

POLÍTICA EMPRESARIAL PREVIA Y SUPRESIÓN DE LA EXPECTATIVA DE PRIVACIDAD: UNA REFLEXIÓN CRÍTICA SOBRE LAS FACULTADES DE CONTROL DEL ORDENADOR UTILIZADO POR EL TRABAJADOR

IVÁN ANTONIO RODRÍGUEZ CARDO

*Profesor Titular de Universidad. Derecho del Trabajo
y de la Seguridad Social
Universidad de Oviedo*

EXTRACTO

Palabras clave: Contrato de trabajo, privacidad, derechos fundamentales, poder de control empresarial, uso del ordenador

Las facultades de control y vigilancia que se insertan en el contenido del poder de dirección no pueden utilizarse de tal modo que supongan una lesión de derechos fundamentales, especialmente los derechos a la intimidad y al secreto de las comunicaciones. En los últimos años son cada vez más frecuentes los litigios en este ámbito, y el Tribunal Constitucional ha elaborado una rica doctrina, inclusive en relación con el uso del ordenador en el trabajo. En estos casos, el control parece depender de la política empresarial previa, criterio que aparentemente proporciona seguridad jurídica, pero que también suscita dudas de compatibilidad con los derechos fundamentales. El presente estudio pretende clarificar si la doctrina sobre el control del uso del ordenador rediseña el alcance de las facultades empresariales, y en último término propone una interpretación alternativa.

ABSTRACT

Key words: Contract of employment, right to privacy, fundamental rights, corporate control, computer use

The powers of control and surveillance, which are inserted into the contents of the employer's power, cannot be used in such a way that they pose an injury of fundamental rights, especially the rights to privacy and to secrecy of communications. The litigation in this area are increasingly frequent in recent years, and the Constitutional Court has developed a rich doctrine, including in relation to the use of the computer at work. In these cases, the control seems to depend on previous business policy, criteria which apparently provides legal certainty, but which also raises doubts of compatibility with fundamental rights. This study aims to clarify whether the doctrine on the use of computer control redesigns the scope of employer's power, and ultimately proposes an alternative interpretation.

ÍNDICE

1. INTRODUCCIÓN: MEDIOS LÍCITOS DE CONTROL DE LA ACTIVIDAD DEL TRABAJADOR.
2. LA UTILIZACIÓN DE MEDIOS EMPRESARIALES (NO INFORMÁTICOS) CON FINES PERSONALES.
3. EL CONTROL DEL USO DEL ORDENADOR POR PARTE DEL TRABAJADOR EN LA JURISPRUDENCIA CONSISTITUCIONAL: LA PROPIEDAD DE LA EMPRESA Y LA POLÍTICA EMPRESARIAL PREVIA COMO ELEMENTOS PRINCIPALES DE JUICIO.
4. ¿NUEVO CRITERIO JURISPRUDENCIAL O DOCTRINA DIFERENTE PARA EL CONTROL DEL ORDENADOR Y DE OTROS MEDIOS EMPRESARIALES?
5. REDISEÑANDO LOS LÍMITES AL CONTROL EMPRESARIAL DEL ORDENADOR: ALCANCE Y EFECTOS DE LA PROHIBICIÓN EMPRESARIAL DE USO PERSONAL DEL ORDENADOR.
6. FACULTADES DE CONTROL EMPRESARIAL PARA CONSTATAR LA VERACIDAD DE UNA SOSPECHA.
7. CONTROLES EN AUSENCIA DE SOSPECHA: LA FINALIDAD COMO ELEMENTO DETERMINANTE DE LAS FACULTADES EMPRESARIALES.
8. A MODO DE CONCLUSIÓN: EL CONVENIENTE RETORNO AL JUICIO DE PONDERACIÓN Y AL CRITERIO DEL USO INOCUO.

1. INTRODUCCIÓN: MEDIOS LÍCITOS DE CONTROL DE LA ACTIVIDAD DEL TRABAJADOR

Como es bien sabido, el art. 18 ET dispone que «sólo podrán realizarse registros sobre la persona del trabajador, en sus taquillas y efectos particulares, cuando sean necesarios para la protección del patrimonio empresarial y del de los demás trabajadores de la empresa, dentro del centro de trabajo y en horas de trabajo»¹. Por su parte, el art. 20.3 ET permite que el empleador adopte «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». Este marco normativo se debe ajustar, desde luego, a las exigencias que derivan del derecho fundamental a la intimidad (art. 18 CE), en su conexión con la dignidad de la persona (art. 10 CE).

