

COLISIÓN DE LOS DERECHOS DEL ARTÍCULO 18 CE CON LOS MÉTODOS MODERNOS DE CONTROL EMPRESARIAL: ESPECIAL REFERENCIA A LA JURISPRUDENCIA. COMPARACIÓN CON EL DERECHO FRANCÉS Y EL DERECHO ALEMÁN

EDUARDO ENRIQUE TALENS VISCONTI
PEDRO CHAPARRO MATAMOROS

*Estudiantes de ADE-Derecho.
Universidad de Valencia*

Este trabajo ha sido seleccionado para su publicación por: don Luis Enrique DE LA VILLA GIL, doña Teresa Díez MERIEL, don Ignacio GARCÍA-PERROTE ESCARTÍN, don Eugenio LANZADERA ARENCIBIA, doña Lourdes LÓPEZ CUMBRE y doña Rosa María VIROLÉS PIÑOL.

Extracto:

EN las siguientes páginas se abordará el problema de la efectividad de los derechos del artículo 18 CE en el ámbito laboral. Estos derechos de carácter personalísimo ostentan la protección constitucional, formando parte del grupo de los llamados derechos fundamentales. Precisamente, su configuración como derechos fundamentales hace que requieran una atención e importancia capital. Existiendo diversos tipos de injerencias que pueden conculcar los referidos derechos, nos centraremos principalmente en la concreta violación de los mismos que resulta de la instalación de videocámaras y sistemas de microfonía ocultos, así como en la originada por el control de las aplicaciones informáticas (correo electrónico, MSN Messenger, etc.).

Adelantaremos ahora que el establecimiento de videocámaras puede ocasionar injerencias tanto en el derecho a la intimidad como en el derecho a la propia imagen. Por su parte, la grabación de la voz emitida por el trabajador únicamente constituirá intromisión en el derecho a la intimidad, no así, como resulta evidente, en el derecho a la propia imagen. No obstante, es también frecuente la combinación de ambas medidas; así, no se habla tanto de videovigilancia o de reproducción por microfonía de la voz del trabajador, sino de captaciones audiovisuales. De otro lado, nuestro otro foco de atención, esto es, la fiscalización de los medios informáticos puestos a disposición del trabajador, causa también intromisiones en la intimidad (en ningún caso en la propia imagen), si bien colisiona en mayor medida con otro de los derechos contemplados en el artículo 18 CE, el derecho al secreto de las comunicaciones. A continuación, se hará una explicación y delimitación de estos derechos en base a la prolija jurisprudencia constitucional antes de entrar de lleno en el meollo de la cuestión.

Palabras clave: artículo 18 CE, control ilícito, captaciones audiovisuales, correo electrónico y derecho comparado.

Sumario

I. Parte general.

1. Derechos del artículo 18 CE.
2. Esfera privada del trabajador: estado de la cuestión.
3. Obligaciones del empresario en relación con los representantes de los trabajadores.
4. Aproximación a los métodos modernos de vigilancia y control.

II. Captaciones audiovisuales.

5. Captaciones audiovisuales.

III. Aplicaciones informáticas.

6. Uso desviado de las aplicaciones informáticas (correo electrónico) y su control por el empresario.

IV. Consecuencias del control ilícito.

7. Consecuencias derivadas para el empresario del control ilícito.
8. Interdicción procesal de las pruebas obtenidas de modo ilícito.

V. Derecho comparado.

9. Derecho comparado.

I. PARTE GENERAL

1. Derechos del artículo 18 CE.

El artículo 18 CE proclama, en lo que aquí nos interesa, lo siguiente:

«1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.

...

3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial».

En primer lugar, procede explicar estos derechos desde la perspectiva civilista. En este sentido, los derechos del artículo 18.1 CE forman parte de los llamados derechos de la personalidad en el ámbito civil. Se entiende en esta sede la intimidad como el derecho a mantener una esfera propia reservada, siendo esta protegida ante intromisiones ajenas, así como el derecho a impedir la divulgación de datos que pertenezcan a esta esfera. Por su parte, la propia imagen consiste en impedir o consentir acerca de la reproducción de la imagen de la persona por cualquier medio. Estos derechos son inalienables, en tanto en cuanto no pueden ser transmitidos a otras personas, e irrenunciables. De otro lado, se trata de dos derechos cuyo titular es la persona individualmente considerada, a quien corresponde el ejercicio de los mismos. Ahora bien, esto se debe exceptuar en el caso de la protección *post mortem*, donde es posible ejercer acciones cuando una persona ha fallecido sin haber podido ejercitar sus acciones de protección o cuando las intromisiones se realizan una vez muerta aquella ¹.

La validez de una intromisión queda otorgada con la autorización expresa por ley o por el consentimiento expreso del titular del derecho, como se dispone en el artículo 2.2 de la Ley Orgánica 1/1982, de protección civil de derechos del artículo 18.1 CE. Asimismo, el consentimiento es revocable en cualquier momento, pudiendo conllevar indemnización «los perjuicios causados y las expectativas justificadas». Las vías para poder acceder a la tutela de estos derechos son la penal (en el caso de intromisiones tipificadas como delito, como la calumnia) y la civil. La tutela judicial debe adoptar las medidas necesarias para conseguir el cese de la intromisión, así como ordenar la indemnización, en su caso, del daño causado por aquella.

¹ DÍEZ-PICAZO Y PONCE DE LEÓN, LUIS y GULLÓN BALLESTEROS, ANTONIO: *Sistema de derecho civil (vol. I): Introducción. Derecho de la persona. Autonomía Privada. Persona jurídica*, Madrid, Editorial Tecnos, 2005, págs. 344-346.

Centrándonos ya en la perspectiva constitucional, los derechos aludidos están ubicados dentro del grupo de los derechos fundamentales, aquellos que gozan de una posición privilegiada en nuestro entramado constitucional y, asimismo, ostentan una protección exorbitante. No obstante, todo derecho fundamental puede ser sometido a ciertos límites, siempre que estos sean necesarios, idóneos y proporcionales, sin que quede afectado en ningún caso el contenido esencial del mismo. De lo que resulta que, a pesar de su configuración como fundamentales, estos derechos no tendrán prioridad en todos los casos, sino que los operadores jurídicos deberán ponderar los intereses y derechos en conflicto antes de decantarse por su preponderancia o sumisión a otro derecho, interés o fin (en este caso, el interés del empresario). La Ley Orgánica 1/1982 citada anteriormente es la que desarrolla estos derechos fundamentales de intimidad y propia imagen (junto al del honor, derecho no susceptible de ser violado en los supuestos que explicaremos y que, por tanto, no será comentado).

A pesar de la confusión inicial sobre su aparente superposición, el TC ha proclamado la autonomía del derecho a la propia imagen respecto del derecho al honor y, en especial, respecto del derecho a la intimidad, con el que la conexión que guarda resulta más evidente ². La STC 81/2001 define y delimita el derecho a la propia imagen. En esta sentencia se establece que «lo específico del derecho a la propia imagen es la protección frente a las reproducciones de la misma, que afectando a la esfera personal, no lesionan su buen nombre ni dan a conocer su vida íntima. El derecho a la propia imagen pretende salvaguardar un ámbito propio y reservado, pero no íntimo». Por tanto, es un derecho subjetivo que protege ante la mera reproducción de la imagen por medio de un dibujo, caricatura, foto, etc. Cabe precisar aquí que una reproducción de la imagen con una cámara puede llevar aparejada una violación de la intimidad. De lo que se sigue que, a pesar de ser derechos diferentes, pueden aparecer vinculados ante una misma injerencia.

Por otro lado, la STC 115/2000 define de manera concisa y clara el derecho a la intimidad, al establecer que este «tiene por objeto garantizar al individuo un ámbito reservado de su vida, vinculado con el respeto de su dignidad como persona (art. 10.1 CE), frente a la acción y el conocimiento de los demás, sean estos poderes públicos o simples particulares». En este sentido, añade el tribunal que «lo que el artículo 18.1 CE garantiza es, pues, el secreto sobre nuestra propia esfera de intimidad, y por tanto, veda que sean los terceros, particulares o poderes públicos, quienes decidan cuáles son los lindes de nuestra vida privada». Ergo queda en manos de cada individuo decidir reservarse un espacio más o menos amplio de intimidad.

En cuanto al tercer derecho fundamental en juego en los casos de control empresarial, cabe decir que el TC ha precisado el concepto de secreto de las comunicaciones en sus SSTC 114/1984 y 34/1996, entendiéndolo que «tiene un carácter formal, en el sentido de que se predica de lo comunicado, sea cual sea su contenido y pertenezca o no el objeto de la comunicación misma al ámbito de lo personal, lo íntimo o lo reservado». Además, habla el TC en el mismo lugar de «la presunción *iuris et de iure* de que lo comunicado es "secreto" en sentido sustancial». Así, secreto en sentido objetivo y con base en la cobertura técnica que le proporciona el canal cerrado.

² DE VERDA y BEAMONTE, José Ramón y otros: *Veinticinco años de Aplicación de la Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen*, Editorial Aranzadi, 2007, págs. 217-218.

Las SSTC 70/2002 y 123/2002 han añadido que debe considerarse secreto de las comunicaciones «cualquiera que sea la técnica de transmisión utilizada», con independencia del contenido del mensaje «conversaciones, informaciones, datos, imágenes, votos, etc.»³.

2. Esfera privada del trabajador: estado de la cuestión.

Una de las más importantes (y problemáticas) manifestaciones de los derechos a la intimidad y a la propia imagen se produce en el ámbito de las relaciones de carácter laboral. Consagrados en el artículo 38 CE los poderes de dirección del empresario como parte del contenido esencial de la libertad de empresa, el reconocimiento de los derechos aquí estudiados al trabajador actúa como límite a las facultades discrecionales del empresario, produciéndose pues un choque frontal entre derechos fundamentales. En este sentido, ha advertido GOÑI SEIN (acertadamente a nuestro juicio) que «la situación de subordinación que caracteriza la relación de trabajo no puede explicarse en manifestaciones de ejercicio del poder empresarial que lesionan instancias irreductibles de libertad o intimidad»⁴.

Desafortunadamente, la cuestión de la protección de los derechos a la intimidad, a la propia imagen y al secreto de las comunicaciones en el ámbito laboral ha sido olvidada en cierta medida por el legislador español. De un lado, no existe una ley que regule expresamente el tratamiento que se ha de dar a los datos obtenidos por el empleo de videocámaras y otros métodos de vigilancia (entre ellos la «cibervigilancia»). Por otra parte, tampoco existe en el Estatuto de los Trabajadores (ET) una regulación específica sobre el ejercicio del derecho a la propia imagen en la relación de trabajo, si bien este derecho parece encontrarse implícito en el artículo 4.2 e) de dicha ley (modificado primeramente por el art. 37.2 de la Ley 62/2003 y que ostenta su redacción actual a tenor de la modificación realizada por la Ley Orgánica 3/2007, en su disp. adic. undécima, apartado primero)⁵, al pergeñar este que «en la relación de trabajo, los trabajadores tienen derecho [...] al respeto de su intimidad y a la consideración debida a su dignidad...». Del mismo modo, el artículo 8.11 de la LISOS califica como infracciones muy graves «los actos del empresario que fueren contrarios al respeto de la intimidad y consideración debida a la dignidad de los trabajadores».

