REVISTA ELECTRÓNICA
DE ACCESO ABIERTO
ISSN 2282-2313

Revista Internacional y Comparada de

RELACIONES LABORALES Y DERECHO DEL EMPLEO

ADAPT
www.adapt.it
UNIVERSITY PRESS

Revista Internacional y Comparada de RELACIONES LABORALES Y DERECHO DEL EMPLEO

Escuela Internacional de Alta Formación en Relaciones Laborales y de Trabajo de ADAPT

Trabajadores "transparentes": la facultad fiscalizadora del empresario *vs* derechos fundamentales de los empleados (I)[*]

Carolina BLASCO JOVER[**]

RESUMEN: El trabajo, dividido en dos partes, procede al estudio del impacto que ha tenido sobre la facultad fiscalizadora del empresario y los derechos fundamentales del trabajador la introducción en la empresa de las tecnologías de la información y de la comunicación. Así, en esta primera parte, se abordan dos problemáticas que han tenido eco en la jurisprudencia del Tribunal Europeo de Derechos Humanos. Por un lado, la monitorización de los medios informáticos puestos a disposición del empleado. Por otro, el control del trabajador a través de los sistemas de videovigilancia. De ambas cuestiones se dará cumplida cuenta en este trabajo, analizándose cuáles son exactamente los derechos confrontados y las soluciones a adoptar para alcanzar el adecuado equilibro entre los intereses en juego.

Palabras clave: Poder de dirección, medios informáticos, control, derechos del trabajador, video vigilancia.

SUMARIO: 1. A modo de introducción. 2. La monitorización de los medios tecnológicos e informáticos puestos a disposición del empleado. 2.1. La facultad fiscalizadora del empresario: justificación. 2.2. La jurisprudencia del Tribunal Supremo: la necesidad de establecer una política de uso de medios informáticos y su alcance. 2.3. La doctrina del Tribunal Constitucional: la devaluación del juicio de proporcionalidad. 2.4. Las sentencias del Tribunal Europeo de Derechos Humanos: hacia una mayor rigurosidad en el examen de la medida fiscalizadora empresarial. 2.5. La STS de 8 de febrero de 2018: ¿realmente Barbulescu II no añade "nada sustancial" a la doctrina tradicional del Tribunal Supremo? 3. El control a través de videovigilancia: la STEDH de 9 de enero de 2018 (caso López Ribalda y otras *vs* España) y su confrontación con la doctrina constitucional. 4. Bibliografía.

[*] El presente trabajo ha sido elaborado en el marco del proyecto de investigación "Digitalización y Trabajo: el impacto de la economía 4.0 sobre el empleo, las relaciones laborales y la protección social" (DER2017-82444-R).

[**] Profesora Contratada Doctora (Titular acreditada) Departamento Derecho del Trabajo y de la Seguridad Social de la Universidad de Alicante.

"Transparent" workers: employers' supervisory powers *vs* employees' fundamental rights (I)

ABSTRACT: In this study, we examine the impact of information and communication technologies on employers' supervisory power and workers' fundamental rights. The work is divided into two parts. In this first part, we address two issues that have resonated in the European Court of Human Rights' case law: the monitoring of IT resources made available to employees and worker control through video surveillance systems. Both issues are reviewed in depth as we analyse which specific rights are affected as well as the solutions to achieve an adequate balance between the interests at stake.

Key Words: Management power, IT resources, control, workers' rights, labour rights, video surveillance.

1. A modo de introducción

Sin lugar a dudas, la implantación de la digitalización en las empresas ha tenido un fuerte impacto en las relaciones laborales. No sólo es que las nuevas tecnologías de la información y de la comunicación hayan facilitado y optimizado con mucho el proceso productivo empresarial, sino que las consecuencias de ello ya se han hecho notar en los trabajadores y en su vida profesional y personal. De hecho, de acuerdo con un reciente informe de Eurofound-OIT del año 2017[1], los profundos cambios tecnológicos ya estarían provocando un alargamiento de la jornada laboral, una mayor intensidad de trabajo o la intromisión del trabajo remunerado en los espacios y tiempos normalmente reservados para la vida personal, con lo que ello implica para la conciliación de la vida laboral con la personal y la familiar. Y ello sin olvidar, que es lo aquí nos interesa, que la simple utilización del ordenador de la empresa, del teléfono móvil del trabajo o de la tableta, de las redes sociales o del correo electrónico permiten acumular una ingente cantidad de datos, personales y profesionales, del trabajador que, valorados en su conjunto, permiten al empresario hacerse una idea bastante fiable del perfil de empleado que tiene en su plantilla, de sus opiniones, comportamientos laborales y personales y opciones de vida. El trabajador se vuelve "transparente"[2] entonces para su empresario y, en este punto, es donde se puede plantear -y de hecho, se plantea- el conflicto entre la facultad fiscalizadora del empresario y los derechos fundamentales del trabajador, principalmente la intimidad (art. 18.1 CE), pero también el secreto de las comunicaciones (art. 18.3 CE), el derecho al honor o a la propia imagen (art. 18.1 CE).

Dónde acabe una y empiecen los otros es una cuestión problemática que en absoluto es extraña en sede judicial, habiendo sido resuelta tradicionalmente con la aplicación al caso del criterio de proporcionalidad y últimamente con el de la "expectativa razonable de confidencialidad". No obstante, con la incorporación de instrumentos de control tecnológicamente avanzados que refuerzan el poder de vigilancia empresarial y, por ende, su facultad sancionadora, no está de más cuestionarse acerca de si deben exigirse, como así parece plantear el

[1] Disponible en http://www.ilo.org/travail/whatwedo/publications/WCMS_544226/lang--es/index.htm.

[2] Sobre este concepto, vid. Mercader Uguina, J., *El futuro del trabajo en la era de la digitalización y la robótica*, Valencia, Tirant lo Blanch, 2018, pp. 121-126 y Rodríguez Escanciano, S., *El derecho a la protección de datos personales de los trabajadores: nuevas perspectivas*, Albacete, Bomarzo, 2009, pp. 65-69.

Tribunal Europeo de Derechos Humanos, unos controles más estrictos que sirvan de contrapeso a la cada vez más invasiva capacidad fiscalizadora empresarial. Este trabajo, dividido en dos partes, pretende profundizar sobre el tema, tratando de situar adecuadamente los fallos de las últimas sentencias dictadas sobre el particular. En esta primera parte, se abordará, de un lado, la monitorización de los medios informáticos puestos a disposición del empleado y, de otro, el control del trabajador a través de los sistemas de videovigilancia. De ambas cuestiones se dará cumplida cuenta en este trabajo, analizándose cuáles son exactamente los derechos confrontados y las soluciones a adoptar para alcanzar el adecuado equilibro entre los intereses en juego.

2. La monitorización de los medios tecnológicos e informáticos puestos a disposición del empleado

2.1. La facultad fiscalizadora del empresario: justificación

Como es bien sabido, a través del contrato de trabajo se formaliza jurídicamente la desigualdad real que en el plano económico existe entre el empresario y el trabajador. El poder que la mera realidad económica otorga al empresario se legitima por medio del contrato, en el que el trabajador, ajeno a los medios de producción y a los resultados de su trabajo, acepta de antemano una relación de dependencia a cambio de un salario.

Pero, además, el contrato implica habitualmente la incorporación del trabajador a una organización productiva, la empresa. El reconocimiento de ésta como institución básica del sistema y la atención que se le dispensa para que sea rentable añade a la situación de subordinación del trabajador nuevos elementos de supeditación jurídica, manifestaciones de poderes empresariales que se basan en presupuestos jurídicos ajenos y anteriores al contrato mismo. Tales presupuestos hay que buscarlos, evidentemente, en la consagración en nuestro texto constitucional de la libertad de empresa en el marco de una economía libre de mercado; libertad que, además de dar carta de naturaleza al empresario, en cuanto propietario de los medios de producción, le otorga un genérico poder dirigido a lo que se viene llamando "organización del trabajo en la empresa". Se trata de un poder de organización o de dirección, en sentido amplio, que es intrínseco a la figura del empresario y, por ende, irrenunciable. Y se manifiesta a través de una serie de específicos poderes, facultades o derechos mediante los cuales el ordenamiento se encarga de articular su ejercicio, bien referido a

la organización general del trabajo (estableciendo políticas de contratación, clasificación profesional, salariales, de control de la actividad, de ordenación del tiempo de trabajo, de prevención de riesgos laborales, etc.), bien dirigido a disponer de las concretas obligaciones contractuales (mediante su determinación, modificación, suspensión o extinción de las mismas).

