas por incumplimiento laboral; así como el lugar de colocación de las cámaras (puestos de trabajo o zonas comunes de paso).

Conforme a la citada Instrucción de la Agencia, deberá facilitarse un cartel informativo, así como el correspondiente aviso legal, en aquellas zonas que vayan a encontrase videovigiladas. Las imágenes deberán ser canceladas en un plazo máximo de 30 días, pudiendo conservarse bloqueadas aquellas que registren una infracción o incumplimiento de los deberes laborales de los empleados. En todo caso deberán adoptarse las medidas necesarias para garantizar la confidencialidad, integridad y seguridad de la información, evitando accesos por terceros no autorizados o su utilización con finalidades diferentes a las enunciadas. Así las cosas, los sistemas deberán ser respetuosos con los derechos a la intimidad y el a la protección de datos y garantizar el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, reconocidos en nuestra norma, con las salvedades del propio sistema de videovigilancia.

En relación con la instalación y mantenimiento de los sistemas, debe recordarse lo establecido en la Ley 5/2014, de 4 de abril, de Seguridad Privada, y firmar los correspondientes contratos de acceso a datos y normativas de confidencialidad. Debe recordarse, adicionalmente, que las imágenes obtenidas podrán ser conservadas durante un mes máximo desde su obtención, pudiendo permanecer posteriormente bloqueadas en caso de que sean utilizadas para denunciar tipos delictivos o infracciones, con la finalidad de ser aportadas, tanto a las fuerzas y cuerpos de seguridad, como al Juzgado, en caso de ser requeridas.

A mayor abundamiento, el Proyecto de Ley Orgánica de Protección de Datos, en tramitación parlamentaria, también establece condiciones concretas para los tratamientos de datos con fines de videovigilancia (*ex* art. 15), en una línea continuista con lo ya regulado y con una remisión expresa a la Ley de Seguridad Privada manteniendo, en cualquier caso, el deber de proceder a la colocación de, al menos, un distintivo informativo ubicado en un lugar lo suficientemente visible en los accesos de las zonas videovigiladas a fin de cumplir con el deber de información establecido en la norma comunitaria.

Por último, cabe mencionar que en materia de cumplimiento laboral del derecho de información de los órganos de representación legal de los trabajadores (*e.g.* delegado de persona o comité de empresa), en virtud del art. 64.5 ET, la empresa estará obligada, con carácter previo a la instalación de una sistema de videovigilancia con finalidad de control laboral, a informar a los representantes de los trabajadores a los efectos de que puedan emitir informe con carácter previo a la ejecución por parte del empresario de las decisiones adoptadas por este, sobre la implantación de sistemas de control del trabajo, tales como puede ser un sistema de videovigilancia con finalidad de control laboral.

V. Sistemas de videovigilancia oculta o secreta

Con carácter general, y de acuerdo con la doctrina anterior, no cabría, a priori, una habilitación legal expresa para permitir a la empresa omitir al trabajador el derecho a la información sobre el tratamiento de sus datos personales, como pueden ser imágenes grabadas, en el ámbito de las relaciones laborales, y «tampoco podría situarse su fundamento en el interés empresarial de controlar la actividad laboral a través de sistemas sorpresivos o no informados de tratamiento de datos que aseguren la máxima eficacia en el propósito de vigilancia» (STS 13/05/14).

Sin embargo, y específicamente en lo que se refiere a instalación de cámaras ocultas, existe una línea doctrinal de suplicación, que aplicando la tesis de la «instalación y grabación puntual

ante sospechas de incumplimiento» (STC 186/2000, de 10 de julio), está admitiendo en determinados supuestos y con límites muy específicos la validez de la prueba videográfica para acreditar la procedencia de los despidos de trabajadores, con base en las grabaciones realizadas por un sistema de cámara oculta.

La procedencia del despido, en estos casos, se justifica, según esta línea doctrinal, por consistir la prueba en grabaciones episódicas y de breve duración que se realiza «porque ya existían sospechas fundadas de que la falta de prendas y otros objetos del establecimiento mercantil que se venía observando en el cómputo obedecía a su sustracción por algún trabajador» y «[…] sería absurdo exigir a la empresa una comunicación a los trabajadores de la instalación de unas cámaras de grabación […], así como la colocación de carteles de publicidad, pues de esta forma se arruinaría con toda seguridad la finalidad buscada», tesis que, en cualquier caso, debe ser considerada como una excepción a la norma general de la necesidad de información previa.