En cuanto a la protección de estos derechos brindada por la citada Ley 1/1982, hay que tener en cuenta, en lo que aquí interesa, que el artículo 7, en relación con el artículo 2, considera intromisiones ilegítimas en el derecho a la intimidad, entre otras «el emplazamiento en cualquier lugar de aparatos de escucha, de filmación, de dispositivos ópticos o de cualquier otro medio apto para grabar o reproducir la vida íntima de las personas» y «la utilización de aparatos de escucha, dispositivos ópticos, o de cualquier otro medio para el conocimiento de la vida íntima de las personas o de manifestaciones o cartas privadas no destinadas a quien haga uso de tales medios, así como su grabación, registro o reproducción».

³ COTINO HUESO, Lorenzo: *Derecho constitucional II. Derechos fundamentales*, Valencia, Publicaciones Universidad de Valencia (PUV), 2007, pág. 230

⁴ GOÑI SEIN, José Luis: *El respeto a la esfera privada del trabajador*, Madrid, Editorial Civitas, 1988, pág. 21.

⁵ DE VERDA Y BEAMONTE, José Ramón y otros: *Veinticinco años de Aplicación...*, pág. 220.

En ocasiones, el empresario (al fin y al cabo el sujeto más interesado en el devenir del negocio, en tanto en cuanto pone los medios de producción y el capital necesario para el desarrollo de la actividad) siente curiosidad (y sospechas) acerca del rendimiento de sus trabajadores, rendimiento que puede ser evaluado de distintas maneras. Desde estas líneas, proponemos diversos métodos, todos ellos con cabida constitucional, como inspecciones rutinarias o controles sistemáticos. También puede realizar controles *a priori*, antes de la contratación, evaluando por medio de tests y pruebas psicotécnicas las capacidades del trabajador y, en definitiva, su adecuación al puesto solicitado. Sin embargo, y a pesar de las múltiples formas de evaluación del rendimiento, la práctica ha puesto de manifiesto que para el empresario resulta mucho más atractiva la vigilancia, el control *stricto sensu* de la actividad del asalariado, e, incluso, por qué no decirlo así, el espionaje, métodos que no siempre gozan de la protección constitucional por invadir la esfera privada del trabajador. De ahora en adelante nuestra función será explicar los métodos modernos de control (principalmente captaciones audiovisuales) y deslindar, en base a la jurisprudencia más reciente, aquellos supuestos que infringen los derechos a la intimidad y a la propia imagen de los que no lo hacen.

3. Obligaciones del empresario en relación con los representantes de los trabajadores.

Es habitual que los distintos ordenamientos jurídicos contengan alguna norma que haga referencia a la obligación del empresario de poner en conocimiento de los representantes de los trabajadores las medidas a implantar, previamente a la ejecución de estas, a fin de que aquellos tengan algo que decir, vinculante o no, en defensa de los intereses de sus representados.

Así, en el panorama normativo europeo encontramos algunas disposiciones que tratan el tema de la comunicación de las medidas a los representantes de los trabajadores. En este sentido, la Recomendación del Consejo de Europa número R (89) 2 dispone en su artículo 3 que los empleadores deben informar o consultar a los empleados o a sus representantes antes de introducir un cambio en los sistemas automatizados para la recogida y utilización de datos. Además, se aplica también al cambio de los procesos técnicos destinados al control de la productividad y de los movimientos de los trabajadores. El apartado segundo de este mismo artículo continúa diciendo que «debería buscarse el acuerdo con los trabajadores o sus representantes antes de la introducción o la modificación de tales sistemas o procesos cuando [...] revele una posibilidad de atentado al respeto de la vida privada y a la dignidad humana de los trabajadores, a menos que se prevean otras garantías en la legislación o en la práctica nacional». Igualmente, la Organización Internacional del Trabajo, en el apartado octavo del artículo 5 del Repertorio de recomendaciones que ha elaborado sobre la protección de los datos personales de los trabajadores, establece que «los trabajadores y sus representantes deberían ser informados de toda actividad de acopio de datos, de las reglas que la gobiernan y de sus derechos». Por su parte, el artículo 12, que versa sobre derechos colectivos, va más allá y dispone que los representantes deberán ser informados sobre la instalación y modificación de sistemas automatizados que traten datos personales de los trabajadores y antes de que se instalen sistemas de videovigilancia del comportamiento de los trabajadores en el lugar de trabajo ⁶.

⁶ THIBAUT ARANDA, Javier: «El papel de los representantes de los trabajadores», *Revista Aranzadi de Derecho y Nuevas Tecnologías*, número 1, 2003, 357-375, págs. 359-360.

En el derecho español la necesidad del deber de previa información a los trabajadores o sus representantes y la valoración por parte de los tribunales es un tanto laxa. *A sensu contrario*, en el derecho francés el deber de información opera de una manera más taxativa e incluso en ocasiones casi como el único elemento que sirve como objeto de debate (más adelante se entrará con más detalle en la diferencia de tratamiento entre los tribunales españoles y franceses). La norma española en la materia es el artículo 64 ET, recientemente modificado por la Ley 38/2007, de 16 de noviembre, que impone al empresario diferentes obligaciones respecto del comité de empresa en relación a la adopción de medidas de vigilancia de los empleados. En primer lugar, el artículo 64.1 del ET dispone que «el comité de empresa tendrá derecho a ser informado y consultado por el empresario sobre aquellas cuestiones que puedan afectar a los trabajadores». Por su parte, el apartado f) del tercer párrafo del artículo 64.5 preceptúa que «el comité de empresa tendrá derecho a emitir informe, con carácter previo a la ejecución por parte del empresario de las decisiones adoptadas por este, sobre [...] la implantación y revisión de sistemas de organización y control del trabajo, estudios de tiempos, establecimiento de sistemas de primas e incentivos y valoración de puestos de trabajo». Tras la lectura de este artículo se puede decir que el informe previo en el que se valore la medida a adoptar es simplemente facultativo («tendrá derecho»), si bien, como es lógico, en la práctica el informe deriva en preceptivo dado el interés del comité de empresa en defender de la mejor manera posible los intereses de los trabajadores. De otro lado, el informe no es vinculante para el empresario.

Aparentemente, de estos imperativos legales se deduce que el traslado al comité de empresa de toda intención de adoptar medidas de control de los trabajadores opera como una condición *sine qua non* en orden a que la medida sea considerada legítima. No obstante, la práctica de los tribunales ha venido suavizando estos requisitos, al entender que la puesta en conocimiento de los trabajadores de las eventuales medidas de vigilancia podría frustrar la finalidad del empresario, que no es otra sino detectar irregularidades en el desempeño del puesto de trabajo. De suerte que la jurisprudencia ha venido permitiendo el incumplimiento de las obligaciones contenidas en los preceptos citados en determinados supuestos en que se antojaba necesario el desconocimiento del trabajador de la eventual medida de control. Así, la sentencia más importante en la materia, la STC 186/2000, vino a admitir la falta de comunicación a los representantes e incluso al propio trabajador afectado, «sin duda por el justificado temor de la empresa de que el conocimiento de la existencia del sistema de filmación frustraría la finalidad apetecida». Esta doctrina ha sido reproducida por los diferentes Tribunales Superiores de Justicia, pudiéndose citar las siguientes sentencias: STSJ de Galicia de 20 de marzo de 2002, STSJ de La Rioja de 30 de mayo de 2002, STSJ de Extremadura de 14 de abril de 2004, STSJ de Madrid de 9 de mayo de 2006 y STSJ de Cataluña de 28 de octubre de 2006.

Así pues, consideramos necesario un cambio legislativo en la materia que delimite claramente los supuestos en los que el empresario pueda omitir dar traslado al comité de la intención de adoptar medidas de control, de forma y manera que la determinación de los supuestos en los que se ha infringido tal mandato venga reglada y no dependa tanto de la libre valoración de los tribunales. En opinión del profesor Javier THIBAULT, «se debería de dar una concertación *ex ante* y dinámica que permita, por ejemplo, a los representantes de los trabajadores [...] contribuir a definir qué datos sobre productividad y calidad pueden recogerse por vía informática, vigilar el control de acceso por tarjetas inteligentes o adaptar los principios de proporcionalidad y finalidad a cada situación parti-

cular»⁷. Ante la laxitud de las normas y medidas en el derecho español, THIBAUT propone, acertadamente a nuestro juicio, una mayor integración de los sujetos colectivos en la tutela preventiva de los derechos de los asalariados y una *concertación ex ante* realizada entre empresario y representantes de los trabajadores para intentar evitar ulteriores conflictos. La mejora de este aspecto nos acercaría más a la perspectiva de otros países europeos como Francia o Alemania.

4. Aproximación a los métodos modernos de vigilancia y control.

Las nuevas tecnologías han operado un cambio en los sistemas tradicionales de vigilancia de los trabajadores. Las funciones de los vigilantes jurados y, en general, de los agentes investigadores privados, han quedado obsoletas debido a la aparición de nuevos métodos de control basados en la automatización. Estos aportan varias ventajas: no solo suponen un menor coste para el empresario, sino que también ofrecen una información más objetiva, detallada y precisa sobre la actividad del trabajador.

No obstante, el avance de la tecnología en el control empresarial no siempre es compatible con el debido respeto a los derechos fundamentales del trabajador. En palabras de GOÑI SEIN, «las aplicaciones de la informática, a la vez que alteran la estructura actual o el papel de los vigilantes de empresa, comportan una seria amenaza a las libertades y derechos de los trabajadores». En este mismo sentido, SMURAGLIA dirá que «encontrar el punto de confluencia entre las exigencias del progreso y el respeto a la dignidad y también del desarrollo de la personalidad es uno de los problemas fundamentales de la sociedad moderna»⁸.

Los aparatos de control más utilizados por las empresas son los medios audiovisuales, que permiten grabar el sonido y captar la imagen del trabajador, destacando de entre los exclusivamente ópticos las filmadoras y, más concretamente, las cámaras de televisión a control remoto y de circuito interno.

Por su parte, la velocidad que caracteriza el sistema productivo actual, con la necesidad de interacción constante entre proveedores, clientes, competencia, etc., obliga a todas las empresas a tener un personal de informática y administrativo que se encargue de realizar estas labores. Surge así, casi sin quererlo, un nuevo y eficaz medio de control consistente en el escrutinio de las computadoras en busca de eventuales irregularidades cometidas por el trabajador en el desempeño de su puesto de trabajo. Este y el anterior son, a opinión nuestra, los medios de control de la actividad del trabajador más apasionantes, y por ello constituirán el objeto de nuestro estudio.