Ligado, pues, a ese poder de dirección empresarial, se encuentran los poderes de vigilancia y control de la actividad laboral, poderes cuyo ejercicio siempre ha generado cierta controversia judicial por su más que probable choque con los derechos fundamentales del trabajador. En relación con esta facultad, el art. 20.3 del Estatuto de los Trabajadores (en adelante, 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 y teniendo en cuenta, en su caso, la capacidad real de los trabajadores con discapacidad". La aplicación de este precepto[3] y de los mecanismos de control que, en su virtud, se puedan desplegar, requiere la búsqueda de un equilibrio entre todos los derechos e intereses en juego; equilibro, ello no obstante, que, en numerosas ocasiones, es difícil de alcanzar, como se ha demostrado cuando del control de los instrumentos tecnológicos e informáticos propiedad de la empresa se trata habida cuenta del nivel de litigiosidad alcanzado.

Así las cosas, resulta obligado plantearse cuáles son las pautas o criterios que deben seguirse para verificar que la actuación empresarial en este contexto es ajena a cualquier lesión de los derechos fundamentales del trabajador. Tales pautas no las encontramos en la normativa, puesto que, más allá de las previsiones contenidas en algunos convenios o códigos de conducta, no existe precepto legal alguno que regule específicamente el uso por parte de los trabajadores de los medios tecnológicos e informáticos (ordenadores, correo electrónico, tabletas, smartphones, Whatsapp, Intranet, redes sociales) propiedad de la empresa. Por lo tanto, debe acudirse a la jurisprudencia y doctrina constitucional y europea para dilucidar cómo y con qué alcance las empresas pueden fiscalizar legítimamente tales instrumentos y la utilización, profesional o personal, que los trabajadores realicen de ellos[4].

[3] Y no del art. 18 ET, pues éste se refiere a los registros sobre la persona del trabajador, en sus taquillas y efectos particulares y no a los medios propiedad de la empresa sobre los que el empleador ostenta lógicamente facultades de control sobre su utilización, que incluyen también su examen (STS de 26 de septiembre de 2007, Rec. n. 966/2006).

[4] Ya advertido por Sala Franco, T., "El derecho a la intimidad y a la propia imagen y las

2.2. La jurisprudencia del Tribunal Supremo: la necesidad de establecer una política de uso de medios informáticos y su alcance

En la importante sentencia del Tribunal Supremo de 26 de septiembre de 2007 (Rec. n. 966/2006), en la que se resuelve sobre el uso personal del ordenador y de la red de Internet de la empresa para navegar por páginas poco seguras y absolutamente ajenas al ámbito profesional, se sienta la base de que existe un hábito social generalizado de tolerancia con el uso personal moderado de los medios informáticos facilitados por la empresa y que esa situación de tolerancia genera una expectativa razonable de intimidad o confidencialidad para el trabajador; expectativa de intimidad, por cierto, que no sólo se extendería al correo electrónico, sino también a los archivos personales del trabajador e, incluso, a los archivos temporales por poderse contener en ellos informaciones reveladoras sobre determinados aspectos de la vida privada del trabajador (ideología, orientación sexual, aficiones personales, afinidades políticas, etc.).

En consecuencia, si el empresario quiere controlar el uso del ordenador por parte del trabajador, debe establecer previamente las reglas de uso de esos medios (con prohibiciones absolutas o parciales) e informar a los trabajadores de que va existir control y de los medios que se van a utilizar, así como de las medidas que se adoptarán para garantizar la efectiva utilización laboral del medio.

Lógicamente, de esta doctrina deriva una consecuencia lógica: si, a pesar de todo, el ordenador (o, por extensión, cualquier instrumento tecnológico propiedad de la empresa) se utiliza para usos privados en contra de las prohibiciones impuestas y con conocimiento de los controles y medidas aplicables, no podrá entenderse que se ha vulnerado la expectativa razonable de intimidad del trabajador. Pero es que, además, esta sentencia supone que entrará en juego otro criterio, más allá del consabido juicio de proporcionalidad, para ponderar si el empresario ha hecho un uso lícito de su facultad de fiscalización: la calidad y la cantidad de la información o de las instrucciones que haya suministrado a sus empleados sobre el particular. Ello quiere decir que no procederá un examen excesivamente rigorista de los medios de vigilancia empleados si el empresario ha cumplido proporcionando una completa información

nuevas tecnologías de control laboral", en AA.VV., *Trabajo y libertades públicas,* Madrid, La Ley, 1999, p. 205.

sobre el uso que puede o no puede hacerse de los instrumentos informáticos y tecnológicos de su propiedad. Y, al contrario: de no mediar tal información o no de ser lo suficientemente clara o precisa, el control sobre la facultad fiscalizadora del empresario deberá ser más severo y concluir seguramente en la intromisión ilegítima a la intimidad del trabajador y, en su caso, en la consideración como nula de la prueba obtenida y llevada a juicio.

Esta doctrina se consolida en sentencias de 8 de marzo (Rec. n. 1826/2010) y 6 de octubre de 2011 (Rec. n. 4053/2010), siendo ésta última la que introduce una matización que conviene apuntar por el paso adelante que comporta. Así, se señala expresamente que la terminante prohibición de uso personal de los medios informáticos implica que ya no exista tolerancia empresarial y que decaiga para el trabajador la expectativa razonable de intimidad de la que antes se ha hablado. Y ello con independencia -y aquí viene la salvedad- del nivel o de la calidad de la información que la empresa haya podido proporcionar sobre el control de los medios y el alcance de la monitorización. De este modo, del simple hecho de que exista una prohibición absoluta de utilización personal de tales instrumentos cabrá extraer que puedan estar lícitamente sometidos a la vigilancia empresarial y que si el trabajador, a pesar de todo, los utiliza para fines personales, debe ser consciente que no le ampara garantía de confidencialidad alguna.

2.3. La doctrina del Tribunal Constitucional: la devaluación del juicio de proporcionalidad

El planteamiento que antecede fue acogido por el Tribunal Constitucional, que pasó de exigir que la medida de fiscalización empresarial superara el triple juicio de proporcionalidad para ser considerara legítima (SSTC 292/1993, de 18 de octubre y 98/2000, de 10 de abril) a reforzar las posibilidades de control y vigilancia y favorecer, así, la posición empresarial. Así, se dictamina, en sentencia 241/2012, de 17 de diciembre, que la prohibición de instalar programas informáticos en el ordenador de la empresa implica, por derivación, que quede prohibido el uso personal de este instrumento y que, en consecuencia, decaiga para el trabajador toda expectativa razonable de intimidad y se admita la injerencia empresarial en los mensajes[5]. Por otro lado, la sentencia

[5] Como señala el Tribunal, "la prohibición expresa de instalar programas en el ordenador de uso común se conculca por la recurrente y otra trabajadora, quienes instalaron el

170/2013, de 7 de octubre, da un paso más allá (criticable a mi modo de ver por la situación de vulnerabilidad en la que deja al trabajador)[6] y señala que basta con que el convenio colectivo aplicable señale que "el correo electrónico es de exclusivo uso profesional" y sancione su utilización para fines personales para que resulte legitimada la monitorización del sistema sin mediar información o comunicación alguna sobre las reglas de uso y control de las herramientas informáticas propiedad de la empresa[7].

En cualquier caso y antes de entrar en las importantes sentencias dictadas por el Tribunal Europeo de Derechos Humanos, conviene hacer referencia a la matización introducida por la STS, Sala de lo Penal, de 16 de junio de 2014 (Rec. n. 2229/2013) en la que se resolvía sobre un posible acto delictivo llevado a cabo por el trabajador y sobre la validez

programa de mensajería instantánea denominado *Trillian*. Por tanto, no existiendo una situación de tolerancia a la instalación de programas y, por ende, al uso personal del ordenador, no podía existir una expectativa razonable de confidencialidad derivada de la utilización del programa instalado, que era de acceso totalmente abierto y además incurría en contravención de la orden empresarial" (Fundamento Jurídico n. 6). A partir de este presupuesto, se niega el carácter secreto de las comunicaciones controvertidas y se admite la injerencia empresarial en los mensajes, descartándose la vulneración del art. 18.3 CE y también del art. 18.1 CE, porque fueron las propias trabajadoras quienes realizaron actos dispositivos que determinaron la eliminación de la privacidad de sus conversaciones. La sentencia, con todo, cuenta con un voto particular que discrepa del sentir mayoritario de la Sala y en el que se señala que "la trasgresión de una orden empresarial de prohibición de instalación de sistemas de mensajería electrónica o de empleo de los existentes para un fin ajeno a la actividad laboral, no habilita en modo alguno interferencias en el proceso o en el contenido de la comunicación, sin perjuicio de que pueda acarrear algún tipo de sanción. En otros términos, la infracción de las ordenes empresariales tolera la imposición de las sanciones previstas en el ordenamiento jurídico, pero ni consiente la vulneración directa de derechos fundamentales al amparo del incumplimiento de la orden empresarial, ni tampoco las intromisiones empresariales enderezada a verificar o comprobar la existencia de las comunicaciones".

[6] En el mismo sentido, Terradillos Ormaetxea, E., "El principio de proporcionalidad como referencia garantista de los derechos de los trabajadores en las últimas sentencias del TEDH dictadas en materia de ciberderechos: un contraste con la doctrina del Tribunal Constitucional español", *Revista de Derecho Social*, n. 80, 2017, p. 156.