Ahora bien, los avances tecnológicos han propiciado que los mecanismos de control aumenten exponencialmente su potencial lesivo respecto de los derechos del trabajador, y en particular la afectación al derecho a la intimidad ha sido objeto de litigios frecuentes. No conviene olvidar que el deseo de organizar de la manera más eficiente posible la actividad productiva puede derivar en medidas dirigidas a maximizar el rendimiento laboral y la productividad, intensificando los mecanismos de control a través de medios que pueden resultar invasivos.

¹ Vid. C. Molero Manglano, *Inviolabilidad de la persona del trabajador*, REDT, nº 100, 2000, pp. 543 y ss.; J.I. García Ninet, “De los registros del trabajador y del respeto máximo a la dignidad e intimidad de éste”, en J.I. García Ninet (Dir.), *El control empresarial*, CISS, Valencia, 2005, pp. 181 y ss.

La jurisprudencia constitucional relativa a la delimitación y alcance de las medidas de control y vigilancia es abundante, y muy rica en matices, con el objetivo último de conciliar esas facultades empresariales con los derechos del trabajador. Entre esa jurisprudencia cabe destacar la relativa a la utilización de cámaras de video² o micrófonos³, cuya lícita instalación está supeditada a la acreditación de un interés empresarial legítimo y al respeto al principio de proporcionalidad, ya que no cabe un «exceso en el control»⁴ o una «invasión excesiva del ámbito personal del trabajador»⁵.

Es obvio que tales medios de control no se justifican en determinadas dependencias empresariales, donde el derecho a la intimidad prevalece claramente sobre los intereses del empleador (*v.gr.*, aseos, vestuarios). Las facultades empresariales cuentan con más intensidad en los lugares donde se desarrolla la actividad laboral, pero también en ellos el derecho a la intimidad permite establecer limitaciones, puesto que pueden «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» (STC 98/2000, de 10 de abril, FJ 6º). A efectos del imprescindible juicio de ponderación, debe tomarse en consideración no sólo el lugar donde el mecanismo o instrumento de control actúa, sino también factores muy distintos, como el carácter masivo o indiscriminado de tales medios, si son o no visibles o conocidos, y cuál es su finalidad.

La jurisprudencia constitucional no se ha limitado a establecer esos criterios de necesidad y razonabilidad, sino que ha introducido un nuevo requisito: la información al trabajador cuando el incumplimiento se haya detectado a través de un medio no diseñado específicamente para el control del trabajador o de su actividad. En palabras de la STC 29/2013, de 11 de febrero, «las cámaras de video-vigilancia instaladas en el recinto universitario reprodujeron la imagen del recurrente y permitieron el control de su jornada de trabajo; captaron, por tanto, su imagen, que constituye un dato de carácter personal, y se emplearon para el seguimiento del cumplimiento de su contrato. De los hechos probados se desprende que la persona jurídica titular del establecimiento donde se encuentran instaladas las videocámaras es la Universidad de Sevilla y que

² Vid. STC 186/2000, de 10 de julio.

³ Vid. STC 98/2000, de 10 de abril.

⁴ Cfr. S. Del Rey Guanter, «Los límites del control por el empresario en el centro de trabajo mediante mecanismo auditivos», en M. Alonso Olea y A. Montoya Melgar (Dir.), *Jurisprudencia constitucional sobre Trabajo y Seguridad Social. Tomo XVIII (2000)*, Civitas, Madrid, 2001, pág. 198.

⁵ Cfr. A. Montoya Melgar, «Control del trabajador desleal y alcance del derecho de éste a la intimidad», en M. Alonso Olea y A. Montoya Melgar (Dir.), *Jurisprudencia constitucional sobre Trabajo y Seguridad Social. Tomo XVIII (2000)*, Civitas, Madrid, 2001, pág. 317.

ella fue quien utilizó al fin descrito las grabaciones, siendo la responsable del tratamiento de los datos sin haber informado al trabajador sobre esa utilidad de supervisión laboral asociada a las capturas de su imagen» (FJ 8º)⁶.