Similar a los anteriores, en tanto en cuanto suponen un control ajeno al conocimiento del trabajador, son utilizados (con relativa frecuencia) los sistemas de «ventanas polarizadas» y de ventanas transparentes en un solo sentido que permiten ejercer el control desde dentro sin ser visto desde fuera por los trabajadores.

⁷ THIBAUT ARANDA, Javier: «El papel de los representantes ...», pág. 362.

⁸ GOÑI SEIN, José Luis: *El respeto a la esfera privada...*, pág. 140.

No se puede, sin embargo, desconocer (ni desmerecer) la existencia de muchos otros medios de control en las empresas, si bien entrañan un control más compatible con los derechos fundamentales de los trabajadores y, por tanto, menos problemático, habida cuenta su conocimiento por aquellos. En este sentido, se puede citar el caso del reloj de control del personal a la entrada del centro de trabajo conectado a un ordenador central, que permite registrar las horas de entrada y salida de aquel, así como las ausencias, retrasos, salidas anticipadas, etc. Con este sistema no es necesario tener que consultar una por una cada ficha ni pedir información al jefe de turno.

Asimismo, existen otras formas mecánicas más efectivas de vigilancia; por ejemplo, la consistente en instalar en cada dependencia de la empresa un aparato de cerradura automática que, conectado a un ordenador central, abra o cierre la puerta al introducir en la base de la cerradura una tarjeta perforada o magnetizada de uso personal.

En definitiva, las nuevas tecnologías están brindando al empleador un sinnúmero de medidas únicamente limitadas por la inteligencia humana, de suerte que la panoplia de dispositivos de vigilancia de los que puede disponer aquel va *in crescendo* al compás del desarrollo de la microelectrónica y otras ciencias relacionadas con la tecnología.

Cabe adelantar ahora que, a pesar de la aparente ilicitud de algunos de estos mecanismos de control (los que afectan a la intimidad, a la propia imagen del trabajador y al secreto de las comunicaciones), el artículo 20.3 del ET dispone que «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». De lo que se deduce *prima facie* que no toda medida de control resulta ilícita.

II. CAPTACIONES AUDIOVISUALES

5. Captaciones audiovisuales.

a) *Lesión de derechos: en general.*

Las captaciones audiovisuales pueden violar o afectar a un amplio abanico de derechos. Por un lado, mediante imágenes obtenidas con teleobjetivos o micrófonos orientados hacia el interior de las viviendas, afectando con ello al derecho fundamental de la inviolabilidad del domicilio. La inviolabilidad del domicilio viene considerándose por la jurisprudencia como una manifestación de la intimidad. Pero como en este escrito se intenta esclarecer la captación audiovisual en el centro de trabajo, este derecho fundamental no quedaría afectado según la interpretación del domicilio que da el TC en su sentencia 10/2002. En esta sentencia se aduce que no se puede extender el derecho de

inviolabilidad del domicilio a aquellos lugares cerrados que «tengan un destino o sirvan a cometidos incompatibles con la idea de privacidad». El alto tribunal excluye expresamente de la protección de este derecho a las fábricas, oficinas, almacenes y locales comerciales.

Por otro lado, también pueden verse afectados por captaciones audiovisuales los derechos de reunión y manifestación. Estos derechos pueden ser vulnerados cuando los ejercitantes llegan a verse disuadidos en su ejercicio por el empleo de la videovigilancia. En relación con el derecho del trabajo, cabe referirse a la STC 37/1998, de 17 de febrero, en la que el tribunal falla reconociendo violados los derechos de libertad sindical y huelga (art. 28.1 y 28.2 CE), por ser grabados los ejercitantes por las autoridades policiales en el desarrollo de su derecho de huelga «sin mediar explicación alguna», «sin la existencia de disposición legal que estableciese un régimen de garantías de los derechos» y habiendo transcurrido la huelga con normalidad y sin incidentes. La medida en este caso resultó innecesaria y desproporcionada disuadiéndose con ello el libre ejercicio del derecho.

Por último, las captaciones audiovisuales pueden afectar a los derechos del artículo 18.1 CE (honor, intimidad y propia imagen). La captación audiovisual no provoca inicialmente una violación del derecho al honor, que sí podrá surgir *a posteriori*, cuando se difunda lo grabado. El caso particular de la lesión de la intimidad y propia imagen se abordará en el epígrafe que sigue.

b) Lesión de derechos: caso especial intimidad y propia imagen.

Se ha dicho en algún lugar anterior que los derechos a la intimidad y a la propia imagen pueden aparecer vinculados en una misma injerencia. Así sucederá cuando se capte la imagen de un trabajador: ambos derechos se verán afectados. Afectados, que no necesariamente lesionados. En cambio, cuando lo único que se obtenga por medio del control sea la grabación de sonidos procedentes del trabajador, queda afectado el derecho a la intimidad, pero no el derecho a la propia imagen. Una vez hecha esta precisión, necesaria para evitar errores conceptuales, cabe adentrarse en el estudio de la lesión de estos derechos.

Debe partirse de la desmitificación de la supuesta premisa de que el centro de trabajo no constituye por su idiosincrasia un espacio destinado al ejercicio del derecho de intimidad por parte de los empleados, quedando fuera de la protección de este derecho las conversaciones que mantengan los trabajadores entre sí y con los clientes en el desempeño de su puesto de trabajo. Antes al contrario, y como ha reconocido el TC en algunas sentencias (*vid.* STC 180/1999), la actividad profesional supone la proyección en el ámbito laboral de los derechos personalísimos del individuo, en especial del derecho al honor. Por tanto, la protección de los derechos del artículo 18 CE no debe limitarse a los lugares de descanso, vestuarios o similares, sino que hay que entenderla extendida sobre el resto de espacios del centro de trabajo en los que el trabajador desempeña su actividad. En este sentido, las SSTC 231/1988 y 197/1991 disponen que «no puede descartarse que también en aquellos lugares de la empresa en los que se desarrolla la actividad laboral puedan producirse intromisiones ilegítimas por parte del empresario en el derecho a la intimidad de los trabajadores, como podría serlo la grabación de conversaciones entre un trabajador y un cliente, o entre los propios trabajadores, en las que

se aborden cuestiones ajenas a la relación laboral que se integran en lo que hemos denominado propia esfera de desenvolvimiento del individuo».

De otro lado, la vinculación entre la captación de la imagen y sonido del trabajador por medios audiovisuales y la lesión de la intimidad y de la propia imagen no se configura como una relación causa-efecto. De suerte que el control audiovisual llevado a cabo por el empresario no siempre supone lesión de los derechos de la personalidad.

La regla general en la materia es la no admisión de las intromisiones en la intimidad de los trabajadores. En este sentido, la importante STC 186/2000, establece al efecto que «el empresario no queda apoderado para llevar a cabo, so pretexto de las facultades de vigilancia y control que le confiere el artículo 20.3 de la LET, intromisiones ilegítimas en la intimidad de sus empleados en los centros de trabajo».

No obstante lo anterior, es lugar común entre la doctrina y la jurisprudencia admitir la instalación de sistemas audiovisuales de control en aquellos casos en que exista una sospecha objetivamente fundada (y no una mera sospecha) de que el asalariado está descuidando sus obligaciones o está incurriendo en actuaciones delictivas (tales como la sustracción de dinero en efectivo de un cajero, deterioro de instalaciones, etc.), debiendo concurrir en la medida de control elegida los siguientes requisitos, establecidos con carácter general por el TC para determinar si ha existido lesión de un derecho fundamental:

1. Ha de venir justificada por algún acontecimiento, dato contable o elemento fáctico de la realidad que haya alertado al empresario de la posible comisión por parte del empleado (o de los empleados) de irregularidades en su puesto de trabajo que contribuyan a despilfarrar o reducir los recursos y el beneficio de la empresa; por tanto, lo que se prohíben son las medidas arbitrarias o caprichosas.
2. Ha de ser susceptible de lograr el objetivo propuesto (juicio de idoneidad).
3. Ha de ser necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia; esto es, dentro de las posibles, la medida elegida ha de suponer el menor agravio posible a los derechos fundamentales del trabajador (juicio de necesidad).
4. De la misma se han de derivar más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto).

La plasmación jurisprudencial de estos requisitos fue llevada a cabo por la citada STC 186/2000 (que supuso un cambio en relación a la línea jurisprudencial seguida hasta entonces). Esta denegó el amparo al recurrente por considerar que la instalación de un circuito cerrado de televisión que controlaba la zona donde aquel desempeñaba su actividad laboral «era una medida justificada (ya que existían razonables sospechas de la comisión por parte del recurrente de graves irregularidades en su puesto de trabajo); idónea para la finalidad pretendida por la empresa (verificar si el trabajador cometía efectivamente las irregularidades sospechadas y en tal caso adoptar las medidas disciplinarias

correspondientes); necesaria (ya que la grabación serviría de prueba de tales irregularidades); y equilibrada (pues la grabación de imágenes se limitó a la zona de la caja y a una duración temporal limitada, la suficiente para comprobar que no se trataba de un hecho aislado o de una confusión, sino de una conducta ilícita reiterada), por lo que no debe descartarse que se haya producido lesión alguna del derecho a la intimidad personal consagrado en el artículo 18.1 CE».

Continuando con el carácter eminentemente práctico e ilustrativo que hemos pretendido adoptar en este escrito, procede ahora referirse a otra importante sentencia en la materia, la STC 98/2000. En este caso, la empresa, un casino, contaba con sistema de control y seguridad consistente en video-vigilancia. Como complemento del indicado sistema, decidió instalar un sistema de grabación de audio. En este supuesto, entiende el TC que la implantación del nuevo sistema de control resulta lesivo del derecho fundamental a la intimidad, al no acreditarse la necesidad de un control general más intenso al preexistente como el que se pretendía establecer. «Como acertadamente advierte el Ministerio Fiscal, la instalación de los micrófonos no ha sido efectuada como consecuencia de la detección de una quiebra en los sistemas de seguridad y control anteriormente establecidos sino que, como se deduce del comunicado que la empresa remitió al Comité de empresa dando cuenta de la implantación del sistema de audición, se tomó dicha decisión para complementar los sistemas de seguridad ya existentes en el casino. Es decir, no ha quedado acreditado que la instalación del sistema de captación y grabación de sonidos sea indispensable para la seguridad y buen funcionamiento del casino. Así las cosas, el uso de un sistema que permite la audición continuada e indiscriminada de todo tipo de conversaciones, tanto de los propios trabajadores, como de los clientes del casino, constituye una actuación que rebasa ampliamente las facultades que al empresario otorga el artículo 20.3 de la LET y supone, en definitiva, una intromisión ilegítima en el derecho a la intimidad consagrado en el artículo 18.1 de la CE».