[7] Señala así el Tribunal que "la expresa prohibición convencional del uso extralaboral del correo electrónico y su consiguiente limitación a fines profesionales llevaba implícita la facultad de la empresa de controlar su utilización, al objeto de verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, incluida la adecuación de su prestación a las exigencias de la buena fe. En el supuesto analizado la remisión de mensajes enjuiciada se llevó, pues, a cabo a través de un canal de comunicación que, conforme a las previsiones legales y convencionales indicadas, se hallaba abierto al ejercicio del poder de inspección reconocido al empresario; sometido en consecuencia a su posible fiscalización, con lo que quedaba fuera de la protección constitucional del art. 18.3 CE" (Fundamento Jurídico n. 4).

penal de una prueba consistente en el registro del correo electrónico corporativo de aquél.

En esta sentencia, la Sala parte de la base de que el art. 18.3 CE es claro y tajante cuando afirma que sólo por resolución judicial puede decaer el secreto de las comunicaciones, no contemplando el precepto "ninguna posibilidad ni supuesto, ni acerca de la titularidad de la herramienta comunicativa (ordenador, teléfono, etc. propiedad de tercero ajeno al comunicante), ni del carácter del tiempo en el que se utiliza (jornada laboral) ni, tan siquiera, de la naturaleza del cauce empleado (correo corporativo), para excepcionar la necesaria e imprescindible reserva jurisdiccional en la autorización de la injerencia". Siendo ello así, se concluye que, a los estrictos efectos del ámbito penal, "para que pueda otorgarse valor y eficacia probatoria al resultado de la prueba consistente en la intervención de las comunicaciones protegidas por el derecho consagrado en el artículo 18.3 de la Constitución, resultará siempre necesaria la autorización e intervención judicial". Requisito éste de la autorización, no obstante, que no será necesario respecto de "los denominados datos de tráfico, de la posible utilización del equipo informático para acceder a otros servicios de la red como páginas web o de los mensajes una vez recibidos y ya abiertos por su destinatario".

Parece, por tanto, que esta resolución vendría a perfilar aún más la potestad fiscalizadora del empresario, recortando sus posibilidades de control sobre el correo electrónico del trabajador. De hecho, podría derivarse que la apertura por el empresario de un mensaje que todavía estuviera en la bandeja de entrada sin leer constituiría un delito penal, habida cuenta de que ese mensaje estaría todavía en curso a su destinatario y, por ello, protegido por el secreto de las comunicaciones. Consecuencia lógica de ello sería que el empresario, si quisiera acometer tal actuación, debería solicitar, siempre y en todo caso, la necesaria autorización judicial.

No entiendo, ello no obstante, que el fallo de esta sentencia tenga que interpretarse de este modo. Al decir de la Sala, su razonamiento lo es a los efectos del procedimiento penal, no, por tanto, a los del social, por lo que parece más razonable sostener que sólo si la infracción cometida por el trabajador excediera del ámbito laboral para pasar a constituir una posible infracción penal, habría de requerirse la intervención judicial. Defender lo contrario y requerir autorización judicial previa para que se pueda fiscalizar el uso que los trabajadores dan a los medios propiedad de la empresa quizá sería tanto como vaciar de contenido la facultad de vigilancia y control empresarial consagrada en el art. 20.3 ET[8].

[8] Del mismo parecer, Mercader Uguina, J., *El futuro del trabajo en*…, *op. cit.*, p. 150 y

2.4. Las sentencias del Tribunal Europeo de Derechos Humanos: hacia una mayor rigurosidad en el examen de la medida fiscalizadora empresarial

Siguiendo con este *iter* jurisprudencial, cabe detenerse ahora en la doctrina acogida por el Tribunal Europeo de Derechos Humanos, que ha dictado en poco espacio de tiempo dos sentencias contrarias entre sí, enmendando la segunda a la primera. Así, en la sentencia de 12 de enero de 2016 (Barbulescu I), se enjuiciaba, como ya es conocido, la validez de un despido producido a consecuencia de un uso personal de un conocido sistema de mensajería instantánea instalado en el ordenador de la empresa y la legitimidad de la monitorización del medio llevada a cabo por el empresario sin advertírselo previamente al trabajador y llegándose a divulgar mensajes privados a terceros. El trabajador demandó a la empresa ante los Tribunales del país (Rumania) por considerar vulnerados sus derechos al secreto de las comunicaciones y a la intimidad. No obstante, tanto el juez de instancia como el Tribunal superior le negaron su amparo por considerar, básicamente, que la existencia de una prohibición de uso de los medios telemáticos de la empresa para fines personales legitiman *per se* la vigilancia empresarial, siendo este método el único posible para comprobar si los trabajadores cumplen con su labor.

En estas circunstancias, el trabajador plantea demanda ante el Tribunal Europeo de Derechos Humanos por considerar vulnerado el art. 8 del Convenio Europeo de Derechos Humanos (CEDH), que sanciona el derecho de toda persona "al respeto de su vida privada y familiar, de su domicilio y de su correspondencia". No obstante, el Tribunal, tras examinar la procedencia de la demanda, confirma las tesis de los Tribunales nacionales sobre la base de que, existiendo una normativa de uso de los medios conocida por el trabajador, éste no puede tener una expectativa razonable de intimidad, no puede esperar, en fin, que sus conversaciones no sean auditadas.

La sentencia, como puede comprobarse, va en la línea de las resoluciones dictadas por el Tribunal Supremo y el Tribunal Constitucional anteriormente citadas al reforzar el poder de control del empresario y debilitar la posición del trabajador. Ahora bien, aunque no es lugar para realizar un detallado y exhaustivo análisis de esta resolución, sí cabe

Molina Navarrete, C., "Expectativa razonable de privacidad y poder de vigilancia empresarial: ¿*quo vadis* justicia laboral?", *Estudios Financieros,* n. 399, 2016, p. 180.

detenerse siquiera en dos cuestiones que merecen resaltarse.

Por lo pronto, la misma sentencia arroja dudas acerca de la implementación en la empresa de una correcta y completa política de uso de los medios telemáticos puestos a disposición del trabajador que informe debidamente de la existencia de un control y del alcance del mismo; pero, ello no obstante, el Tribunal prefiere no entrar en ello y sostener que la expectativa razonable de intimidad del trabajador decae ante la existencia de una mera prohibición genérica de uso personal, reconociéndose así una suerte de derecho del empleador, general y abstracto, a monitorizar los medios telemáticos de su propiedad[9].

Por otro lado, señala el Tribunal que la actuación empresarial fue proporcionada en atención al fin perseguido (demostrar el incumplimiento laboral del trabajador) porque la monitorización se ciñó al examen de las comunicaciones del trabajador, pero no a otros datos y documentos almacenados en el ordenador. Ciertamente, no se puede estar más de acuerdo con quien opina que este criterio no es en absoluto consistente, porque el respeto, por así decirlo, a los demás archivos y documentos existentes no excluye que puedan cometerse actos de injerencia ilegítima en las comunicaciones de mensajería del trabajador[10].

Esta sentencia es enmendada por otra de la Gran Sala del TEDH dictada el 5 de septiembre de 2017 como consecuencia de la petición de reenvío del asunto por parte del demandante y que viene a ser conocida como Barbulescu II. La sentencia parte del presupuesto de que el trabajador no fue convenientemente informado acerca de la política de uso de los medios tecnológicos puestos a su disposición por la empresa ni de la extensión del posible control sobre ellos; control, todo hay que decirlo, que el Tribunal considera legítimo para asegurar el buen funcionamiento de la empresa.

No obstante y en cualquier caso, lo que viene a afirmar la sentencia es que la mera existencia de una prohibición de uso de los medios telemáticos de la empresa para fines personales no deben legitimar *per se* la vigilancia empresarial. De este modo, para proceder a la fiscalización de estos medios es necesario, según el TEDH, que los Tribunales naciones evalúen

[9] Muy crítico con ello Molina Navarrete, C., "Expectativa razonable de…", *op. cit.*, pp. 176 y 177.

[10] Goñi Sein, J.L., "La vigilancia empresarial de las comunicaciones electrónicas de los trabajadores", *Trabajo y Derecho*, n. 18, 2016, p. 3 (versión *on line*). De la misma opinión es el juez que emite el voto particular de la sentencia, quien considera que la actuación fiscalizadora empresarial fue desproporcionada al divulgarse a terceros los mensajes privados del trabajador y al tener esta decisión efectos indirectos drásticos en su vida personal y social.

si la medida empresarial supera el siguiente test:

a) Debe valorarse si existió una información previa y clara a los trabajadores de las medidas de control que pueden utilizarse, de su alcance y de su puesta en práctica.
b) Debe valorarse el grado de fiscalización empresarial y su extensión, tanto temporal como material.
c) Debe valorarse si existe un motivo legítimo que justifique la monitorización, al ser una medida invasiva e intrusiva.
d) Debe juzgarse si existen otras medidas alternativas menos intrusivas y más respetuosas con la vida privada del trabajador y demás derechos fundamentales.
e) Debe evaluarse qué uso le da el empresario a los datos obtenidos como consecuencia de la monitorización y si ese uso es legítimo para conseguir la finalidad que se pretenda.
f) Deben existir garantías para el trabajador, de tal modo que si se accede al contenido de sus comunicaciones debe haber sido previamente notificado. Igualmente, ha de valorarse, en aras del principio de transparencia, si la medida de fiscalización se ha realizado al inicio del procedimiento sancionador y no después.