Por lo tanto, a diferencia de la línea doctrinal general, donde resulta necesaria la información previa a todos los empleados sobre la instalación preventiva y permanente de un sistema de video-vigilancia y con una finalidad de control laboral y de cumplimiento del contrato de trabajo para que no sea necesario el consentimiento, en determinados casos de «instalación puntual y temporal de una cámara tras acreditadas razonables sospechas de incumplimientos contractuales que se emplea con la exclusiva finalidad de verificación de tales hechos», a priori, no se vería vulnerado el art. 18.1 ni el 18.4 CE (STC 186/2000) y se vería aceptada la prueba videográfica con cámara oculta.

La justificación de la utilización de un sistema oculto de videovigilancia, en aplicación de esta línea doctrinal, así como de las recomendaciones internacionales (Repertorio de Recomendaciones Prácticas de la Organización Internacional del Trabajo sobre protección de datos de los trabajadores) para la captación de incumplimientos laborales solo se admitirá si lo permite la normativa nacional (que hasta el momento no es el caso del derecho español) o bien si existen sospechas fundadas suficientes de actividad delictiva y/u otras infracciones graves por parte de los empleados

Existe una línea doctrinal de suplicación, que está admitiendo en determinados supuestos y con límites muy específicos la validez de la prueba videográfica obtenida a través de un sistema de cámara oculta

En lo que respecta a nuestro ordenamiento jurídico *de lege ferenda*, cabe mencionar el art. 22.5 del Proyecto de Ley de Protección de Datos de Carácter Personal establece que: «en el supuesto de que las imágenes hayan captado la comisión flagrante de un acto delictivo, la ausencia de la información a la que se refiere el apartado anterior no privará de valor probatorio a las imágenes, sin perjuicio de las responsabilidades que pudieran derivarse de dicha ausencia», lo que validaría normativamente el supuesto de cámara oculta en el ámbito laboral sin perjuicio de las posibles sanciones administrativas que se pudieran imponer a la empresa por esa falta de información.

Y en lo que respecta a las «sospechas fundadas» que pudiera tener la empresa, para que entre en juego el principio de proporcionalidad, no será suficiente la mera afirmación de que existían sospechas fundadas de estar el trabajador cometiendo una infracción grave, sin explicar y concretar (en la carta de despido) cuáles eran esas precisas sospechas.

No obstante, lo anterior, y como consecuencia de la excepcionalidad de la utilización de este sistema de cámara oculta, se requiere una prueba extraordinaria a la empresa para justificar su utilización. Alguno de los parámetros tenidos en cuenta por la jurisprudencia en la casuística analizada de cámara oculta son los siguientes:

- Instalación de cámara oculta de forma puntual y temporal ante sospechas razonables de robos de un miembro del comité. Información previa al presidente del Comité. Supuesto de sospechas de hurtos no de una persona en concreto, sino en general del personal interno. Instalación de la cámara enfocando puntos concretos, en este caso, a los armarios donde se

guardaba el producto y otros cuatro puestos de trabajo donde se sospechaba que se estaban produciendo las irregularidades, durante 5 días de grabación. En este caso, ante la posible frustración de avisar con carteles o distintivos, el Tribunal consideró admisible «la sustitución de la información a los trabajadores por la efectuada al presidente del comité de empresa» (STSJ Madrid 9-2-2015).

- Calidad de las «sospechas razonables». Será necesario que las sospechas razonables o fundadas respondan a hechos concretos que permitan concluir, de forma indiciaria pero razonable, que se puede estar cometiendo una infracción de gravedad, y especialmente de que el responsable de esa infracción es seguramente el trabajador concreto investigado. Así, por ejemplo, se entenderán sospechas fundadas casos en los que se producen descuadres de inventario o quejas de clientes por faltarles productos en los envíos, cuyas fechas vengan a coincidir habitualmente con los días en los que el trabajador investigado prestaba servicios (STSJ Canarias 27-3-17).