Particularmente curioso resulta el caso de la sentencia del TSJ de Galicia de fecha 20 de marzo de 2002. El actor, vigilante de seguridad, destinado en horario nocturno en un museo, fue despedido en base a las imágenes filmadas por una cámara de vídeo, sin sonido. Las mismas constataron que el recurrente abandonó su puesto de trabajo y estuvo durante varias horas manipulando un ordenador y masturbándose. El TSJ de Galicia resuelve el caso proyectando la doctrina de la STC 186/2000: «la Sala alcanza la conclusión de que no existió vulneración del derecho a la intimidad del trabajador por la grabación o filmación del modo de desempeñar las funciones propias del cometido de vigilancia del Museo de Lugo que tenía encomendada. Y ello es así, por cuanto la instalación de una microcámara en las dependencias del citado Museo que controlaba una sala que —como antes se dijo— forma parte de su lugar de trabajo, era una medida justificada con la que se consiguió el objetivo propuesto por la empleadora de comprobar y constatar el comportamiento del trabajador. Tampoco cabe apreciar por esta Sala la existencia de otra medida por parte de la empresa más moderada para conseguir dicho propósito, singularmente a la vista de lo que se afirma al final del Séptimo Fundamento de Derecho de la sentencia recurrida (penúltimo párrafo) sobre las condiciones en que se desarrollaba el trabajo por el actor y sus compañeros de vigilancia; siendo así que al tratarse de jornada laboral nocturna, el Museo permanecía cerrado, de forma que solo el propio vigilante que se encontraba en su interior era quien podía abrir la puerta para permitir el acceso al Museo, de forma que la grabación se tornaba como el medio más idóneo y necesario para constatar la conducta laboral del empleado durante el desarrollo de su jornada laboral. En resumen, el medio de control empleado se realiza de forma esporádica, afecta a todos los trabajadores, que como el actor realizan su jornada nocturna en el mencio-

nado Museo, la empleadora no cuenta con otro medio más racional y proporcionado de control por la razón antes apuntada, del cierre del Museo, la medida no afecta a la intimidad del trabajador, porque se realiza en el lugar de trabajo, y no en un espacio reservado para la salvaguarda de la intimidad del trabajador, por todo ello, a juicio de la Sala, se respeta el principio de proporcionalidad entre tal medida y el fin pretendido».

Del conjunto de estas sentencias se deduce que el TC tiene como regla general la inadmisión de la implantación en el centro de trabajo de aparatos de escucha que, complementando a la videovigilancia, puedan grabar las conversaciones del trabajador, en tanto en cuanto habitualmente no constituye una medida que pueda servir de utilidad a los fines indagatorios del empresario. La grabación de los sonidos emitidos por el asalariado no suele erigirse en elemento esencial para determinar si el empleado está descuidando o no sus labores, ya que en la mayoría de puestos de trabajo unas imágenes resultan suficientes para esta tarea. *A sensu contrario*, es admisible la grabación de sonidos en aquellos puestos de trabajo en los que la voz y las conversaciones resultan elementos determinantes para comprobar si el empleado ha eludido su actividad laboral, siempre que aquella sea compatible con todos los intereses en conflicto. Piénsese en el caso de operadores telefónicos, recepcionistas o similares, cuya función consiste principalmente en hablar por teléfono, siendo necesario en este caso el establecimiento de aparatos de grabación de sonidos para el control del trabajador en caso de sospechas. En este sentido, la STS de 5 de diciembre de 2003 admite como ajustada a Derecho la implantación de un sistema de monitorización de las llamadas recibidas por los asesores comerciales de «Telefónica de España SAU». El caso es el siguiente: los trabajadores (asesores comerciales) tienen que realizar actividades de telemarketing en la empresa mediante el uso de teléfonos. Son avisados (y por tanto conscientes) de que la empresa de telefonía graba aleatoriamente algunas conversaciones (solo se controlan las llamadas de entrada –de los clientes a los asesores–, y no así las de salida). La finalidad del control es la de corregir defectos en la técnica de marketing y poder así dar las instrucciones oportunas. Asimismo, se debe saber que los trabajadores cuentan con teléfonos no intervenidos en las salas de descanso mediante los cuales pueden realizar y recibir llamadas personales. Sabido todo lo anterior, el TS procede a resolver la cuestión en el sentido de entender que «se trata de un control que es necesario puesto que no se conoce otro método más moderado para obtener la finalidad que se pretende –juicio de necesidad–, es idóneo para el mismo fin –juicio de idoneidad– y ponderado o equilibrado porque de ese control se pueden derivar beneficios para el servicio que presta la empresa y no parece que del mismo se puedan derivar perjuicios para el derecho fundamental de los trabajadores –proporcionalidad en sentido estricto–».

c) Presupuestos de la lesión.

Decía la STSJ de Cataluña número 919/1996, de 13 de febrero de 1996, que «las cintas videográficas no son por sí mismas un medio ilegítimo aun cuando se pueda dudar de su eficacia para acreditar determinados hechos». En efecto, la práctica de los tribunales ha puesto de manifiesto la necesidad de la concurrencia de una serie de presupuestos para admitir la lesión del derecho a la intimidad (producida mediante grabación por medios ópticos, por microfónica o mediante la conjunción de ambos, esto es, control audiovisual) y, en su caso, del derecho a la propia imagen (la imagen del trabajador, en el sentido que le confiere la STC 81/2001, no se ve afectada ni lesionada por la mera grabación de los sonidos que profiera, sino que se exige la efectiva captación de aquella).

Estos presupuestos son los que siguen:

1. *Es necesario, en primer lugar, que el empleado desconozca la existencia del sistema de vigilancia.* Partiendo de la base de que el establecimiento de medidas de control por parte del empresario es perfectamente admisible a tenor del artículo 20.3 del ET, la puesta en conocimiento del trabajador de estas medidas de control adoptadas por la empresa no hace sino contribuir a garantizar la legitimidad de las mismas, permitiendo que los trabajadores afectados tomen las precauciones necesarias para salvaguardar su intimidad.

A mayor abundamiento, la recién citada STSJ de Cataluña número 919/1996 establece que «no atenta a la intimidad personal de los trabajadores la monitorización de la actividad propia de la prestación de servicios, no solo porque esta es plenamente conocida por los trabajadores, sino porque, además, obedece a la finalidad de asegurar el resultado de esa misma actividad en tanto se trata del cuidado y vigilancia nocturna de unos enfermos con especiales características de riesgo». En el mismo sentido se pronuncia la también citada STS de 5 de diciembre de 2003, en tanto en cuanto admite la legalidad de la monitorización efectuada por el empresario basándose, entre otros motivos, en el conocimiento de los asesores comerciales de la posibilidad de ser intervenidos sus teléfonos por aquel. De lo que se deduce que los tribunales han descartado que el conocimiento de las medidas de vigilancia enerve la intimidad.

2. *En segundo lugar, ha de existir una vinculación directa entre la filmación (y/o grabación de sonido) y el control del trabajador.* Así, no constituiría lesión de los derechos a la intimidad y a la propia imagen una monitorización cuya finalidad fuera distinta a la de controlar al empleado, pero que, sin embargo, entrañe un control indirecto sobre este, como las que se producen en bancos o cajeros de centros comerciales, cuyo objetivo no es sino tratar de identificar a eventuales delincuentes. Cabe añadir al respecto que en estos casos los empleados suelen conocer la existencia de las medidas de control, por lo que pueden cuidarse de tomar las precauciones necesarias. En todo caso, este es un terreno fangoso en el que resulta difícil a la empresa probar que la medida no constituye un control sobre el empleado, habiendo aplicado los tribunales el principio *in dubio pro operario* en aquellos casos en que se aprecie dificultad para discernir el verdadero fin de la medida de vigilancia.
3. *El tercer y último presupuesto que ha de concurrir es que la medida de vigilancia no cumpla alguno de los requisitos exigidos por la jurisprudencia para admitir su conformidad a Derecho (justificación, idoneidad, necesidad y proporcionalidad).* En efecto, toda medida que, afectando a los derechos a la intimidad y a la propia imagen, aspire a ser lícita, ha de venir justificada por algún elemento o circunstancia que alerte al empresario de la posible comisión de irregularidades en el puesto de trabajo por parte del empleado, debiendo ser aquella además idónea, necesaria y proporcional. A título de ejemplo, la anteriormente citada STC 98/2000, estableció la ilegalidad de la medida empresarial (y por tanto la lesión del derecho a la intimidad) consistente en complementar el sistema de videovigilancia con micrófonos, al no acreditarse una justificación de estos distinta a la de lograr un control más exhaustivo de los empleados.

III. APLICACIONES INFORMÁTICAS

6. Uso desviado de las aplicaciones informáticas (correo electrónico) y su control por el empresario.

a) *En general.*

La propia idiosincrasia de determinadas prestaciones laborales y la proliferación de las nuevas tecnologías en la actualidad ha contribuido a que el trabajo haya ido perdiendo ese componente físico que en buena medida lo determinaba, pasando de concebirse únicamente como una actividad de esfuerzo material a concebirse cada vez más como una actividad de esfuerzo intelectual, coherente con la sociedad de la información y de los servicios.

Ello también ha repercutido en la forma de control de los empresarios, habida cuenta la dificultad de probar el rendimiento real de empleados cuya prestación consiste en realizar una serie de actividades determinadas en mayor o menor medida apoyándose en una computadora. Máxime cuando es bastante frecuente la inexistencia de dos personas en el mismo centro de trabajo que, utilizando para sus labores computadora, realicen tareas idénticas o similares, de suerte que en principio no suele ser posible la comparación en el rendimiento que sí es factible realizar en los trabajos que incorporan un componente de esfuerzo físico.

De otro lado, la multiplicidad de tareas que se pueden llevar a cabo con una computadora eludiendo la prestación pactada desvirtúa cualquier propósito de control, no solo de las medidas de vigilancia tradicional, sino también de las medidas de vigilancia audiovisual, dada su imposibilidad para determinar con exactitud los fines a los que está respondiendo el uso de la computadora. De lo que se deriva para el empresario la necesidad de buscar nuevos cauces que le permitan realizar un control efectivo sobre aquellos empleados cuya prestación se efectúe mediando equipos informáticos.

b) *Tipos de control.*

Es frecuente que los asalariados para realizar su prestación requieran de computadora y utilicen esta para fines diferentes a los asignados por el empresario. Desde leer la edición digital del periódico hasta utilizar el correo con fines particulares, un sinfín de posibilidades se abren al empleado que trabaja con equipos informáticos conectados a la red. Por tanto, las nuevas formas de control empresarial a las que antes hacíamos referencia pasan de ser unas medidas explícitas, en tanto en cuanto el empleado era pillado *in fraganti*, a unas medidas de naturaleza indirecta, en la medida en que no responden a un control directo y explícito sino que se basan en las *huellas* dejadas por el trabajador en el equipo informático. Así, se pueden destacar de entre las medidas de control las siguientes:

- **Historial:** en la barra de tareas superior de las páginas de Internet aparece un icono que responde a la denominación de *historial*. Esta función del equipo almacena todas las páginas

visitadas por el usuario, de forma y manera que permite al empresario controlar el uso que el empleado hace de Internet.