Ese marco general debería resultar asimismo de aplicación a los supuestos de control y vigilancia del uso de las herramientas que el empleador pone a disposición de los trabajadores, pero que también son susceptibles de una utilización con finalidad personal, como el coche de empresa o un teléfono móvil. Los tribunales han extendido las reglas generales a ese ámbito, pero el control del ordenador puesto a disposición del trabajador ha dado lugar a una doctrina que aparentemente parte de premisas diferentes. Esa línea interpretativa, que pone el acento sobre la información previa proporcionada por el empleador, es compartida por el TC, el TS y la Agencia Española de Protección de Datos. Pese a ello, los criterios sobre los que se asienta esa doctrina, si no se vinculan a las peculiaridades del caso concreto, podrían dar lugar a interpretaciones de muy diverso signo, y alguna de ellas conduciría a resultados desproporcionados. Conviene, así pues, realizar un balance de esa reciente doctrina para constatar si se ha producido un cambio jurisprudencial, bien sea en lo relativo a la eficacia de los derechos a la intimidad y al secreto de las comunicaciones en el ámbito de la relación de trabajo, bien sea en relación con el uso del ordenador proporcionado por el empresario, en comparación con la utilización de otros medios o herramientas de trabajo.

2. LA UTILIZACIÓN DE MEDIOS EMPRESARIALES (NO INFORMÁTICOS) CON FINES PERSONALES

El control empresarial sobre el trabajador puede exceder de la mera comprobación del cumplimiento de las obligaciones laborales básicas, de la ejecución de la prestación de trabajo en sentido estricto, y extenderse a todas aquellas facetas de la relación laboral que, en caso de conducta reprobable, pudieran encajar en la transgresión de la buena fe contractual. Por tanto, esos medios de control y vigilancia podrían dirigirse a averiguar si el trabajador uti-

⁶ Abundando en ese argumento, la sentencia afirma que «no contrarresta esa conclusión que existieran distintivos anunciando la instalación de cámaras y captación de imágenes en el recinto universitario, ni que se hubiera notificado la creación del fichero a la Agencia Española de Protección de Datos; era necesaria además la información previa y expresa, precisa, clara e inequívoca a los trabajadores de la finalidad de control de la actividad laboral a la que esa captación podía ser dirigida. Una información que debía concretar las características y el alcance del tratamiento de datos que iba a realizarse, esto es, en qué casos las grabaciones podían ser examinadas, durante cuánto tiempo y con qué propósitos, explicitando muy particularmente que podían utilizarse para la imposición de sanciones disciplinarias por incumplimientos del contrato de trabajo».

liza los medios empresariales con fines personales⁷, y eventualmente podrían llegar a afectar a la esfera personal o íntima del individuo, a circunstancias que deberían encontrarse al margen del alcance del poder de dirección.

La forma de controlar el contenido de los medios empresariales puestos a disposición de los trabajadores (ordenador, teléfonos fijo y móvil, etc.) constituye, desde luego, un punto de fricción cada vez más habitual, por los riesgos potenciales que supone la introducción de medios telemáticos, y en particular de internet, en el entorno de trabajo⁸. El derecho a la intimidad personal coadyuva en algunas de estas situaciones con la garantía del «secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial» (art. 18.3 CE), pero esos derechos deben conciliarse con la libertad de empresa, y, desde luego, con los legítimos poderes empresariales de control y vigilancia.

En relación con los medios no informáticos, los tribunales suelen valorar, principalmente, la frecuencia de la conducta inapropiada del trabajador y la eventual tolerancia de la empresa, amén de unas instrucciones claras sobre el uso. Una conducta ocasional o previamente tolerada –mediando incluso una autorización genérica para el uso privado-⁹, aunque eventualmente podría ser objeto de sanción, no presenta de ordinario una dosis suficiente de gravedad como para justificar el despido; alguna sentencia introduce también el concepto de «uso normal o razonable» para limitar los supuestos de despido a las situaciones de mayor gravedad, que constituyen un abuso de confianza¹⁰.