A la luz de estas pautas, el Tribunal llega a la conclusión de que la empresa, al controlar las comunicaciones del trabajador, vulneró el art. 8 CEDH. En primer lugar, porque el demandante no parece que hubiera sido informado con antelación "del alcance y de la naturaleza del control efectuado por la empresa o de la posibilidad de que la empresa tuviera acceso al contenido de sus comunicaciones". En segundo lugar, porque el grado de fiscalización fue excesivo, al registrar el empresario "en tiempo real todas las comunicaciones hechas por el demandante durante el período de vigilancia, que tuvo acceso a ellas y que imprimió el contenido". En tercer lugar, porque no se comprobó suficientemente por los Tribunales nacionales "la existencia de razones legítimas que justificaran el establecimiento de un control de las comunicaciones del trabajador". Tampoco se examinó suficientemente y en cuarto lugar, "si el objetivo perseguido podía haberse logrado mediante métodos menos intrusivos que el acceso al contenido mismo de las comunicaciones del demandante". Además y en quinto lugar, no se examinó "la gravedad de las consecuencias de la medida de control y del procedimiento disciplinario que se siguió". Finalmente, no se comprobó "si, cuando compareció el trabajador para que explicara el uso que había hecho de los recursos de la empresa, el empresario había tenido ya acceso al contenido de las comunicaciones en cuestión".

Ciertamente, con la plasmación de estos cánones, puede decirse que la

sentencia representa un punto de inflexión en la materia que nos ocupa, pues el control de los medios telemáticos debiera regirse ahora por unos estándares más estrictos que los aportados por el Tribunal Supremo y el Tribunal Constitucional, no siendo suficiente, en consecuencia, para destruir la expectativa de confidencialidad, la mera prohibición del uso del ordenador para fines personales. Así es, la doctrina del TEDH vuelve a recuperar el principio de proporcionalidad -quizá dejado a un lado por las sentencias nacionales antes comentadas- para juzgar la licitud de la medida fiscalizadora empresarial; y se recupera de una forma más rigurosa, exigiendo mayores y más estrictos condicionantes que, en mi opinión, juegan a favor de las dos partes del conflicto, trabajador y empresario, pues de lo que se trata es de buscar el mejor equilibrio entre los derechos e intereses de uno y de otro y de que ambos, en aras al principio de buena fe que debe regir en la relación laboral, sepan a qué atenerse[11]. Ello se consigue implementando, a través de los convenios colectivos, de los contratos o de los códigos de buenas conductas, una política de uso de los medios tecnológicos en la que se determine de forma previa[12], clara y concreta tanto los límites a los que deben sujetarse los trabajadores como el alcance y extensión, material y temporal, de la vigilancia que se quiera practicar y las posibles sanciones a aplicar. Una política, además, que será conveniente actualizar periódicamente o siempre que fuera necesario habida cuenta de la evolución tan rápida de las tecnologías de la información y de la comunicación[13].

La transparencia que debe regir en este asunto se erige, pues, en elemento fundamental para legitimar la facultad fiscalizadora del empresario. Tanto que, de faltar, parece meridianamente lógico entender que no tendría sentido continuar con el examen de legitimidad de la medida empresarial[14]. No obstante, y suponiendo que en el caso concreto exista esa transparencia que el TEDH reclama, también es relevante que se proporcionen razones suficientes que justifiquen la intromisión (no

[11] En sentido similar, Molina Navarrete, C., "El poder empresarial de control digital: ¿nueva doctrina del TEDH o mayor rigor aplicativo de la precedente?", *Ius Labor,* n. 3, 2017, p. 296.

[12] A salvo, obviamente, de los posibles controles extraordinarios que se quieran practicar por la sospecha de comisión de ilícitos (v. gr. hurtos, competencia desleal, revelación de secretos) y que la empresa, para garantizar su eficacia, habría de mantener en secreto.

[13] Sobre los rigores de la implementación de esta política de uso, puede leerse con mayor detalle Blázquez Agudo, E.Mª., *Aplicación práctica de la protección de datos en las relaciones laborales*, CISS-Wolters Kluwer, Madrid, 2018, pp. 173-175.

[14] De la misma opinión, Terradillos Ormaetxea, E., "El principio de proporcionalidad como…", *op. cit.*, pp. 146 y 147.

bastando, entonces, motivos abstractos o la mera conveniencia)[15] y que la medida que se adopte sea, dentro lo posible, la menos gravosa posible para el derecho fundamental afectado[16], recayendo la carga de la prueba sobre este hecho, a mi entender, en el empresario en aplicación del principio de disponibilidad y facilidad probatoria.

Por lo demás, no debe obviarse que en esta materia han de entrar en juego también las normas y principios contemplados en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, de reciente entrada en vigor. En la medida en que los sistemas de control empleados recogen y almacenan información o datos no sólo de carácter profesional, sino también de carácter personal del trabajador[17], será necesario que el empresario de, también, estricto cumplimiento a las exigencias propias de la protección de datos, entre ellas, la transparencia informativa por la que se le obliga a suministrar al trabajador la identidad y los datos de contacto del responsable del tratamiento y, en su caso, de su representante, los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento o el plazo durante el cual se conservarán los datos personales[18].

Con todo, no se desconoce que, en el curso de este año, concretamente el 22 de febrero de 2018, el TEDH ha dictado otra sentencia que parece entrar en contradicción con la sentencia Barbulescu II. En esta sentencia (caso Libert *vs* Francia), el Tribunal entra de nuevo a valorar si la fiscalización que efectúa el empresario en el ordenador del trabajador (aunque de propiedad de la empresa) vulnera el art. 8 CEDH.

---

[15] Se podría argumentar, por ejemplo, la introducción de virus en el sistema informático de la empresa, el bajo rendimiento de los empleados a causa de las distracciones, los costes económicos para la empresa, etc.

[16] Desde luego, no es lo mismo controlar el flujo de la información o el ancho de banda que consume el trabajador que el contenido de la información en sí, siendo éste último un método más gravoso para la intimidad del trabajador. No obstante, habrá determinados casos en los que, por las circunstancias concurrentes, el único modo de conocer si ha habido un uso personal y extralimitado del medio telemático sea conociendo el contenido de esos mensajes. Ciertamente, la medición del flujo de la información no permite comprobar qué tipo de uso, personal o profesional, se realiza del medio en sí. Sobre ello, vid. Desdentado Bonete, A. y Desdentado Daroca, E., "La segunda sentencia del TEDH en el caso Barbulescu y sus consecuencias sobre el control del uso laboral del ordenador", *Revista de Información laboral,* n. 1, 2018, p. 11 (versión *on line*).

[17] Resolución de la Agencia Española de Protección de Datos R/01755/2013.

[18] Entre otros y en el mismo sentido, Goñi Sein, J.L., "La vigilancia empresarial de…", *op. cit.*, p. 8.

En concreto, el caso que se plantea es el del despido de un trabajador del sector público que almacena en el ordenador de la empresa una serie de archivos, calificados como "personales", con material pornográfico y una serie de certificados falsos expedidos en favor de terceros. Los Tribunales franceses entendieron que no se había vulnerado el derecho a la intimidad del trabajador porque existía base legal para que el empresario procediera a la fiscalización del ordenador. Y es que según normativa interna francesa, el empresario puede acceder, en aras de su poder de control de la actividad laboral, a los ficheros que se encuentran en el ordenador de la empresa que utiliza el trabajador, a salvo de aquéllos que éste hubiese calificado como "privados". A ellos sólo podrá acceder previo consentimiento del trabajador o en su presencia. No siendo éste el caso (ya se ha dicho que el trabajador los había calificado de archivos "personales"), los Tribunales internos ratifican la decisión del empresario de fiscalizar el ordenador del trabajador sobre el entendimiento de que aquél tiene la legítima facultad de asegurarse que sus empleados utilizan los medios informáticos puestos a su disposición de acuerdo con las obligaciones contractuales y la normativa aplicable.

El conflicto llega al TEDH, quien, tras analizar los hechos, coincide con las autoridades judiciales nacionales en afirmar que el control efectuado por el empresario es totalmente lícito, justificado y proporcionado por las razones expuestas anteriormente (que para el Tribunal son "pertinentes y suficientes"). Añade, además, que el trabajador había contravenido de forma frecuente el código deontológico de la empresa, documento que contemplaba el uso profesional de los medios tecnológicos puestos a disposición de los empleados, pero que toleraba de manera puntual un uso personal de los mismos, lo que no sucedía en el presente caso[19].