- Dirección: del mismo modo, en la barra de tareas superior de las páginas de Internet aparece un ítem que responde a la denominación de *dirección*, seguido de un espacio para que el usuario teclee la página a la que guste tener acceso. Se pueden controlar de esta forma todas las páginas a las que el empleado ha accedido directamente.
- Google: una tercera medida de control similar consiste en observar las palabras claves que el usuario ha utilizado en el buscador, y que se puede llevar a cabo situándose sobre el icono de google que aparece en la barra de tareas superior de las páginas de Internet.
- Messenger: otra medida sería la del control por medio del servicio de mensajería instantánea MSN Messenger. Es este un programa que permite a los usuarios comunicarse en tiempo real e incluso enviar mensajes de voz, quedando registradas las conversaciones mantenidas. Este tipo de control y el siguiente plantean algunas cuestiones de orden ético y moral que plantearemos más adelante.
- Correo electrónico: es la medida de control por excelencia. Algunos ordenadores tienen desactivadas e imposibilitadas determinadas funciones (como, por ejemplo, visitar determinadas páginas de contenido no recomendable o acceder al MSN Messenger), si bien en todos ellos se permite la utilización del correo electrónico. Esto es así porque el trabajo de muchos de estos empleados consiste precisamente en una continua interacción con el correo, para enviar mensajes a proveedores, clientes, grupos de interés, etc., o bien para recibirlos. De suerte que la fiscalización del correo electrónico se erige en la medida de control más proclive a ser utilizada por el empresario.

Estas son algunas de las medidas más significativas y utilizadas, un listado sin carácter exhaustivo, que en ningún caso constituye un *numerus clausus*. Existen muchas otras, de mayor complejidad técnica y superior coste, que van desde un examen detenido de la computadora en búsqueda de documentos y archivos personales hasta la utilización de programas espía.

c) Virtualidad de este tipo de control en la práctica y colisión con el derecho al secreto de las comunicaciones.

Antes de continuar, es menester realizar dos apreciaciones de vital importancia. La primera se refiere a la virtualidad de estas formas de control en la práctica. En este sentido, la propia naturaleza del control, generalmente indirecta, le resta eficacia en comparación con las medidas de vigilancia audiovisual. En efecto, el control por medios informáticos está condicionado a la pericia informática del empleado. Y es que las medidas señaladas son muy débiles, en tanto en cuanto el trabajador que ostente unos determinados conocimientos de informática e Internet puede hacer desaparecer sus *huellas* de la computadora.

En todo caso, un experto informático podría encontrar siempre rastros, si bien es evidente que para que el empresario recurra a aquel el rendimiento del empleado tiene que distar mucho de lo

esperado y prolongarse esta situación en el tiempo, ya que, como se acaba de decir, unas ligeras sospechas del empresario pueden ser fácilmente eliminadas por el trabajador, haciéndole creer que su rendimiento es el adecuado.

La otra precisión que debe hacerse es que este tipo de medidas entraña un problema de orden ético-moral. Cabe decir al respecto que el control por medios informáticos puede ir más allá de lo que es el estricto control del trabajo del empleado, y adentrarse en la esfera íntima y personal irreductible de este. En efecto, puede resultar que el empresario constata, por ejemplo, que un determinado empleado se dedica en horas de trabajo a mantener conversaciones con seres cercanos por el servicio de mensajería instantánea MSN Messenger. Pero puede también pasar que no lo compruebe únicamente, sino que también se dedique a indagar en la vida personal de su empleado, leyendo a tal efecto las conversaciones registradas.

Esta actitud del empresario choca frontalmente con otro de los derechos fundamentales proclamados en el artículo 18 CE. Dicho precepto de la Carta Magna, en su apartado 3, dispone que «se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial».

La conculcación del derecho al secreto de las comunicaciones no se produce únicamente en esta sede, sino que también es probable que pueda darse con las medidas de vigilancia que incluyan control por microfonía. No obstante, es aquí, en el control por medios informáticos, donde adquiere mayor relieve la posibilidad de lesionar este derecho, y es por tanto donde los tribunales deben apoyar los medios de reacción más enérgicos, comenzando por declarar la ilegalidad de aquellos controles que el empleado consiga probar que, sin finalidad lícita, han invadido su esfera íntima y personal irreductible. De otra parte, dejaremos a un lado los supuestos de uso sindical del correo electrónico, en tanto en cuanto afectan a un derecho (libertad sindical) no integrado en nuestro objeto de estudio.

d) Jurisprudencia en la materia.

Llegados aquí, la labor de la jurisprudencia se ha centrado en juzgar hasta qué punto es admisible el control por el empresario de las aplicaciones de los equipos informáticos, y no en desaprobarlo de raíz. En este sentido, la doctrina de los tribunales es muy similar a la de la vigilancia audiovisual antes explicada.

La regla general es la inadmisión de intromisiones en los derechos a la intimidad y al secreto de las comunicaciones (aquí, como resulta evidente, no se viola el derecho a la propia imagen). En todo caso, como se dijo en el caso de la vigilancia audiovisual, esta regla general puede ceder siempre y cuando la medida de control cumpla los requisitos establecidos por la STC 186/2000: justificación, idoneidad, necesidad y proporcionalidad, que son de aplicación también aquí en el ámbito del control por medios informáticos.

Cabe decir al respecto que el examen de la justificación, idoneidad y necesidad es muy similar al realizado en el caso de captaciones audiovisuales. No obstante, en orden a la ponderación de los

intereses y derechos en conflicto (juicio de proporcionalidad) juegan aquí un papel fundamental tres elementos: 1) conocimiento del empleado del control de los equipos informáticos; 2) consentimiento del empleado para el control de aquellos y 3) imposibilidad de utilizar el correo electrónico y otras aplicaciones de Internet para fines privados. Estos elementos actúan como legitimadores del control; su concurrencia suele implicar la declaración de la medida como ajustada a Derecho por los tribunales y su ausencia suele ser sinónimo de ilegalidad del control, si bien constituyen criterios meramente orientativos. Los examinaremos separadamente a pesar de su proximidad conceptual.

Respecto del primer elemento, cabe decir que es razonable pensar que si el trabajador tiene conocimiento del control de los equipos informáticos es muy probable que se cuide de tomar las precauciones adecuadas en orden a no ser detectado por el empresario. Por tanto, el conocimiento del control de tales medios ofrece al trabajador varias posibilidades: de un lado, la posibilidad de borrar las huellas que haya podido dejar en la computadora y, de otro (y principalmente), la no utilización de los equipos informáticos para fines distintos a los asignados por el empresario. De forma y manera que los tribunales han venido entendiendo que el conocimiento por parte de los empleados de las medidas de control constituye un elemento legitimador de estos. Así, en la STSJ de Cataluña de 11 de marzo de 2004 se acredita como hecho probado en la sentencia recurrida que «en fecha de 10-02-2003 la empresa y la actora firmaron un anexo a su contrato de trabajo en el cual se autorizaba a la empresa a supervisar periódicamente los listados de llamadas efectuadas desde las distintas extensiones, los listados de páginas web visitadas por cada usuario, así como los correos enviados y recibidos, estableciéndose que el acceso a Internet con lo equipos de la empresa solo se utilizará cuando sea necesario para la realización del trabajo», motivo utilizado después en los fundamentos de derecho para desestimar la pretendida lesión de los derechos a la intimidad y al secreto de las comunicaciones.

No obstante, *a sensu contrario*, resulta lógico pensar (en congruencia con la jurisprudencia señalada) que, aun mediando el conocimiento del trabajador de la medida de control, esta sea declarada ilegal por los tribunales cuando sea meramente arbitraria y no responda a ningún indicio.

Por su parte, el desconocimiento por parte del asalariado del escrutinio de los equipos informáticos tiende a privar de legitimidad al control, si bien no conlleva necesariamente la ilegalidad de la medida. De un lado, es evidente que cuando el control responda a criterios arbitrarios o caprichosos la medida empleada será ilegal. En este sentido, cabe destacar la STSJ de la Comunidad Valenciana de 19 de julio de 2005. El caso es el siguiente: una empleada es despedida por haber sido encontradas entre sus conversaciones del chat MSN Messenger (utilizado por la empresa para la comunicación con compañeros de otras delegaciones o empresas filiales) diversas afirmaciones injuriosas e irrespetuosas hacia la empresa, su gerente y distintos compañeros de trabajo. No existía ningún indicio sobre posibles irregularidades en el puesto de trabajo, tratándose por tanto de un control caprichoso. El TSJ de la Comunidad Valenciana dispuso al respecto que «como se ha señalado por la doctrina más autorizada, las medidas empresariales encaminadas a realizar una actuación inspectora o controladora de la actividad laboral de sus trabajadores, deben ir precedidas, en todo caso, de la necesaria información a los destinatarios de los sistemas de control establecidos. Así, se ha venido considerando, que sería contrario a la buena fe contractual que debe presidir las relaciones laborales en la empresa el establecimiento subrepticio de mecanismos de supervisión del uso que hacen los trabajadores de los medios informáticos puestos a su disposición por la empresa para el ejercicio de su quehacer laboral, sobre todo si la

implantación de tales mecanismos no obedece a una sospecha previa de actuación fraudulenta por parte del trabajador investigado». Añade dicha sentencia que «en definitiva, no se pone en duda la legítima facultad empresarial de efectuar un control de la actividad laboral de sus empleados, lo que se cuestiona es la manera que en el presente caso fue puesta en práctica tal facultad, pues ni los trabajadores estaban advertidos, siquiera que con carácter general, del establecimiento de mecanismos de control, ni tampoco consta que el empresario procediera en virtud del principio de intervención indiciaria, según el cual cabría una justificación de las medidas adoptadas cuando se acreditara la existencia de indicios reveladores de una actuación irregular por parte del trabajador. En definitiva, pues, la actuación empresarial no puede calificarse de justificada, en los términos analizados en la STC 186/2000 (RTC 2000, 186), toda vez que, como se ha dicho, no consta que existieran razonables sospechas de la comisión por parte de la recurrente de graves irregularidades en su puesto de trabajo. Por lo que debe entenderse que la medida adoptada obedeció al propósito de vigilar y controlar genéricamente el cumplimiento por los trabajadores de las obligaciones que les incumben, lo que la STC 98/2000 (RTC 2000, 98) rechazó como razón suficiente justificativa del establecimiento de medidas de control empresarial que, como las empleadas en el presente caso, pudieran afectar a la intimidad de los trabajadores».