- Test constitucional de proporcionalidad: la instalación de cámaras ocultas que controlaban la zona de trabajo (centro de control de exteriores y accesos) donde el trabajador demandante desempeñaba su actividad laboral era una medida justificada (ya que se habían denunciado robos de cables y materiales, aunque la denuncia se refiriera, obviamente, a periodo anterior, respecto del que era imposible obtener imágenes del centro de control por no haberse colocado antes en él cámara de videovigilancia); idónea para la finalidad pretendida por la empresa (evitar o prevenir futuros robos y verificar si algunos trabajadores, aunque fueran otros distintos de los que había antes en ese servicio, cometían irregularidades que los posibilitaran y, en tal caso, adoptar las medidas disciplinarias correspondientes); necesaria (ya que la grabación serviría de prueba de tales irregularidades, siendo, además, la única posible y útil —no lo serían, por ejemplo, aleatorias y temporales visitas de inspección—); y equilibrada (pues la grabación de imágenes se limitó al centro de control que era el lugar de trabajo) (STSJ Comunidad Valenciana 13-10-17). En el mismo sentido la STSJ Andalucía 13-6-2016.

- Doble sistema de vigilancia, visible por motivos de seguridad y oculta por sospecha de robos de cobre por empleados cobre por un vigilante de seguridad (Caso Securitas Seguridad). Aun sin haber informado previamente al propio trabajador sospechoso ni a los representantes de los trabajadores. De la grabación se detecta que el vigilante se quedada dormido en sus turnos. Se aplica el test de proporcionalidad de la STC 186/2000 (supuesto de cámara oculta) que se encontraría justificada cuando existen serias sospechas de las irregularidades cometidas por el trabajador, porque tal medida: 1) es idónea para el fin perseguido; 2) es necesaria al no existir otra vía de actuación menos fuerte; 3) es equilibrada o proporcionada al limitarse al lugar y tiempo imprescindibles para comprobar el comportamiento inadecuado del empleado sospechoso y la concurrencia de «irregularidades» denunciadas por el cliente de la empresa (entre 2 y 4 semanas de grabación). Los hechos que determinaron la proporcionalidad fueron: a) limitado la instalación de la cámara oculta temporalmente al periodo necesario para verificar el modo de prestación del servicio de vigilancia; b) siendo retirada cuando se realizaron las oportunas comprobaciones, y c) además, se limitó al lugar en el que el trabajador prestaba el servicio nocturno de vigilancia (STSJ Comunidad Valenciana 30-12-2016 y en igual sentido STSJ Andalucía 22-2-2017).

- Doble sistema, visible y oculto, sin cartel de la Agencia Española de Protección de Datos, pero con Nota informativa de la existencia de un sistema de videovigilancia con finalidad, entre otras, de control laboral tanto a los empleados como a los representantes de los trabajadores (Caso Campsa). Despido por hurtos y otras irregularidades (consumir estupefacientes en horas de trabajo, permitir el acceso a la oficina a personas ajenas a la empresa, etc.) a raíz de las grabaciones de la cámara oculta en la oficina de la estación de servicios. No nulidad del despido con base en: a) proporcionalidad de la grabación (idónea, necesaria, equilibrada, al colocarse en la oficina donde habitualmente se encontraba el trabajador); b) existencia de información previa de la existencia de cámaras para control laboral, no siendo relevante la información sobre la ubicación de las cámaras, existiendo además en la misma zona (oficina) una cámara visible y otra oculta (STSJ País Vasco 6-10-2015).

- Falta de necesidad e idoneidad de la instalación de la cámara (caso clínica esterilización).

Nulidad de la prueba de grabación oculta en la zona de esterilización que grabó irregularidades de la empleada, al existir, según el Tribunal, informes de «trazabilidad de las incidencias» del material procesado, de modo que la empresa podía identificar al personal que interviene cuando se detecta una incidencia (STSJ Cataluña 9-3-2017).

- Aplicación doctrina overruling STC 39/2016. Contenido del derecho de información previa. Diferenciación videovigilancia Vs. grabación detective. Cámara oculta. Si bien se declara la nulidad de la prueba por la ausencia de sospechas razonables, se concreta, en atención a la doctrina constitucional y normativa de protección de datos, qué comprende el derecho de información previa, el cual se puede cumplir de diversas maneras para garantizar el derecho del trabajador: a) existencia de información sobre zona videovigilada en un espacio físico concreto (no necesariamente visible) (también STSJ Comunidad Valenciana 7-9-2016); b) no es necesaria la información sobre la concreta ubicación de las cámaras y «mucho menos especificar en la información que las cámaras se instalan precisamente para controlar la actividad de un concreto trabajador respecto del cual concurren sospechas de comportamientos ilícitos»; c) información, no al trabajador, pero si a los representantes legales (STSJ Canarias 20-6-2017).