Repárese en que la resolución parece seguir la línea de la sentencia Barbulescu I, en la que, si se recuerda, el Tribunal señalaba que la actuación empresarial fue proporcionada en atención al fin perseguido, que era demostrar el incumplimiento laboral del trabajador en aras al legítimo propósito del empresario de controlar el uso que le dan sus empleados a los medios tecnológicos puestos a su disposición. Ello no obstante, difiere, y esto es evidente, de los criterios sentados por la sentencia Barbulescu II, por lo que no es de extrañar que sea previsiblemente recurrida ante la Gran Sala con el fin de unificar doctrina.

Sea como fuere, lo cierto es que el TEDH, en esta última sentencia, ha sentado unos criterios más rigurosos y estrictos que los que venían

[19] Concretamente, el trabajador había almacenado 1562 archivos pornográficos que representaban un volumen de 787 megabytes durante un período de cuatro años.

aplicando los Tribunales españoles sobre el control por la empresa de los medios informáticos puestos a disposición de los trabajadores. Ello conduce irremediablemente a defender una reforma del art. 20.3 ET por la que se adapte su tenor, demasiado genérico y apoyado en conceptos muy amplios, tanto a la doctrina emanada por el TEDH (de aplicación a España por mor del art. 10.2 CE)[20] como a la nueva realidad tecnológica, en constante evolución[21]. Hasta que eso ocurra habrá que ver cómo aplican los jueces nacionales los más rigurosos estándares de evaluación que propone el Tribunal de Estrasburgo, lo que nos lleva al examen de la sentencia del Tribunal Supremo de 8 de febrero de 2018 (Rec. n. 1121/2015).

2.5. La STS de 8 de febrero de 2018: ¿realmente Barbulescu II no añade "nada sustancial" a la doctrina tradicional del Tribunal Supremo?

La sentencia de la Sala de lo Social del Tribunal Supremo de 8 de febrero de 2018, dictada en unificación de doctrina, se cuestiona sobre si la medida empresarial dirigida a revisar los correos electrónicos de un trabajador es acorde tanto con la doctrina fijada por el Tribunal Constitucional (particularmente en su sentencia 170/2013), como con la fijada por la Gran Sala del TEDH en su sentencia Barbulescu II[22].

En el supuesto de hecho enjuiciado, la empresa procede al despido disciplinario de un trabajador por la comisión de faltas muy graves tipificadas en el art. 54.2.d) ET (transgresión de la buena fe contractual y abuso de confianza)[23]; faltas de las que la empresa tuvo constancia a través

[20] También STC 155/2009, de 25 de junio.

[21] Petición también realizada, entre otros, por Casas Baamonde, Mª.E., "Informar antes que vigilar. ¿Tiene el Estado la obligación positiva de garantizar un mínimo de vida privada a los trabajadores en la empresa en la era digital? La necesaria intervención del legislador laboral", *Derecho de las Relaciones Laborales*, n. 2, 2018, p. 119.

[22] Por su trascendencia, se cita y explica esta sentencia del Tribunal Supremo. No obstante, no se desconoce que, anteriormente, el juzgado de lo social n. 19 de Madrid ya había tenido la oportunidad de aplicar los criterios de la sentencia Barbulescu II para la resolución del asunto que se le planteaba (sentencia JS n. 19 Madrid, de 17 de noviembre de 2017, Autos 737/2017).

[23] En concreto, se trataba de una vulneración del Código de Conducta y Prácticas Responsables de la empresa Inditex que señala, en uno de sus apartados, que "ningún empleado de Inditex podrá ofrecer, conceder, solicitar o aceptar, directa o indirectamente, regalos o dádivas, favores o compensaciones, en metálico o en especie, cualquiera que sea su naturaleza, que puedan influir en el proceso de toma de decisiones relacionado con el desempeño de las funciones derivadas de su cargo".

de un "hallazgo casual" por parte de otro empleado y que, para corroborarlas, toma la decisión de revisar los correos electrónicos del trabajador despedido, sin consentimiento ni conocimiento de éste, aportándolos como prueba al juicio. Cabe señalar que la empresa lleva a cabo este control en tanto que cuenta con una clara y concreta política de uso de los medios tecnológicos puestos a disposición de los trabajadores que limita el uso de los mismos "a los estrictos fines laborales" y prohíbe su utilización para cuestiones personales. Además, es de resaltar también el hecho de que cada vez que los trabajadores acceden con su ordenador a los sistemas informáticos de la compañía y de forma previa a ese acceso, deben aceptar las directrices establecidas en esa política de uso, en las que se vuelve a reiterar que "el acceso lo es para fines estrictamente profesionales, reservándose la empresa el derecho a adoptar las medidas de vigilancia y control necesarias para comprobar la correcta utilización de las herramientas que pone a disposición de sus empleados". Por lo tanto, en este concreto caso, se da la circunstancia de que el trabajador conocía, por partida doble, que no podía utilizar el ordenador para fines personales y que la empresa podía legítimamente fiscalizar su uso.

El control, por lo demás, se efectúa "examinando ciertos correos electrónicos de la cuenta de correo corporativo del trabajador, pero no de modo genérico e indiscriminado, sino tratando de encontrar elementos que permitieran seleccionar qué correos examinar, utilizando para ello palabras clave que pudieran inferir en qué correos podría existir información relevante para la investigación y atendiendo a la proximidad con las transferencias bancarias que se habían realizado a favor del trabajador".

Los Tribunales de instancia (Juzgado de lo Social n. 1 de A Coruña y TSJ de A Coruña) declararon procedente el despido efectuado. Ello no obstante, la sentencia del Tribunal Superior llega a considerar nulas las pruebas obtenidas a través del correo electrónico del trabajador (no el resto, las anteriores a ese momento) por entender que esta actuación empresarial vulneraba el derecho a la intimidad del trabajador y su derecho al secreto de comunicaciones.

Tanto la empresa como el trabajador recurren al Tribunal Supremo en unificación de doctrina. Ello no obstante, el recurso de la parte trabajadora no prospera en tanto que la Sala considera que no existe contradicción entre las sentencias de contraste aportadas y la sentencia recurrida del TSJ de A Coruña[24]. Distinta suerte corre el recurso de la empresa que aporta como sentencia de contraste la anteriormente

[24] *In extenso*, Fundamento Jurídico n. 2.

comentada (y criticada) STC 170/2013, de 7 de octubre. Si se recuerda, esta sentencia señala que basta con que el convenio colectivo aplicable contemple que "el correo electrónico es de exclusivo uso profesional" y sancione su utilización para fines personales para que resulte legitimada la monitorización del sistema sin mediar información o comunicación alguna sobre las reglas de uso y control de las herramientas informáticas propiedad de la empresa.

A partir de este punto, la Sala hace el ímprobo esfuerzo de salvar de alguna forma la doctrina plasmada en aquella sentencia y, al tiempo –y ello es lo controvertido de esta resolución–, de recuperar la aplicación del triple juicio de proporcionalidad, que entiende que nunca quedó desautorizado. De este modo, se sostiene, a la vista de las concretas circunstancias del caso enjuiciado, que es "palmario" que la doctrina ajustada a Derecho es "la mantenida por el Tribunal Constitucional en la exhaustiva decisión de contraste", que coincide "en algunos extremos con la previa jurisprudencia de esta Sala (así, SSTS 26 de septiembre de 2007, 8 de marzo de 2011 y 6 de octubre de 2011)".

Tras esta declaración, que ya augura cuál será el sentido del fallo (inexistencia de vulneración de derechos del trabajador), el Tribunal repasa algunos de los criterios ya señalados anteriormente: 1) que el poder de dirección del empresario es imprescindible para la buena marcha de la organización productiva (arts. 33 y 38 CE) y se reconoce en el art. 20.3 ET; 2) que en el marco de ese poder, no cabe duda que es admisible la ordenación y regulación del uso de los medios informáticos de titularidad empresarial por parte del trabajador, así como la facultad de vigilancia y control del cumplimiento de las obligaciones relativas a la utilización del medio en cuestión; 3) que los grados de intensidad o rigidez con que deben ser valoradas las medidas empresariales de vigilancia y control son variables en función de la propia configuración de las condiciones de disposición y uso de las herramientas informáticas y de las instrucciones que hayan podido ser impartidas por el empresario a tal fin; 4) que el uso del correo electrónico por los trabajadores en el ámbito laboral queda dentro del ámbito de protección del derecho a la intimidad y su ámbito de cobertura viene determinado por la existencia en el caso de una expectativa razonable de privacidad; 5) que, existiendo previsión colectivamente fijada sobre prohibición del uso del ordenador para fines personales, debe inferirse que sólo está permitido al trabajador el uso profesional del correo electrónico de titularidad empresarial y que la empresa puede ejercer legítimamente su facultad fiscalizadora por mor del art. 20.3 ET.