En cambio, no puede desconocerse la validez del control siempre que con él se pretendan detectar conductas irregulares que hayan quedado suficientemente acreditadas, aun cuando no se haya avisado al trabajador de la intervención de las computadoras. En este orden de ideas, la STSJ de Madrid de 13 mayo de 2003 (que resuelve un supuesto en el que los trabajadores están advertidos de la posibilidad de que sus ordenadores sean controlados) admite que «[...] siendo evidente que notificar al trabajador cuándo se va a realizar la inspección conllevaría la desaparición y destrucción de la prueba, y por tanto, de todo vestigio de una conducta irregular».

Toca ahora referirse al segundo de los elementos a los que aludíamos antes: el consentimiento del empleado para el control de los equipos informáticos. Es este un elemento que comparte muchas similitudes con el anterior y que en la práctica suelen equipararse, si bien no son idénticos. Es evidente que cuando un trabajador conoce que su computadora puede ser sometida a escrutinio periódico está aceptando implícitamente que se produzca ese control (aunque no sea esa su voluntad), no pudiendo oponerse al mismo, pues los equipos informáticos se adscriben general y únicamente a un fin ajeno al del empleado y que tiene que ver con la actividad de la empresa, de suerte que la información almacenada en ellos interesa de forma capital al empresario. Podemos hablar, por tanto, en estos casos de un consentimiento tácito, generalmente incardinado en los preceptos del convenio colectivo aplicable suscrito por los representantes de los trabajadores. Dicho consentimiento tácito legitimaría el control informático del empresario. En este sentido, cfr. STSJ de Cataluña de 6 de mayo de 2005 y STSJ de Madrid de 13 de mayo de 2003.

En sentido opuesto, en ocasiones el consentimiento tácito no es suficiente para habilitar al empresario a realizar un escrutinio de los equipos informáticos de sus empleados, sino que necesita del consentimiento expreso de estos, bien porque aquellos se destinen también a fines particulares o por cualquier otro motivo. Igualmente, la concurrencia del consentimiento expreso legitima la medida de control empleada por el empresario. Así, en la antes citada STSJ de Cataluña de 11 de marzo de 2004 se establece como argumento para desestimar la lesión de los derechos a la intimidad y al secreto de las comunicaciones el hecho de que «la demandante aceptó, en el tan repetido anexo al contrato de trabajo de 10

de febrero de 2003 la supervisión periódica de los listados de las páginas web visitadas por cada usuario y correos enviados y recibidos con indicación de la dirección, fecha, hora, y tiempo de utilización, que es lo que en definitiva hizo legítimamente la demandada para averiguar la actividad laboral de la demandante sin incidir, según el hecho probado décimo, en el contenido del programa utilizado por esta».

Por último, un tercer elemento que contribuye a legitimar la medida de control es la imposibilidad de emplear el correo electrónico, y, en fin, cualesquiera otras aplicaciones informáticas y de Internet para usos privados, ajenos al objeto de la actividad empresarial. En la mayoría de los casos, las empresas se cuidan de prohibir el acceso a la red para fines particulares, estableciendo consecuencias disciplinarias para aquellos trabajadores que hagan caso omiso de dicha interdicción. En este sentido, las citadas sentencias del TSJ de Madrid de 13 de mayo de 2002 y del TSJ de Cataluña de 11 de marzo de 2004 se apoyan en el hecho de que el uso de Internet para fines privados no está permitido para desestimar la pretendida lesión de los derechos a la intimidad y al secreto de las comunicaciones.

En otros casos, lo que se prohíbe no es el uso, sino el abuso, si bien aquel se encuentra generalmente limitado a las páginas de contenido compatible con los valores de la empresa y, en definitiva, de la sociedad, siendo frecuente la prohibición de visitar páginas de contenido erótico o sexual y páginas que puedan poner en peligro datos o información de la empresa. La cuestión aquí consiste en determinar cuándo se sobrepasa el umbral que separa el uso del abuso. En este sentido, la importante STSJ de Cataluña de 11 de marzo de 2004 establece que «como se ha dicho resulta del anexo del contrato que tal permisión (de uso de Internet para fines personales no vinculados al trabajo) está constreñida a la forma más restringida posible y en ningún caso abusiva, lo que sin duda no concuerda con la conducta de la trabajadora sancionada que, según el hecho probado tercero de la sentencia, no impugnado, utilizó Internet para asuntos personales no relacionados con su trabajo durante sesenta y dos horas, trece minutos y veinticuatro segundos en doce días, lo que evidentemente sobrepasa con mucho la permisividad empresarial que se constata en el anexo del contrato de trabajo constituyendo un incumplimiento contractual grave y culpable».

A sensu contrario, la STSJ del País Vasco de 21 de diciembre de 2004, tomando como hechos acreditados en la sentencia de instancia que «el demandante, así como los demás trabajadores de la empresa, tiene asignado una dirección de e-mail y acceso a Internet, habiendo utilizado estos para usos particulares durante el tiempo de trabajo accediendo a páginas pornográficas o chateando con personas ajenas a la empresa, disponiendo en su despacho de varias pantallas. No existe prohibición expresa en la empresa para la utilización de estos medios», dispuso al efecto que «si el trabajador tiene posibilidades de mantener un ámbito privado y particular, autorizado por la empresa, y ello lo deducimos de la falta de prohibición específica, así como de los medios entregados al trabajador, deduciremos que la investigación que se le ha practicado incide sobre un derecho fundamental, y en tanto la prueba obtenida para alcanzar la gravedad de los hechos resulta ilícita, por inmiscuirse en el artículo 18 CE», si bien en este caso la declaración de la lesión de los derechos del artículo 18 CE se admitió en base a unos parámetros de uso de Internet mucho menores a los que se acreditaron en la STSJ de Cataluña de 11 de marzo de 2004.

En el mismo sentido (favorable al empleado) que la anterior se pronuncia otra sentencia del TSJ del País Vasco, curiosamente de la misma fecha, 21 de diciembre de 2004, que resuelve otro recurso de suplicación. En los antecedentes de hecho, se transcribe como hecho probado en la sentencia de instan-

cia que «ni la dirección de la empresa ni el Jefe de Personal habían comunicado o requerido nunca al actor que no podía utilizar para fines particulares medios de comunicación de la empresa», para después llegar a concluir en los fundamentos de derecho, en coherencia con el juzgado de instancia, que había consentimiento para utilizar los equipos informáticos para fines privados, habida cuenta que «no se había prohibido expresamente al recurrente –al parecer a nadie en la empresa– utilizar el correo electrónico instalado en el ordenador puesto a disposición por la empresa, para fines particulares». Adviértase también que en ningún caso se trató de un uso desmedido de las aplicaciones informáticas.

Por tanto, podemos concluir que aquí no existen reglas generales, sino que el umbral que separa el uso del abuso depende del caso concreto. Así pues, los límites los marca la razón y el correcto desempeño del puesto de trabajo. Cuando el uso de Internet comprometa el rendimiento del trabajador en su puesto, la medida de control utilizada para corroborarlo adquirirá plena legitimidad.

IV. CONSECUENCIAS DEL CONTROL ILÍCITO

7. Consecuencias derivadas para el empresario del control ilícito.

Cuando un empresario adopta la decisión de instalar un sistema de control de los trabajadores, suele hacerlo en base a unas sospechas que le hacen dudar del rendimiento real de aquellos, medida considerada ajustada a Derecho por los tribunales siempre que las sospechas estén fundadas y el sistema de control sea el que cause menor agravio a los empleados. No obstante, es muy frecuente que la medida de control adoptada por el empleador no esté basada siquiera sea en ligeras sospechas, sino que se trate de una medida de control genérico (expresamente prohibido por el TC) o simplemente responda a una decisión arbitraria o caprichosa.

En este último supuesto, tras la implantación por parte del empresario de una cámara de vigilancia pueden devenir dos tipos de sanciones. La primera de ellas se da cuando la medida de control obedece a un acto de discriminación, tales como que solo se hayan puesto cámaras a los empleados que están afiliados a un sindicato o si el propósito es seguir el trabajo de algún empleado de color, etc. En el caso de que medie discriminación en la medida debemos de atenernos al artículo 17.1 del ET, según el cual «se entenderán nulos y sin efecto los preceptos reglamentarios, las cláusulas de los convenios colectivos, los pactos individuales y las decisiones unilaterales del empresario que contengan discriminaciones directas o indirectas desfavorables...». Por tanto, se presume la nulidad de un eventual despido en el caso que nos ocupa, en tanto en cuanto se demuestre que la medida de control respondía a criterios discriminatorios y atentatorios contra la igualdad (en este caso, los efectos de la medida discriminatoria se equiparan a los de una medida de control genérico).

Para los restantes incumplimientos en que no medie discriminación, es decir, cuando la medida adoptada por el empresario de forma unilateral conculque solo el derecho a la intimidad (y, en su caso, el derecho a la propia imagen) cabe atenerse al artículo 50.1 del ET⁹, concretamente a los apar-

⁹ RAMÍREZ MARTÍNEZ, Juan Manuel y otros: *Curso de Derecho del Trabajo*, Valencia, Tirant lo Blanch, 2007, pág. 456.

tados a) y c), según los cuales «serán causas justas para que el trabajador pueda solicitar la extinción del contrato:

- a) Las modificaciones sustanciales en las condiciones de trabajo que redunden en perjuicio de su formación profesional o en menoscabo de su dignidad.
- c) Cualquier otro incumplimiento grave de sus obligaciones por parte del empresario, salvo los supuestos de fuerza mayor, así como la negativa del mismo a reintegrar al trabajador en sus anteriores condiciones de trabajo en los supuestos previstos en los artículos 40 y 41 de la presente Ley, cuando una sentencia judicial haya declarado los mismos injustificados».

En el apartado c) nos encontramos ante un precepto genérico, al contener la ley la expresión «cualquier otro incumplimiento grave». Más concreto resulta el apartado a). La instalación de cámaras de videovigilancia puede acarrear un perjuicio en la formación profesional de los trabajadores, en tanto en cuanto pueden verse cohibidos o sometidos a una presión innecesaria en su puesto de trabajo. Además de poder incluso menoscabar su dignidad. En el caso de que se dieran estas *iustas causas*, el trabajador puede solicitar la extinción de su contrato, sin perjuicio de la solicitud judicial de nulidad.

De darse los supuestos contemplados en el artículo 50 del ET a causa del establecimiento de cámaras y se haya logrado la extinción del contrato, el trabajador tiene derecho a la misma indemnización que resulta de un despido improcedente. Recordando lo prescrito por el artículo 56.1 a) del ET, el empleado podrá obtener «una indemnización de cuarenta y cinco días de salario, por año de servicio, prorrateándose por meses los períodos de tiempo inferiores a un año hasta un máximo de cuarenta y dos mensualidades».