A la postre, la buena fe, el uso inocuo u ocasional, la tolerancia empresarial, las advertencias o amonestaciones previas y el perjuicio económico que sufre la empresa son criterios que sirven para dilucidar si es legítima una sanción por el uso con fines particulares de medios empresariales. La casuística es variada, y la solución depende de la mayor o menor trascendencia en la valoración que se conceda a cada una de esas circunstancias¹¹.

⁷ Vid. F. Pérez De Los Cobos Orihuel, *Nuevas tecnologías y relación de trabajo*, Tirant lo Blanch, Valencia, 1990, pp. 72 y ss.; L.A. Fernández Villazón, *Las facultades empresariales de control de la actividad laboral*, Thomson-Aranzadi, Pamplona, 2003, pp. 184 y ss.; J.R. Mercader Uguina, *Derecho del Trabajo, nuevas tecnologías y sociedad de la información*, Lex Nova, Valladolid, 2002, pp. 95 y ss.

⁸ Vid. M.F. Fernández López, “La intimidad del trabajador y su tutela en el contrato de trabajo”, en M.E. Casas Baamonde, F. Durán López y J. Cruz Villalón (Coord.), *Las transformaciones del Derecho del Trabajo en el marco de la Constitución Española*, La Ley, Madrid, 2006, pp. 658 y ss.

⁹ La STSJ de Cantabria de 28-8-1996 (recurso de suplicación 1189/1996) declara improcedente el despido de un trabajador a consecuencia de que la factura del teléfono móvil corporativo había ascendido a 98.603 pesetas. La sentencia valora que se trataba de un trabajador desplazado al extranjero y que la propia empresa, al entregarle el teléfono, le había autorizado para informar a su familia.

¹⁰ Vid. SSTSJ de Andalucía/Málaga de 9-10-2002 (recurso de suplicación 1364/2002) y de Cataluña de 15-7-2002 (recurso de suplicación 2534/2002).

¹¹ Vid. I.A. Rodríguez Cardo, *Poder de dirección empresarial y esfera personal del trabajador*, CES Asturias, 2009, pp. 128 y ss. (http://www.cesasturias.es/ficha_publicacion.php?idPublicacion=120).

En relación con la utilización del teléfono móvil, la doctrina judicial no valora el medio de control empleado, sino únicamente la licitud de la reacción empresarial una vez descubierto el incumplimiento. Las razones, seguramente, estriban en que la empresa conoce el gasto por ser la titular de la línea, con la consiguiente obligación de hacer frente a la factura. No hay, pues, ninguna intromisión ilegítima en la intimidad del trabajador.

Cuestión distinta es el control y vigilancia de la utilización de otros medios empresariales puestos a disposición del trabajador, como por ejemplo un vehículo. El medio de control más habitual consiste en instalar un dispositivo GPS de localización, lo que supone, a diferencia del teléfono móvil, una conducta activa susceptible de vulneración del derecho a la intimidad. La doctrina judicial faculta al empleador para valerse de esta clase de instrumentos, advirtiendo, en primer lugar, que la medida no se conecta necesariamente con el control del trabajador, sino que puede responder a una finalidad productiva, porque en determinadas actividades permitiría al empresario llamar preferentemente a los trabajadores que se encontrasen más cerca en una eventual situación de urgencia. E incluso tales medios podrían justificarse por razones de seguridad (*v.gr.*, chófer en un vehículo de lujo, comprobación de mejores rutas, etc.).

En su faceta de herramienta de control y vigilancia, la doctrina judicial suele considerar que la instalación de un GPS no es una medida especialmente invasiva, sino que, al contrario, respeta el principio de proporcionalidad, por las dificultades de control que se aprecian cuando el trabajador realiza actividades móviles o itinerantes. La desactivación de ese instrumento por parte del trabajador, cuando su utilización se justifica, es merecedora de sanción¹². En ocasiones simplemente se afirma que este medio de control no lesiona el derecho a la intimidad, mientras que en otras se prefiere obrar con mayor cautela, valorando explícitamente que el empleador haya precisado claramente las obligaciones del trabajador¹³, le haya advertido de la implantación del GPS y, además, que no se hubiera pactado ni tolerado un uso privado del vehículo¹⁴.