En atención a la jurisprudencia anterior, cabe extraer varias conclusiones en relación con la validez o licitud de la instalación de un sistema de cámara oculta para probar irregularidades o ilícitos laborales, partiendo del supuesto de hecho de instalación puntual y temporal de una cámara tras acreditadas razonables sospechas de incumplimientos contractuales se emplea con la exclusiva finalidad de verificación de tales hechos.

- Sin perjuicio de que haya previamente o no instalado otro sistema de videovigilancia visible con carácter preventivo.
- Con carácter general, no es necesario 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 (consentimiento implícito en la propia aceptación del contrato que implica reconocimiento del poder de dirección del empresario.
- Si es necesario el cumplimiento del deber de información previa.
- Ante la evidente frustración que puede plantear el aviso previo al trabajador/es sospechosos, se admite otras fórmulas alternativas de información previa: al comité de empresa o al presidente del comité; con carteles distintivos de zona videovigilada sin necesidad de informar sobre la ubicación de las cámaras, que pueden ser visibles o no; con notas informativas a todos los empleados informando de la existencia de sistema de videovigilancia con finalidad de seguridad y control laboral, etc.
- La relevancia constitucional de la ausencia o deficiencia de información en los supuestos de videovigilancia laboral exige la consiguiente ponderación en cada caso concreto de los derechos y bienes constitucionales en conflicto, es decir la superación del test de proporcionalidad (medida justificada, idónea, necesaria y equilibrada).

De cara a evaluar los indicios de la proporcionalidad de la medida debían tenerse en consideración que: (i) fuera una medida justificada: sospechas razonables. No se puede considerar suficiente una mera afirmación apodíctica de que existían sospechas fundadas de estar el trabajador cometiendo una infracción grave, sin explicar cuáles eran esas precisas sospechas o hechos concretos, tales como robos, hurtos, apropiaciones indebidas de productos concretos, descuadres de caja, etc. Las sospechas se pueden tener de forma individualizada o bien en relación con un puesto de trabajo en concreto donde operan varios trabajadores (ii) medida idónea y necesaria: si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad) y 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). Si la instalación de cámara oculta sirve para verificar si el trabajador —cuál o cuáles de los trabajadores— cometía efectivamente las irregularidades sospechadas y en tal caso adoptar las medidas disciplinarias correspondientes, y las grabaciones sirven de prueba de tales irregularidades, sin que haya otros medios posibles para dicha verificación, se entendería cumplido el requisito constitucional. Sin embargo, si existen otros medios, tales como informes de trazabilidad en los que puedan constar y

acreditar tanto el empleado como la infracción cometida, se podría considerar la medida no necesaria o idónea y (iii) que la medida fuese proporcional o equilibrada: la ubicación de la cámara (enfocando directamente el/los puesto/s de trabajo donde se sospeche que se están produciendo las irregularidades, tales como las líneas de caja, despensa, armarios o dispensarios donde se guardan los productos, etc., o la ubicación física donde se encuentre habitualmente el empleado sospechoso, como por ejemplo una oficina, despacho, pasillo concreto que lleva a una dependencia, salidas y entradas, cocina, etc.); la duración de las grabaciones (entre 4-5 días y dos semanas) breves y episódicas; instalación por una empresa especializada con verificación e informe; eliminando días o imágenes donde aparezcan otros empleados o situaciones irrelevantes para la investigación; son todos ellos indicios de proporcionalidad o equilibrio en el tratamiento de las imágenes obtenidas.

No obstante, en este punto, por su relevancia, debe recordarse la Sentencia del Tribunal Europeo de Derechos Humanos (TEDH) de 9 de enero de 2018. Asunto López Ribalda y otras contra España. En este caso, el TEDH enjuicia un asunto de videovigilancia oculta de los empleados del Cliente ante unas sospechas previas de robo.

El supuesto de hecho enjuiciado consistió en que la empresa instaló un sistema de cámaras visibles y otro de cámaras ocultas, informando a las trabajadoras de la instalación de las cámaras visibles, pero no sobre la presencia de cámaras ocultas, desconociendo las trabajadoras que estaban siendo grabadas.