Además, sin perjuicio de lo anterior (la posibilidad de extinción del contrato con la indemnización correspondiente), el artículo 40.1 c) de la LISOS tipifica la sanción dineraria pertinente ante una infracción muy grave, teniendo presente aquí que el artículo 8.11 califica como *muy graves* las infracciones que conlleven la violación de la intimidad y respeto a la dignidad.

En cualquier caso, al tratarse la no discriminación y la intimidad de unos derechos protegidos por la Constitución en términos de derechos fundamentales (derechos del art. 14 al 29 CE), la controversia judicial a causa de una posible violación o no de los mismos puede llegar ante el TC por medio del recurso de amparo.

8. Interdicción procesal de las pruebas obtenidas de modo ilícito.

Se ha dicho ya que el establecimiento de medidas de vigilancia al empleado es considerado lícito por la jurisprudencia cuando responde a una determinada inquietud fundada del empresario sobre el rendimiento real de alguno (o algunos) de sus trabajadores, requiriéndose además que la medida sea, de entre las posibles, la menos gravosa para aquellos. En estos casos, las pruebas obtenidas con la medida de control son admitidas como válidas por los tribunales, a pesar de su evidente colisión con algunos de los derechos fundamentales del trabajador.

En cambio, las medidas de control en ocasiones no se ajustan a la legalidad, bien por no responder a un fin concreto, o bien porque, respondiendo a un fin concreto, se emplean para objetivos distintos de los que supuestamente motivaron la instalación de las mismas. En el primer caso, el empresario busca un control genérico, omnímodo e indeterminado de sus trabajadores, carente de base legal y prohibido de forma expresa por el TC. Por su parte, en el segundo caso, las medidas empleadas son inicialmente legales en base a un fin concreto y lícito determinado, si bien acaban derivando en antijurídicas por emplearse para cometidos distintos.

Las pruebas obtenidas en estos dos supuestos han venido considerándose ilícitas por los tribunales, de suerte que han privado de licitud a despidos aparentemente procedentes. Y es que los derechos fundamentales del trabajador consagrados en el artículo 18 CE no pueden quedar menoscabados por decisiones arbitrarias o caprichosas del empleador.

La cuestión de la invalidez de las pruebas obtenidas ilícitamente fue planteada y zanjada en un primer momento por la STC 114/1984¹⁰, que resuelve un recurso de amparo interpuesto por un periodista del diario Información de Alicante, quien consideró conculcado su derecho al secreto de las comunicaciones por la Magistratura de Trabajo número 4 de Alicante, en tanto en cuanto declaró procedente su despido a partir de un instrumento (la grabación fonográfica de la conversación por él mantenida, el 14 de septiembre de 1982, con quien ocupaba entonces el cargo de Consejero técnico del Gabinete del Ministerio de Transportes y Comunicaciones) ilícitamente obtenido, así como por la Sala Sexta del TS, a la que culpaba de realizar una «interpretación errónea» del artículo 18 CE. Al respecto, establece el TC que «aun careciendo de regla legal expresa que establezca la interdicción procesal de la prueba ilícitamente adquirida, hay que reconocer que deriva de la posición preferente de los derechos fundamentales en el ordenamiento y de su afirmada condición de "inviolables" (art. 10.1 de la Constitución) la imposibilidad de admitir en el proceso una prueba obtenida violentando un derecho fundamental o una libertad fundamental». Añade el Tribunal que «esta garantía deriva, pues, de la nulidad radical de todo acto –público o, en su caso, privado– violatorio de las situaciones jurídicas reconocidas en la Sección Primera del capítulo segundo del título I de la Constitución y de la necesidad institucional por no confirmar, reconociéndolas efectivas, las contravenciones de los mismos derechos fundamentales».

En el mismo sentido, el alto tribunal sitúa la cuestión de la admisibilidad de la prueba ilícitamente obtenida «en una encrucijada de intereses, debiéndose así optar por la necesaria procuración de la verdad en el proceso o por la garantía –por el ordenamiento en su conjunto– de las situaciones jurídicas subjetivas de los ciudadanos». Así pues, la sentencia viene a rechazar la eficacia de la prueba ilegalmente obtenida, si bien solo tratándose «de derechos fundamentales que traen su causa, directa e inmediata, de la norma primera del ordenamiento», pero no cuando las situaciones jurídicas subjetivas tengan su base en una norma infraconstitucional. Este es el sistema que rige en el derecho francés y en el derecho alemán (que serán tratados más adelante): las pruebas obtenidas conculcando derechos fundamentales del trabajador son inadmitidas de plano en el proceso.

No obstante, la doctrina sobre la eficacia de las pruebas obtenidas de modo ilícito contenida en la STC 114/1984 ha experimentado cambios al socaire de la STC 186/2000. En efecto, la evolución juris-

¹⁰ GOÑI SEIN, José Luis: *El respeto a la esfera privada...*, págs. 158-159.

prudencial que se manifiesta en esta en lo relativo al análisis de la pretendida lesión de derechos fundamentales (se pasa de excluir de raíz cualquier control que lesione derechos fundamentales a admitirlo en determinados casos) se extiende también al tema de las pruebas obtenidas de forma ilícita. En este sentido, se abandona la doctrina que afirmaba la supremacía de los derechos fundamentales del trabajador a la hora de dirimir la admisión o inadmisión de la prueba en juicio [«aun careciendo de regla legal expresa que establezca la interdicción procesal de la prueba ilícitamente adquirida, hay que reconocer que deriva de la posición preferente de los derechos fundamentales en el ordenamiento y de su afirmada condición de "inviolables" (art. 10.1 de la Constitución) la imposibilidad de admitir en el proceso una prueba obtenida violentando un derecho fundamental o una libertad fundamental»] para dar paso a una ponderación (juicio de proporcionalidad) de los intereses y derechos en conflicto, de la que no siempre resultará la preferencia de los derechos fundamentales del trabajador. En la práctica, las pruebas obtenidas de modo ilícito serán admitidas en juicio cuando, existiendo incumplimiento de las obligaciones del trabajador, se acredite que las sospechas del empresario en cuanto a su rendimiento estaban «suficientemente fundadas», esto es, siempre que no se tratara de una medida de control arbitraria.

V. DERECHO COMPARADO

9. Derecho comparado.

a) *Sistema francés.*

Tras un análisis sistemático, la comparativa de las captaciones audiovisuales entre el derecho español y el derecho francés suscita dos grandes diferencias: una primera de carácter normativo y una segunda de orden jurisprudencial.

Comenzando por la diferencia normativa cabe decir, como ya se ha anticipado en otra ocasión, que en el derecho español no encontramos una regulación específica que verse sobre las captaciones audiovisuales y la «cibervigilancia». Del mismo modo, en el ET solo hay un precepto –el 4.2 e)– que se refiera a la intimidad en el ámbito laboral, debiendo entenderse implícita en el mismo la protección del derecho a la propia imagen.

En cambio, en el derecho francés podemos observar un precepto concreto del *Code du Travail* que ofrece algo más acerca de los medios técnicos de control. Nos estamos refiriendo al artículo *L.432-2-1*, que dispone al respecto lo siguiente: «le comité d'entreprise est informé, préalablement à leur utilisation, sur les méthodes ou techniques d'aide au recrutement des candidats à un emploi ainsi que sur toute modification de ceux-ci.

Il est aussi informé, préalablement à leur introduction dans l'entreprise, sur les traitements automatisés de gestion du personnel et sur toute modification de ceux-ci.

Le comité d'entreprise est informé et consulté, préalablement à la décision de mise en oeuvre dans l'entreprise, sur les moyens ou les techniques permettant un contrôle de l'activité des salariés».

Este artículo establece la obligación por parte del empresario de informar al comité de empresa acerca de los medios que permitan controlar la actividad de los trabajadores. En este sentido, también es importante el artículo L.120-2: «nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives des restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché».

La segunda diferencia, la de orden jurisprudencial, alude al distinto tratamiento que dan los tribunales españoles y franceses a esta materia. Como ha quedado bastante asentado durante esta investigación, los tribunales españoles, al no existir una clara regulación normativa y al entrar en juego derechos fundamentales (intimidad y propia imagen), resuelven los casos ateniéndose a un análisis de la justificación, necesidad, idoneidad y proporcionalidad de la medida. Los tribunales galos, como veremos enseguida, actúan de manera distinta.

Antes que nada, decir que distinguiremos en nuestro análisis entre la instalación de cámaras de videovigilancia y el registro de conversaciones telefónicas, a fin de alcanzar una mejor comprensión y delimitar con mayor detalle los supuestos. Respecto de la videovigilancia, es ineludible referirse a una sentencia relativamente reciente, la de 19 de abril de 2005, dictada por la *Cour de Cassation* o Tribunal de Casación. Esta sentencia trata sobre la ilicitud de la prueba obtenida por un sistema de videovigilancia oculto, instalado a fin de controlar a los empleados. En ella se dispone que el empresario no puede instalar una cámara que controle a sus empleados sin ponerlo en conocimiento de los mismos, en coherencia con lo dispuesto en el artículo L.121-8 del *Code du Travail*, que exige que el empresario informe previamente a los trabajadores sobre cualquier técnica que utilice para controlar su actividad en el trabajo, de modo que ninguna información relativa a los trabajadores puede ser recogida sin que se les haya informado de antemano. En cambio, sí que se permite aportar como prueba las imágenes grabadas por una cámara de vigilancia de un local cuya finalidad no es otra sino controlar eventuales robos de clientes, como las instaladas a tal efecto en los centros comerciales o en los bancos.

Otro ejemplo, referido a un caso concreto, lo constituye la Sentencia de la *Cour de Cassation* de 23 de noviembre de 2005. En dicha sentencia, una empleada que trabaja en un bar es despedida por consumir bebidas en horas de trabajo sin registrar en la caja dicho consumo, es decir, bebía sin pagar. Mediante el uso de una cámara oculta el empresario verificó los hechos. El tribunal francés condenó al empresario a pagar cierta cantidad a la empleada porque había instalado la cámara sin dar conocimiento de la misma. La sentencia aclara que «il ne peut mettre en oeuvre un dispositif de contrôle qui n'a pas été porté préalablement à la connaissance des salariés», es decir, no se puede implementar un dispositivo de control (en este caso de videovigilancia) sin ponerlo en conocimiento de los asalariados (o sus representantes).