Por supuesto, en caso de sospecha previa las limitaciones son menores, precisamente porque el medio de control se utiliza con una finalidad concreta, y no de forma indiscriminada¹⁵, y en estos casos la advertencia de control puede ser genérica, sin indicación explícita sobre la instalación de un GPS¹⁶. Tampoco conviene olvidar que mediante un dispositivo GPS se obtiene exclusivamente la localización del vehículo, y no se graban imágenes ni sonido, por lo que la intromisión en la intimidad del trabajador resulta sensiblemente

¹² Vid. STSJ de Andalucía/Granada de 25-1-2012 (recurso 2924/2011).

¹³ Vid. STSJ de Madrid de 13-10-2009 (recurso 4032/2009).

¹⁴ Vid. STSJ de Galicia de 17-1-2014 (recurso 3483/2013).

¹⁵ Vid. STSJ de Madrid de 20-11-2013 (recurso 1496/2013).

¹⁶ Vid. STSJ de Cataluña de 5-3-2012 (recurso 5194/2011).

menor, salvo que el control y vigilancia se extienda a actividades privadas. En este sentido, si tales dispositivos permiten localizar al trabajador fuera del tiempo y lugar de trabajo, y por tanto en el contexto de su vida privada, sólo en supuestos excepcionales cabría admitir que la medida empresarial resulta legítima¹⁷.

3. EL CONTROL DEL USO DEL ORDENADOR POR PARTE DEL TRABAJADOR EN LA JURISPRUDENCIA CONSTITUCIONAL: LA PROPIEDAD DE LA EMPRESA Y LA POLÍTICA EMPRESARIAL PREVIA COMO ELEMENTOS PRINCIPALES DE JUICIO

Como es bien sabido, las SSTC 241/2012, de 17 diciembre, y 170/2013, de 7 octubre, contienen la doctrina más reciente relativa al control y vigilancia de la utilización del ordenador por el trabajador, en conexión con los derechos fundamentales a la intimidad y al secreto de las comunicaciones. Toda la argumentación se construye a partir de la premisa de que el ordenador es una herramienta de trabajo propiedad de la empresa, de modo que el empleador puede limitar su utilización con fines personales, en cualquiera de las funcionalidades que admite ese instrumento.

Las sentencias citadas valoran especialmente que exista una prohibición empresarial explícita de uso personal de los medios empresariales. En presencia de una política empresarial clara, la sentencia 241/2012, analizando el acceso a unos ficheros informáticos en los que habían quedado registradas las conversaciones electrónicas mantenidas por dos trabajadoras a través de un programa de mensajería que habían instalado en un ordenador de uso común a todos los trabajadores y sin contraseña, advierte que no existe una «situación de tolerancia a la instalación de programas y, por ende, al uso personal del ordenador», y por consiguiente, «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» (FJ 6º STC 241/2012).

El hecho de que el medio utilizado para la comunicación entre trabajadores no estuviera protegido por contraseña o encriptado parece adquirir una relevancia fundamental, pues ese canal «abierto», accesible por todos, admite el control empresarial sin vulnerar el secreto de las comunicaciones, a la vez que implica, en cierto modo, una renuncia al derecho a la intimidad de los trabajadores que utilizan ese medio. En este sentido, la sentencia advierte que «la

¹⁷ Vid. STSJ del País Vasco de 10-5-2011 (recurso 644/2011), en relación con la colocación de un GPS en el vehículo particular del trabajador con el fin de constatar si realizaba actividades incompatibles con su estado durante una situación de IT.

atribución de espacios individualizados o exclusivos puede tener relevancia desde el punto de vista de la actuación empresarial de control»¹⁸.

Esa doctrina se completa con la contenida en la STC 170/2013, en un supuesto de hecho particular, donde la empresa, ante la sospecha de que el trabajador proporcionaba información confidencial a la competencia, había accedido al ordenador portátil puesto a disposición del trabajador con el fin de comprobar los correos electrónicos enviados y recibidos, constatándose efectivamente el incumplimiento. La sentencia considera que la tipificación en el convenio colectivo, como infracción leve, del uso de los medios informáticos propiedad de la empresa con fines personales suponía una prohibición explícita en orden a su utilización, y como consecuencia «el poder de control de la empresa sobre las herramientas informáticas de titularidad empresarial puestas a disposición de los trabajadores podía legítimamente ejercerse, *ex art.* 20.3 LET, tanto a efectos de vigilar el cumplimiento de la prestación laboral realizada a través del uso profesional de estos instrumentos, como para fiscalizar que su utilización no se destinaba a fines personales o ajenos al contenido propio de su prestación de trabajo» (FJ 4º).