Las empleadas sospechosas de robo fueron convocadas a unas entrevistas individuales en las que se les exhibieron los videos que mostraban a las demandantes ayudando a clientes y colegas a robar artículos y robando ellas mismas. Las demandantes reconocieron los hechos fueron despedidas por motivos disciplinarios entre los días 25 y 29 de junio de 2009.

Tres de las cinco demandantes suscribieron un acuerdo extrajudicial en el que reconocían su participación en los robos y renunciaron a impugnar su despido ante la jurisdicción social y la empresa se comprometió, a su vez, a no iniciar un procedimiento penal. Sin embargo, todas las demandantes, tanto las que firmaron el acuerdo como las que no lo hicieron, terminaron por acudir a los tribunales.

Los despidos fueron confirmados en primera instancia por la jurisdicción social y posteriormente en apelación por el Tribunal Superior de Justicia, admitiendo las grabaciones de video como elemento de prueba, considerando que habían sido obtenidas legalmente. Las solicitudes ante el TEDH se presentaron por las demandantes entre el 28 de diciembre de 2012 y enero de 2013.

El Tribunal concluye en particular que, en virtud de la legislación española sobre protección de datos personales, hubiera sido necesario informar a las demandantes que estaban siendo sometidas a vigilancia y que dicha obligación de información previa se omitió.

Asimismo, el Alto Tribunal considera que existían otros medios de proteger los derechos de la empresa y que este hubiera podido, como mínimo, comunicar a las demandantes una información general en relación con la vigilancia a las que se le había sometido, censurando a las jurisdicciones nacionales por no mantener un justo equilibrio entre el derecho de las demandantes al respeto de su vida privada y los derechos patrimoniales de la empresa.

Sin perjuicio de lo anterior, el Tribunal concluye que en cualquier caso el procedimiento en su conjunto ha sido equitativo ya que las grabaciones de video no constituyeron el único elemento de prueba en el que se apoyaron los jueces españoles para confirmar las decisiones de despido y las demandantes tuvieron la posibilidad de oponerse a las grabaciones ante los tribunales.

Si bien la actual normativa española, laboral o protección de datos, no recogen expresamente la posibilidad de la empresa de poder utilizar sistemas de grabación ocultas o secretas sin necesidad de información previa a los trabajadores para ejercer su derecho al control de la actividad laboral de los empleados, más allá de la previsión general contenida en el art. 20.3 ET (adopción de las medidas «más oportunas» para la vigilancia y el control laboral) sí que encontramos en el Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal, en fase parlamentaria, dicha referencia.

Así, el apartado quinto del art. 22 del mencionado Proyecto

El Proyecto de LOPD incluye la referencia a esta posibilidad de la empresa de utilizar sistemas de grabación ocultas o secretas sin necesidad de información previa a los trabajadores

dispone que: «Los empleadores podrán tratar los datos obtenidos a través de sistemas de cámaras o videocámaras para el ejercicio de las funciones de control de los trabajadores previstas en el art. 20.3 del Estatuto de los Trabajadores, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo. Los empleadores habrán de informar a los trabajadores acerca de esta medida. En el supuesto de que las imágenes hayan captado la comisión flagrante de un acto delictivo, la ausencia de la información a la que se refiere el apartado anterior no privará de valor probatorio a las imágenes, sin perjuicio de las responsabilidades que pudieran derivarse de dicha ausencia».

El Legislador con esta previsión parece querer dejar abierta la posibilidad de la utilización de sistemas secretos de videovigilancia sin necesidad de información previa, pero siempre que obedezca a sospechas de la comisión de actos delictivos y así fueran captados por las cámaras instaladas, otorgándose valor probatorio a dichas imágenes y sin perjuicio de las posibles sanciones administrativas que de dicha ausencia informativa se pudieran derivar.

De otro lado, por «actos delictivos» se debe entender, al menos en opinión del que suscribe la presente Nota, actos susceptibles de reproche penal, tales como robos, hurtos o cualquier otro que pudiera ser objeto de alguna sanción en el orden penal, excluyéndose meros ilícitos laborales.

VI. Geolocalización

Uno de los sistemas más utilizados para el control laboral es la localización exacta del empleado en todo momento, durante su jornada laboral, sobre todo en puestos de trabajo desarrollados fuera del centro de trabajo, como es el caso de comerciales o vigilantes de seguridad.