La Sala concluye, a la vista de todo lo anterior, que la actuación de la

empresa consistente en supervisar el correo electrónico del trabajador ha sido total y plenamente lícita, básicamente porque cuenta con una concreta y clara política de uso de los medios informático que prohíbe su uso no profesional, porque a los empleados se les recuerda este extremo cada vez que acceden a sus terminales, así como la posibilidad de la empresa de aplicar medidas de vigilancia y, en fin, porque el acceso al correo electrónico se realizó, no de forma indiscriminada, sino de una manera "ponderada" y cuidadosa, utilizando el servidor de la empresa y realizando la búsqueda a través de palabras clave y de la proximidad temporal de los mensajes. Y, en este punto, es donde la Sala recupera la aplicación del juicio de proporcionalidad que parecía haberse olvidado en las sentencias precedentes. En tanto que el control del correo electrónico se realizó de la manera descrita, se afirma que la actuación empresarial supera el juicio de idoneidad (con ella se consigue el objetivo propuesto de constatar un incumplimiento laboral), el juicio de necesidad (no había otra forma más moderada y con igual eficacia para la consecución de aquél propósito) y el juicio de proporcionalidad en sentido estricto (el control fue equilibrado y cauteloso).

La revitalización de este triple juicio para comprobar si la medida empresarial es legítima conduce al Tribunal, a su vez, a mostrarse coincidente con la doctrina sostenida por el TEDH en la sentencia Barbulescu II. De hecho, señala que "la conducta empresarial de autos pasa holgadamente el filtro de los requisitos que el Alto Tribunal europeo exige para atribuir legitimidad a la actividad de control que acabamos de enjuiciar", ya que "las consideraciones del Tribunal Europeo nada sustancial añaden a la doctrina tradicional de esta propia Sala y a la expuesta por el Tribunal Constitucional en la sentencia de contraste (STS 170/2013), pues sin lugar a dudas los factores que para el TEDH deben tenerse en cuenta en la obligada ponderación de intereses, creemos que se reconducen básicamente a los tres sucesivos juicios de idoneidad, necesidad y proporcionalidad requeridos por el Tribunal Constitucional".

Siendo éste el tenor en el que se expresa el Tribunal, existen, a mi modo de ver, argumentos suficientes para mostrar una posición crítica. En primer lugar, repárese en el contrasentido que supone aceptar como sentencia de contraste una resolución que autoriza a que la mera existencia de una política de prohibición de uso personal de los medios informáticos propiedad de la empresa implique de suyo el ejercicio del poder de vigilancia y control del empresario. Ello ya de por sí contraviene la tesis del TEDH en su sentencia Barbulescu II que justo viene a sostener lo contrario.

En segundo lugar, repárese en que no aborda el Tribunal el examen de

uno de los factores que el TEDH considera relevante, la notificación previa al trabajador, entendida como una garantía a su favor, del acceso al contenido de sus comunicaciones. De los hechos probados, se deduce que la empresa revisó los mensajes de correo del trabajador sin conocimiento de éste, pero la Sala no entra a valorar este extremo. ¿Qué consecuencias tendría esta circunstancia sobre la legitimidad de la actuación empresarial?
En tercer lugar, en fin, afirma la Sala que la sentencia del TEDH Barbulescu II no añade "nada sustancial" a la doctrina tradicional de la aplicación al caso del juicio de proporcionalidad. Ciertamente, si se repasan los factores que según el Tribunal Europeo deben tener en cuenta los Tribunales nacionales para enjuiciar la legitimidad de la medida empresarial se llega a la conclusión de que la mayoría son coincidentes con el consabido juicio de idoneidad, necesidad y proporcionalidad. Pero el valor que hay que concederle, en mi opinión, a la resolución del TEDH es el de conseguir que el análisis de este triple juicio deba realizarse de una forma más rigurosa y exigente por los Tribunales nacionales, que ya no podrán legitimar la medida fiscalizadora empresarial, como se ha dicho antes, sobre la existencia de una política de uso de los medios informáticos, sino que deberán revisar si existe la misma, a continuación, ponderar si aquélla supera el triple juicio antes indicado y, finalmente, si se ofrecieron las debidas garantías al trabajador.

3. El control a través de videovigilancia: la STEDH de 9 de enero de 2018 (caso López Ribalda y otras *vs* España) y su confrontación con la doctrina constitucional

Otra de las medidas que el empresario puede adoptar, en virtud del art. 20.3 ET, para controlar el cumplimiento de las obligaciones laborales por parte de sus empleados es la instalación de cámaras de videovigilancia, fijas o móviles, capaces de captar y grabar tanto imágenes como sonidos en el lugar de trabajo. Indudablemente, los derechos que pueden resultar afectados a través de este control son la intimidad del trabajador y su derecho a la protección de datos de carácter personal, por lo que deben aplicarse todas las cautelas posibles para valorar la licitud de la medida empresarial. Cautelas, precisamente, a las que viene a referirse otra de las sentencias del TEDH dictadas recientemente y que es de obligado comentario en un trabajo como éste, la sentencia de 9 de enero de 2018 (caso López Ribalda y otras *vs* España).
El supuesto de hecho que se enjuiciaba era el despido de varias trabajadoras por sustracción de productos de la empresa tomando como

base las imágenes captadas por cámaras de video instaladas en la empresa. Algunas de estas cámaras eran visibles para grabar posibles robos de clientes (de ello se informó a la representación de los trabajadores y a los propios empleados), mientras que otras se mantuvieron ocultas para grabar posibles robos de los empleados y no se informó de su existencia ni a los empleados ni a los representantes. Tras un período de grabación, la empresa citó a las cinco empleadas que aparecían implicadas en los hurtos y todas ellas reconocieron su implicación en los hechos en presencia de los representantes sindicales y del representante legal de la empresa. Además, se les ofreció la posibilidad de suscribir un acuerdo transaccional por el que renunciaban a impugnar el despido a cambio de que la empresa no iniciara acciones penales. Ese pacto fue suscrito por tres de las empleadas.

Ahora bien, no obstante todo ello, las trabajadoras impugnaron los despidos efectuados bajo el principal argumento de que se había vulnerado tanto su derecho a la intimidad como a la protección de datos, pues nunca se les informó de sus derechos de acceso a la información, de rectificación, de cancelación ni de ningún procedimiento de oposición.

Los Tribunales nacionales (juzgado de lo social n. 1 de Granollers y Tribunal Superior de Justicia de Cataluña[25]) desestiman las demandas y legitiman la validez del medio probatorio al considerar, en síntesis y con base en la STC 186/2000, de 10 de julio, que la vigilancia encubierta llevada a cabo sin previo aviso a las trabajadoras estaba justificada (al existir una sospecha razonable de robo), resultaba apropiada para el objetivo pretendido (verificar el motivo de las irregularidades entre el stock de productos de la empresa y lo realmente vendido) y era proporcionada (al no existir otros modos más eficaces de ponderar los intereses contrapuestos). Además, el TSJ pone énfasis también en el hecho de que las recurrentes habían reconocido los hechos ante la presencia de la representación de los trabajadores, por lo que la eventual declaración de nulidad de las imágenes aportadas a juicio no podía alterar el resultado del litigio. A mayor abundamiento, no se llega a cuestionar la validez de los acuerdos transaccionales, pues se llega a la conclusión, una vez analizados "minuciosamente", de que no existía prueba alguna de que mediara coacción en la firma de los mismos.

Las demandantes recurrieron entonces al Tribunal Supremo y al Tribunal Constitucional, pero los recursos se consideraron inadmisibles debido en un caso a la inexistencia de contradicción entre la STSJ de Cataluña

[25] Sentencias de 28 de enero (Rec. n. 4293/2010) y de 24 de febrero de 2011 (Rec. n. 4294/2010).

recurrida y las sentencias aportadas de contraste[26] y en otro a la "manifiesta inexistencia de una violación de un derecho fundamental tutelable en amparo"[27].

El litigio llega, en fin, al TEDH alegándose como principal argumento la vulneración del art. 8 CEDH poniéndolo en relación con el art. 5 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) al haberse realizado una videograbación de las recurrentes en su lugar de trabajo sin informar previamente de ello[28]. De igual manera, se alega la infracción del art. 6 CEDH al estimarse que el uso como prueba de información obtenida en violación del art. 8 suponía que el juicio en su conjunto llevado a cabo por los tribunales nacionales fuera injusto[29].

En cuanto a la vulneración del art. 6 CEDH, el Tribunal considera que no existe tal. Señala que la interpretación correcta de este precepto pasa por valorar "todas las circunstancias del caso, incluido el respeto de los derechos de defensa del demandante y la calidad e importancia de las pruebas en cuestión". Lo que conduce a preguntarse "si se pudo impugnar la autenticidad de las pruebas y oponerse a su uso, si las pruebas eran de suficiente calidad, lo que implica una investigación sobre si las circunstancias en que se obtuvieron podrían arrojar dudas sobre su veracidad o exactitud, si fueron respaldadas por otro material y si las pruebas en cuestión fueron o no decisivas para el resultado del procedimiento".