Una tercera sentencia muy ilustrativa en orden a la ilicitud de la prueba viene a ser la Sentencia de la *Cour de Cassation* de 26 de abril de 2006, en la que se aduce que (traducido a castellano) «constituye un modo de prueba ilícita la que [...] mediante técnicas de registro de imágenes, o de palabras, implique un atentado a la vida privada». Por su parte, la Sentencia de la *Cour de Cassation* de 7 de junio de 2006 utilizó también esta misma doctrina en el caso de un trabajador de Carrefour que había sido despedido. Si bien la cámara fue colocada con el objetivo de controlar a los clientes, la *Cour de Cassation* consideró la grabación como un medio de prueba ilícito al quedar constatado que aquella, inicialmente instalada para vigilar a los clientes, era también utilizada para controlar a los empleados.

Por tanto, podemos concluir que en el derecho francés, en caso de que el empresario avise de la instalación de cámaras, estas pueden violar en algún supuesto concreto la intimidad y la propia imagen, pero, si no se avisa, los tribunales franceses siempre consideran la prueba basada en la captación como ilícita, sin efectuar la ponderación de derechos e intereses que a tal efecto realizan los tribunales españoles.

En el tema de registros o intervenciones en los teléfonos, se sigue una línea más o menos similar a la explicada en las cámaras de videovigilancia. La Sentencia de la *Cour de Cassation* de 7 de octubre de 2004 establece que el registro de una conversación telefónica privada es un procedimiento desleal inadmisibles como prueba. Este sería el caso, por ejemplo, de la intervención telefónica de la conversación de un trabajador de una fábrica cuando habla con un amigo o familiar desde un teléfono de la empresa. En el mismo sentido se pronuncia la Sentencia de la *Cour de Cassation* de 15 de mayo de 2001, al establecer que «la surveillance des numéros de téléphone appelés constitue, si cette surveillance est dissimulée, une surveillance illicite, portant atteinte à la liberté individuelle d'un salarié».

No obstante, la jurisprudencia francesa no excluye de raíz la licitud de las intervenciones telefónicas. Al respecto, la recién citada Sentencia de la *Cour de Cassation* de 15 de mayo de 2001, admite que el empresario pueda intervenir las llamadas para controlar a los trabajadores, pero solo concurriendo una serie de presupuestos. Estos presupuestos son los siguientes: en primer lugar, que la intervención se realice durante el tiempo de trabajo; de otro lado, se requiere obtener un comunicado de France Telecom; en tercer lugar, debe hacerse de manera lícita y, por último, debe comunicarse al trabajador. Concurriendo estos presupuestos cabe la posibilidad de control por parte del empresario y, en caso contrario, la prueba no será admitida en el juicio.

Toca ahora hablar de la cuestión de la «cibervigilancia». No existe tampoco en Francia un cuerpo de normas que traten específicamente este problema, de suerte que el control informático en el trabajo se rige principalmente por leyes que regulan la vigilancia con carácter general. De nuevo resulta importante aquí el citado artículo L.121-8 del *Code du Travail*, que impone al empresario la obligación de informar a los trabajadores, con antelación, sobre cualquier medida de control que vaya a adoptar, de modo que ninguna información relativa a los mismos pueda ser recogida sin que se les haya informado previamente.

En aplicación de dicho artículo, los Tribunales franceses han venido autorizando la «cibervigilancia» únicamente en los casos en que el trabajador haya sido informado, no solo de la vigilancia, sino también de su naturaleza y alcance.

En cuanto a la doctrina judicial, la *Cour de Cassation* abordó esta cuestión en el caso «Nikon» de 2 de octubre de 2001. En relación a este supuesto, en el que el empleador había abierto un correo electrónico privado del trabajador, la Corte sentó como principio general que «el trabajador tiene derecho, también durante el tiempo de trabajo y en el lugar de trabajo, a un respeto de su vida privada; que ello implica en concreto el secreto a la correspondencia; que el empresario no puede por consiguiente, sin violar este derecho fundamental, examinar correos electrónicos enviados y recibidos por un trabajador a través del ordenador puesto a su disposición

como herramienta de trabajo, y ello se aplica incluso si el empresario ha prohibido el uso extra-profesional del ordenador»¹¹.

A la vista de lo mencionado en materia de legislación y en la sentencia, podría tener lugar una paradoja, consistente en que los empresarios legalmente pueden ordenar a los trabajadores no hacer un uso privado de los ordenadores, pero en ningún caso pueden abrir los correos electrónicos privados que los trabajadores pueden enviar o recibir incumpliendo la citada orden. En este sentido, se ha de entender, a juicio de Christophe VIGNEAU, que «el hecho de que la *Cour de Cassation* prohíba a los empresarios abrir los correos electrónicos no les impide imponer sanciones disciplinarias a los trabajadores que transgredan la prohibición de hacer uso de los mismos para fines privados»¹². En opinión del citado autor, el alcance de tales prohibiciones y sanciones dependerá de las circunstancias, criterio similar al que rige en la jurisprudencia española. Así, un uso espontáneo, no abusivo, no acarrearía ninguna sanción al estar tolerado en la práctica en muchas empresas. En cambio, el uso habitual de los medios informáticos para fines privados autorizará al empresario a despedir al trabajador, tal y como sucedió, por ejemplo, en el caso de un trabajador que, según quedó constatado, había estado apostando regularmente a través de Internet. Por tanto, el hecho de que la gravedad de la sanción disciplinaria a imponer esté en consonancia con la intensidad o duración del uso privado de Internet pone de manifiesto la virtualidad en la jurisprudencia francesa del principio de proporcionalidad.

b) La codeterminación alemana.

Las principales fuentes del Derecho Laboral alemán son la legislación federal, los convenios colectivos, los convenios de empresa y la jurisprudencia. No existe un código del trabajo refundido; se establecen normas laborales mínimas en diferentes leyes sobre diversas cuestiones relacionadas con el trabajo, que se complementan con las ordenanzas gubernamentales.

Con respecto a la vigilancia laboral, queda en el derecho alemán sujeta a la codeterminación. Günter SCHAUB explica que la codeterminación es un «acuerdo laboral» entre el empresario y los órganos de representación de los trabajadores, que ostenta un efecto jurídicamente vinculante (excepto cuando propicie una violación del derecho a la personalidad)¹³. En virtud de ello, la jurisprudencia del Tribunal Laboral Federal Alemán ha dispuesto como prohibida la instalación unilateral de cámaras ocultas por parte del empresario, incluso cuando la instalación ha sido dada a conocer a través de un anuncio general (Sentencia 15 de mayo de 1991, publicada en *Entscheidungen des Bundesarbeitsgericht*, 68, 1994, 52). Esta doctrina se basa en la lógica o en la idea de que el empresario no puede sustituir una vigilancia realizada con presencia física por la instalación de un sistema audiovisual, ya que con ello se crearía una impresión de constante vigilancia de la cual un trabajador no puede deshacerse. Además, no solamente se habla de grabaciones efectivas, sino que, incluso una sentencia (concretamente la Sentencia de 25 de julio de 1998, *ArbG Dortmund*, con publicación en

¹¹ VIGNEAU, CHRISTOPHE: «El Derecho francés», *Revista Aranzadi de Derecho y Nuevas Tecnologías*, número 1, 2003, 185-212, pág. 190.

¹² VIGNEAU, CHRISTOPHE: «El Derecho francés...», pág. 192.

¹³ FINKIN, MATTHEW, W.: «Menschenbild: la noción del trabajador como persona en el Derecho occidental», *Revista Aranzadi de Derecho y Nuevas Tecnologías*, número 1, 2003, 405-453, cita 679 en la pág. 411.

Computer Und Recht, 25, 1989, 715) declaró que la instalación de cámaras puede violar el derecho de la personalidad o intimidad incluso cuando estas no están funcionando o grabando ¹⁴.

Como se puede observar, las diferencias con la legislación y jurisprudencia española son evidentes. De un lado, se emplea el método de la codeterminación, que implica un consenso entre empresario y representantes de los trabajadores sobre las medidas a adoptar. En este método se apoya THIBAUT cuando propone para el sistema español la *concertación ex ante*. La virtualidad de la codeterminación en la jurisprudencia alemana conlleva la exclusión de plano de las medidas de control implementadas unilateralmente por el empresario, incluso en los casos en que aquellas sean puestas en conocimiento de todos mediante anuncios generales.

De otro lado, los tribunales germanos rechazan en cualquier caso de raíz los métodos de videovigilancia, incluso cuando las cámaras no estén en funcionamiento, en tanto en cuanto entienden que suponen un agravio innecesario al trabajador que conculca su derecho a la intimidad.

En lo referente al control mediante equipos informáticos, cabe decir antes que nada que, a pesar de la preferencia otorgada a los derechos de los trabajadores en el derecho alemán, el empresario no está obligado a permitir un uso privado de sus equipamientos, pudiendo imponer, en caso de permitirlo, condiciones distintas a los diferentes trabajadores, siempre y cuando existan motivos que justifiquen dicha desigualdad de trato. De otro lado, los empresarios no pueden tener acceso al contenido de los correos electrónicos o a las actividades en Internet de sus trabajadores sin que los mismos hayan sido informados de esta posibilidad de antemano. Por lo general, esta exigencia queda cumplida si el empresario realiza un anuncio general de la posibilidad de llevarse a cabo tales controles. *A sensu contrario*, en el derecho español, como se ha visto, los tribunales admiten el control sin mediar aviso en aquellos casos en los que existan fundadas sospechas de la existencia de irregularidades en el desempeño del puesto de trabajo y aquel se realice de la forma menos gravosa posible al empleado.

Volviendo al derecho alemán, y siguiendo el hilo de lo anterior, en caso de que el empleador desee controlar las actividades de los asalariados porque tenga sospechas de que se está haciendo un uso incorrecto de los equipos informáticos, los representantes de los trabajadores poseen determinadas facultades, habida cuenta que en los procedimientos de despido disciplinario los empresarios no podrán aportar ninguna prueba obtenida sin el consentimiento de aquellos (a diferencia del derecho español, donde el empresario puede omitir el aviso a los representantes, por el temor justificado de que tal aviso frustre la medida de control). Esta interdicción se basa en el influjo de la codeterminación, extendida por el Tribunal Laboral Federal a los casos de control de equipos informáticos.

En cuanto a la naturaleza y alcance del control, procede decir que cuando el empresario autorice el uso privado de los equipos de comunicación, podrá registrar la duración de las comunicaciones, pero no podrá controlar los contenidos de las mismas. De hecho, el trabajador tiene derecho a cifrar sus mensajes privados. Por otro lado, en caso de que el empresario no autorice el uso privado estará legitimado para instalar mecanismos, tales como filtradores, a efectos de hacer cumplir esta prohibición ¹⁵.

¹⁴ FINKIN, MATTHEW W.: «Menschenbild: la noción ...», págs. 411-412.

¹⁵ REINHARD, HANS-JOACHIM: «El Derecho alemán», *Revista Aranzadi de Derecho y Nuevas Tecnologías*, número 1, 2003, 213-239, pág. 230.