La localización por satélite, o geolocalización, permite a la empresa saber la posición exacta del empleado, y por lo tanto controlar la prestación de servicios en el horario y lugar fijados previamente, utilizando para ello sistemas incorporados a dispositivos móviles, GPS en vehículos y ahora también mediante microchips insertados en tarjetas identificativas o incluso implantados bajo la propia piel del empleado.

Indudablemente, la cuestión a resolver en estos casos, es la determinación de los requisitos que se exigen para la instalación por la empresa de sistemas de vigilancia que permitan la geolocalización de los empleados salvaguardando los derechos fundamentales a la intimidad y a la protección de sus datos personales.

Así las cosas, en relación a la implantación de los sistemas de geolocalización, aunque no es requisito imprescindible recabar el consentimiento de los trabajadores, sí es exigible informar previamente a la implantación de la medida, conforme a lo establecido por el art. 5 LOPD, a saber, indicar la existencia de la medida de control de geolocalización que va a adoptar la empresa y a partir de qué fecha; señalar que la misma permite obtener información acerca de la situación geográfica de los trabajadores, exclusivamente durante la jornada laboral; que los datos recogidos con ocasión del citado sistema de geolocalización va a pasar a formar parte del Fichero de Personal de la empresa con la finalidad de gestionar la relación laboral existente, indicando si van a ser cedidos o no a terceros; y finalmente recordando que el trabajador tiene derecho a acceder, rectificar o cancelar los datos referentes a su persona incluidos en ese fichero.

A mayor abundamiento, el Grupo de Trabajo del art. 29, en su Dictamen 13/2011 sobre los servicios de geolocalización en los dispositivos móviles inteligentes, recordaba, entre otros aspectos, que, «el empresario debe siempre buscar los medios menos intrusivos, evitar un seguimiento continuo y, por ejemplo, elegir un sistema que envíe una alerta cuando un empleado cruce una frontera virtual preestablecida. El empleado deberá poder desactivar cualquier dispositivo de vigilancia fuera de las horas de trabajo y deberá instruírsele sobre cómo hacerlo».

En el mismo sentido, se han pronunciado tanto el Tribunal Constitucional (STC 292/2000, entre

otras) como la jurisprudencia de suplicación (STSJ Castilla la Mancha de 23/03/2015, en un caso de videovigilancia por GPS), declarando la licitud de estos sistemas siempre que medie información previa a los trabajadores de su instalación, y de la finalidad que con la misma se persigue.

En nuestra opinión, valoración a parte requiere el sistema de implantación de microchips bajo la piel del propio empleado, ya que, en estos casos, podríamos estar ante una medida desproporcionada y excesiva, no bastando la mera información previa, ya que existen otras medidas menos intrusivas con las que alcanzar el objetivo del control laboral. Es más, incluso en el caso de existir consentimiento, podría declararse nula la cláusula contractual que obligase al trabajador a implantarse un dispositivo de esta naturaleza, aplicando la reciente doctrina del Tribunal Supremo del acceso al trabajo como un «bien escaso». Según esta nueva línea jurisprudencial el consentimiento del trabajador, entendido como la parte más débil del contrato, no sería del todo libre en una situación de crisis económica como la que vivimos, invalidando la voluntad de obligarse a facilitar ciertos datos personales no necesarios para el cumplimiento del contrato de trabajo (STS 21/09/2015).

VII. Epílogo

Sin duda, estamos asistiendo a los albores de una verdadera revolución digital que afecta también, como hemos visto, a la sofisticación tecnológica de los nuevos sistemas de control y vigilancia empresarial del cumplimiento laboral de sus empleados. Una revolución que conlleva la aparición de nuevas formas de desarrollar las funciones laborales, como el teletrabajo o la implementación de políticas «bring your own device», y que necesariamente implica un avance jurídico adaptado a los nuevos tiempos, tecnologías e idiosincrasias de las propias empresas, lo que, unido al momento de profundo cambio en Europa en relación con la próxima aprobación del Reglamento General de protección de datos, aboca el avance tecnológico a la adopción de medidas y garantías por parte del empresario, que salvaguarden la esfera íntima del empleado y sus derechos constitucionalmente reconocidos, tal y como hemos analizado. En todo caso estaremos pendientes de las nuevas fórmulas de vigilancia que se introduzcan en el mercado, así como de los límites jurisprudenciales que se vayan estableciendo a raíz de esta novedosa realidad y el impacto que el Reglamento General de Protección de Datos, así como su aplicación pueda tener sobre los mismos.