Tras aplicar estos criterios al caso en cuestión, el Tribunal concluye que

---

[26] Autos del TS de 5 de octubre de 2011 (Rec. n. 783/2011) y de 7 de febrero de 2012 (Rec. n. 1369/2011).

[27] Providencias de 27 de junio y 18 de julio de 2012. Sobre el inicio del conflicto y las sentencias dictadas por los tribunales españoles, vid., *in extenso*, Rojo Torrecilla, E., "Derecho del trabajador a la privacidad de la empresa y límites a su control por cámaras de vigilancia. Estudio del caso López Ribalda y otras contra España", *Derecho de las relaciones laborales*, n. 2, 2018, pp. 137-145.

[28] Señala el precepto que debe informarse, de modo expreso, preciso e inequívoco, de la "existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de estos y de los destinatarios de la información; del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas; de las consecuencias de la obtención de los datos o de la negativa a suministrarlos; de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición; de la identidad y dirección del responsable del tratamiento o, en su caso, de su representante".

[29] Concretamente, el artículo señala que "toda persona tiene derecho a que su causa sea oída equitativa, públicamente y dentro de un plazo razonable, por un Tribunal independiente e imparcial, establecido por ley, que decidirá los litigios sobre sus derechos y obligaciones de carácter civil o sobre el fundamento de cualquier acusación en materia penal dirigida contra ella".

"no se ha demostrado nada que respalde la conclusión de que los derechos de defensa de las demandantes no se cumplieran adecuadamente con respecto a las pruebas aducidas o que su evaluación por los tribunales nacionales fuera arbitraria". Y ello porque, aunque las recurrentes tuvieron la oportunidad de impugnar tanto la autenticidad como el uso de las grabaciones durante los sucesivos juicios, no lo hicieron. Y porque, además, las grabaciones impugnadas no fueron la única prueba en la que se basaron los tribunales nacionales para confirmar la procedencia de los despidos. También se otorgó importancia a las declaraciones testificales de otros empleados, de los representantes de los trabajadores, del representante de la empresa y del gerente.

Sí que se estimó, por el contrario, la infracción del art. 8 CEDH. El Tribunal comienza afirmando que "la videovigilancia encubierta de un empleado en su puesto de trabajo, como tal, debe ser interpretada como una considerable intrusión sobre su vida privada". Por ello, entiende que, como hiciera en su sentencia Barbulescu II, debe discernir si se logró alcanzar "un equilibrio justo entre el derecho de las demandantes al respeto hacia sus vidas privadas y el interés del empleador en proteger sus derechos organizacionales y de gestión en lo que se refiere al derecho a la propiedad, además del interés público acerca de la correcta administración de la justicia".

Pues bien, para responder a esta pregunta examina las circunstancias del caso y reconoce que la medida podría considerase legítima por existir la sospecha fundada de hurtos en la empresa; ello no obstante, recuerda que "los datos visuales obtenidos implicaban el almacenaje y tratamiento de datos personales, lo cual está estrechamente vinculado al ámbito personal privado" y llama la atención sobre el hecho de que "el material fue procesado y examinado por varias personas que trabajaban para el empleador de las demandantes (entre ellos, el delegado sindical y el representante legal de la empresa) con anterioridad a que las propias demandantes fueran informadas sobre la existencia de las grabaciones".

Observa, además, el Tribunal que el empresario "no cumplió con su obligación en lo que se refiere a informar a los interesados sobre la existencia de una forma de recogida y tratamiento de datos personales", como se prevé tanto en el art. 5 LOPD como en el art. 3 de la Instrucción 1/2006 emitida por la Agencia Española de Protección de Datos que especifica que la obligación de información contemplada en el artículo precedente se aplica "a cualquiera que utilizase sistemas de videovigilancia, en cuyo caso, éstos estarían obligados a colocar, en las zonas videovigiladas, un distintivo informativo, y a tener a disposición de los interesados impresos detallando la información prevista en el artículo 5

LOPD".

Estas previsiones no las tuvieron en cuenta ni el empresario ni los tribunales nacionales, quienes, a pesar de todo, "consideraron que la medida había sido justificada (en el sentido de que existía una sospecha razonable de robo), apropiada para el objetivo deseado, necesaria y proporcional, ya que no existía otra medida más eficiente para proteger los derechos del empleador interfiriendo en menor medida con el derecho de las demandantes al respeto hacia su vida privada". A consecuencia de ello, el Tribunal europeo, por seis votos a favor y uno en contra[30], condena a España por vulneración del art. 8 CEDH, ya que, "en una situación donde el derecho de cada afectado a ser informado de la existencia, el objetivo y la forma de la videovigilancia encubierta estaba claramente regulado y protegido por la ley, las demandantes tenían unas expectativas razonables de privacidad". A mayor abundamiento, llama la atención sobre el hecho de que la videovigilancia encubierta se había efectuado de forma indiscriminada, estando dirigida "a la totalidad del personal que trabajaba en las cajas, con una duración de semanas, sin límite de tiempo y durante todo el horario laboral"[31] y considera, en fin, que "los derechos del empleador podrían haber sido salvaguardados, al menos hasta cierto punto, mediante la utilización de otros medios, concretamente informando a las demandantes, incluso de un modo general, sobre la instalación de un sistema de videovigilancia, y proporcionándoles la información descrita en la LOPD".

Con independencia de que esta última afirmación sobre la existencia de una medida alternativa más inocua sobre la privacidad de las trabajadoras pueda cuestionarse (si de lo que se trata es de confirmar sospechas de hurto y de sancionar al infractor no parece que hubiera dado resultado otro tipo de vigilancia, una vigilancia advertida por así decirlo), lo que pone de nuevo sobre la mesa esta sentencia del Tribunal de Estrasburgo es la necesidad de que los trabajadores, tal y como señala Barbulescu II,

[30] La sentencia cuenta con un voto particular que, en síntesis, viene a decir que el CEDH no debería amparar actuaciones abusivas y contrarias a derecho de los trabajadores, pues "los comportamientos ofensivos son incompatibles con el derecho a la vida privada en virtud del Convenio, [lo que significa que] debe prevalecer el interés público de la sociedad y que la salvaguarda contra la ilegalidad y la arbitrariedad debe limitarse a proteger de una interferencia abusiva".

[31] Establece aquí diferencias el Tribunal entre este asunto y el caso Köpke (Köpke *vs* Alemania, sentencia de 5 de octubre de 2010) donde avaló la video vigilancia encubierta porque, primero, no había regulación legal que fijara "las condiciones bajo las cuales un empleador podía recurrir a la videovigilancia de un empleado para investigar un delito", y segundo, porque "la medida de vigilancia se aplicó durante un tiempo limitado (se realizó a lo largo de dos semanas) y únicamente estaba dirigida a dos empleados".

sean convenientemente informados acerca de la medida de vigilancia implantada por la empresa. Hasta tal punto ello es así que puede afirmarse, como se ha señalado por la doctrina[32], que este deber de información forma parte del contenido esencial de los derechos fundamentales a la intimidad, al secreto de las comunicaciones, a la propia imagen y a la protección de datos de carácter personal.

Este dato es importante señalarlo porque supone desautorizar la doctrina que el Tribunal Constitucional había asentado en su sentencia 39/2016, de 3 de marzo[33], sentencia, por cierto, citada por el TEDH en el caso López Ribalda. Por señalar los antecedentes del caso, de lo que se trataba era de discernir sobre la nulidad o procedencia del despido de una trabajadora sobre la que existían sospechas de que se estaba apropiando de efectivo. Por ello, la empresa, tras advertir irregularidades contables al cuadrar la caja, decidió instalar una cámara de videovigilancia enfocando al puesto de trabajo; instalación que no se comunicó a los trabajadores, si bien en el escaparate del establecimiento, en un lugar visible, se colocó el correspondiente distintivo informativo. Tras la comprobación de las imágenes en las que efectivamente se apreciaba a la trabajadora apropiándose de dinero, se procede a su despido. La trabajadora impugna la decisión empresarial, solicitando la declaración de nulidad, sobre la base de que no existía comunicación al público ni carteles comunicativos de la existencia de cámaras de videograbación, ni tampoco comunicación a la Agencia de Protección de Datos, ni comunicación o informe previo del comité de empresa de la instalación de la videograbación.

Pues bien, aquí el Tribunal, rompiendo con su doctrina anterior en la que exigía una información clara y concreta a los trabajadores del sistema de control implantado y de su finalidad[34], declara que basta para cumplir con el deber de información previa que se deriva de la LOPD con "la colocación en las zonas videovigiladas de un distintivo informativo ubicado en lugar suficientemente visible que incluya una referencia a la ley de protección de datos, una mención a la finalidad para la se tratan los datos ("zona videovigilada") y una mención expresa a la identificación del responsable ante quien puedan ejercitarse los derechos a los que se

[32] Casas Baamonde, Mª.E., "Informar antes que vigilar. ¿Tiene el Estado...", *op. cit.*, p. 115.

[33] Seguida por sentencias de 31 de enero (Rec. n. 3331/2015) y de 2 de febrero de 2017 (Rec. n. 554/2016). Para un análisis en particular, vid. Taléns Visconti, E., "Video-vigilancia en el trabajo: una vuelta a la jurisprudencia clásica", *Trabajo y Derecho*, n. 21, 2016, pp. 1-9 (versión *on line*).

[34] STC 29/2013, de 11 de febrero.

refieren los arts. 15 y siguientes de la Ley Orgánica 15/1999"[35]. Y ello "sin que haya que especificar, más allá de la mera vigilancia, la finalidad exacta que se le ha asignado a ese control".

Parece claro que, con las sentencias Barbulescu II y López Ribalda en la mano, esta "escueta" información sobre la existencia de cámaras de grabación parece que deslegitimaría *per se* el control efectuado por el empresario, pues no se habría dado efectivo cumplimiento a la obligación de transparencia, específica, no genérica, abstracta o presunta, que recae sobre éste.

Por lo demás y al hilo de lo anterior, la sentencia López Ribalda también pone de relieve la importancia de evaluar la medida empresarial de vigilancia a través del prisma que supone el juicio de proporcionalidad, lo que supone dar un segundo toque de atención al Tribunal Constitucional. Y es que, de nuevo en la sentencia de 3 de marzo de 2016, se contempla una conclusión que debe quedar ahora desautorizada por las sentencias europeas: la falta de información no implica necesariamente una vulneración de derechos fundamentales si el control efectuado supera el juicio de proporcionalidad[36]. Es decir, para el Tribunal, el incumplimiento de la obligación de transparencia queda rebajado a mera exigencia formal, pues si la medida de vigilancia se juzga, a la vista de los hechos, idónea, necesaria y equilibrada, se considerará legítima desde el punto de vista constitucional.

Ciertamente, es grave que el propio Tribunal Constitucional desatienda como lo hace el contenido esencial del derecho a la intimidad y a la protección de datos. Como también lo es que se recurra al juicio de proporcionalidad para intentar justificar la legitimidad de una medida de control que resulta ser, ya de inicio, irregular, pero que logra posicionarse por delante de los derechos fundamentales del trabajador de una forma

[35] Previsión ésta, por cierto, que se contempla en el art. 22.4 del proyecto de Ley Orgánica de Protección de Datos de Carácter Personal (BOCG de 24 de noviembre de 2017).

[36] Así, se señala que "el incumplimiento del deber de requerir el consentimiento del afectado para el tratamiento de datos o del deber de información previa sólo supondrá una vulneración del derecho fundamental a la protección de datos tras una ponderación de la proporcionalidad de la medida adoptada" (Fundamento Jurídico n. 3). Y se insiste, a continuación, en que "aunque no se requiere el consentimiento expreso de los trabajadores para adoptar esta medida de vigilancia que implica el tratamiento de datos, persiste el deber de información del art. 5 LOPD. Sin perjuicio de las eventuales sanciones legales que pudieran derivar, para que el incumplimiento de este deber por parte del empresario implique una vulneración del art. 18.4 CE exige valorar la observancia o no del principio de proporcionalidad" (Fundamento Jurídico n. 4).

tan flagrante como incoherente con los mandatos constitucionales[37]. Se podría alegar que la protección que se le debe dispensar a los derechos fundamentales no puede suponer a la postre otorgar "carta blanca" a los trabajadores que hubiesen cometido actuaciones irregulares por reprochables laboralmente. Pero, aunque ello en cierta manera pueda compartirse y fuera causa suficiente para legitimar la videovigilancia encubierta (siempre que existiera una razón excepcional de peso que lo justificara y siempre que el control fuese limitado en el tiempo y selectivo ,no indiscriminado y atemporal como se evidenciaba en el caso enjuiciado por el Tribunal europeo)[38], lo cierto es que pesan sobre el empresario determinados deberes legales que debe cumplir escrupulosamente y más ahora, en estos momentos, con el nuevo Reglamento 2016/679 del Parlamento Europeo y del Consejo de 27 de abril, que aumenta la obligación de transparencia que debe regir en la materia y refuerza el control de las personas sobre sus propios datos.

4. Bibliografía

Blázquez Agudo, E.Mª., *Aplicación práctica de la protección de datos en las relaciones laborales*, CISS-Wolters Kluwer, Madrid, 2018.

Casas Baamonde, Mª.E., "Informar antes que vigilar. ¿Tiene el Estado la obligación positiva de garantizar un mínimo de vida privada a los trabajadores en la empresa en la era digital? La necesaria intervención del legislador laboral", *Derecho de las Relaciones Laborales*, n. 2, 2018, pp. 103-119.

Desdentado Bonete, A. y Desdentado Daroca, E., "La segunda sentencia del TEDH en el caso Barbulescu y sus consecuencias sobre el control del uso laboral del ordenador", *Revista de Información laboral,* n. 1, 2018 (versión *on line*).

Goñi Sein, J.L., "La vigilancia empresarial de las comunicaciones electrónicas de los trabajadores", *Trabajo y Derecho*, n. 18, 2016 (versión *on line*).

Mercader Uguina, J., *El futuro del trabajo en la era de la digitalización y la robótica*, Valencia, Tirant lo Blanch, 2018.

[37] De la misma opinión, Terradillos Ormaetxea, E., "El principio de proporcionalidad como…", *op. cit.*, pp. 157 y 158. También se pronuncia en el mismo sentido el voto particular con el que cuenta la STC 39/2016, de 3 de marzo.

[38] También de esta opinión, Molina Navarrete, C., "De Barbulescu II a López Ribalda: ¿qué hay de nuevo en la protección de datos de los trabajadores?", *Estudios Financieros,* n. 419, 2018, p. 135.

Molina Navarrete, C., "De Barbulescu II a López Ribalda: ¿qué hay de nuevo en la protección de datos de los trabajadores?", *Estudios Financieros,* n. 419, 2018, pp. 125-135.

Molina Navarrete, C., "El poder empresarial de control digital: ¿nueva doctrina del TEDH o mayor rigor aplicativo de la precedente?", *Ius Labor,* n. 3, 2017, pp. 287-297.

Molina Navarrete, C., "Expectativa razonable de privacidad y poder de vigilancia empresarial: ¿*quo vadis* justicia laboral?", *Estudios Financieros,* n. 399, 2016, pp. 171-180.

Rojo Torrecilla, E., "Derecho del trabajador a la privacidad de la empresa y límites a su control por cámaras de vigilancia. Estudio del caso López Ribalda y otras contra España", *Derecho de las relaciones laborales*, n. 2, 2018, pp. 135-152.

Rodríguez Escanciano, S., *El derecho a la protección de datos personales de los trabajadores: nuevas perspectivas*, Albacete, Bomarzo, 2009.

Sala Franco, T., "El derecho a la intimidad y a la propia imagen y las nuevas tecnologías de control laboral", en AA.VV., *Trabajo y libertades públicas,* Madrid, La Ley, 1999, pp. 201-230.

Taléns Visconti, E., "Video-vigilancia en el trabajo: una vuelta a la jurisprudencia clásica", *Trabajo y Derecho*, n. 21, 2016, pp. 1-9 (versión *on line*).

Terradillos Ormaetxea, E., "El principio de proporcionalidad como referencia garantista de los derechos de los trabajadores en las últimas sentencias del TEDH dictadas en materia de ciberderechos: un contraste con la doctrina del Tribunal Constitucional español", *Revista de Derecho Social*, n. 80, 2017, pp. 139-162.

Red Internacional de ADAPT

ADAPT es una Asociación italiana sin ánimo de lucro fundada por Marco Biagi en el año 2000 para promover, desde una perspectiva internacional y comparada, estudios e investigaciones en el campo del derecho del trabajo y las relaciones laborales con el fin de fomentar una nueva forma de "hacer universidad". Estableciendo relaciones estables e intercambios entre centros de enseñanza superior, asociaciones civiles, fundaciones, instituciones, sindicatos y empresas. En colaboración con el DEAL – Centro de Estudios Internacionales y Comparados del Departamento de Economía Marco Biagi (Universidad de Módena y Reggio Emilia, Italia), ADAPT ha promovido la institución de una Escuela de Alta formación en Relaciones Laborales y de Trabajo, hoy acreditada a nivel internacional como centro de excelencia para la investigación, el estudio y la formación en el área de las relaciones laborales y el trabajo. Informaciones adicionales en el sitio *www.adapt.it*.

Para más informaciones sobre la Revista Electrónica y para presentar un artículo, envíe un correo a *redaccion@adaptinternacional.it*