Con gran contundencia, la sentencia insiste en que «no podía existir una expectativa fundada y razonable de confidencialidad respecto al conocimiento de las comunicaciones mantenidas por el trabajador a través de la cuenta de correo proporcionada por la empresa y que habían quedado registradas en el ordenador de propiedad empresarial», ya 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». El secreto de las comunicaciones no resulta vulnerado porque «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» y «sometido en consecuencia a su posible fiscalización».

Esos mismos argumentos son utilizados para rechazar la vulneración del derecho a la intimidad, ya que se insiste en que el trabajador no cuenta con una «expectativa razonable de privacidad respecto a sus correos electrónicos registrados en el ordenador de la entidad empresarial» cuando existe una política clara en contra de la utilización de esos medios con fines personales. En suma, el mismo criterio justifica la medida tanto desde la perspectiva del derecho a la intimidad, como desde la óptica del secreto de las comunicaciones.

¹⁸ Vid. E.E. Talens Visconti, *La expectativa razonable de confidencialidad como presupuesto de vulneración de derechos fundamentales en la fiscalización informática llevada a cabo por el empresario*, AS, nº 8, 2013 (BIB 2013\2377).

La sentencia concluye afirmando que «no consta en las actuaciones que el contenido de estos mensajes refleje aspectos específicos de la vida personal y familiar del trabajador, sino únicamente información relativa a la actividad empresarial, cuya remisión a terceros, conforme a la Sentencia recurrida, implicaba una transgresión de la buena fe contractual». Debe resaltarse, no obstante, que la actuación empresarial venía precedida de una sospecha previa, de modo que el empleador buscaba pruebas para demostrar el incumplimiento, y no había procedido a un control general e indiscriminado del ordenador de todos los trabajadores.

La jurisprudencia ordinaria camina en la misma dirección. En efecto, la STS de 6-10-2011¹⁹, presuponiendo la prohibición previa empresarial, ya afirmó que «si no hay derecho a utilizar el ordenador para usos personales, no habrá tampoco derecho para hacerlo en unas condiciones que impongan un respeto a la intimidad o al secreto de las comunicaciones, porque, al no existir una situación de tolerancia del uso personal, tampoco existe ya una expectativa razonable de intimidad y porque, si el uso personal es ilícito, no puede exigirse al empresario que lo soporte y que además se abstenga de controlarlo». De este modo, se legitiman los controles empresariales a través de «programas espía».

Es una doctrina que coincide sustancialmente con la elaborada por el TEDH, ya que ese Tribunal considera que en ausencia de una advertencia previa sobre el control del uso, el trabajador tiene una «expectativa razonable de privacidad» cuando utiliza los medios empresariales, y, por tanto, la obtención y el almacenamiento de información personal relativa al uso del teléfono o de internet sin conocimiento del trabajador son contrarios al derecho al respeto de la vida privada, salvo que se demuestre una justificación objetiva y razonable²⁰. Tanto el TC como el TS —así como la Agencia Española de Protección de Datos²¹— deducen de esa doctrina que en presencia de una política empresarial restrictiva la expectativa de privacidad desaparece.

4. ¿NUEVO CRITERIO JURISPRUDENCIAL O DOCTRINA DIFERENTE PARA EL CONTROL DEL ORDENADOR Y DE OTROS MEDIOS EMPRESARIALES?

La jurisprudencia más reciente sobre el control empresarial de los medios informáticos puestos a disposición del trabajador genera dudas razonables so-

¹⁹ Rcu. 4053/2010.

²⁰ Vid. STEDH *Copland vs. Reino Unido* (de 3-4-2007, recurso 62617/00), apartado 42.

²¹ Vid. http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/conceptos/common/pdfs/2009-0582_Tratamiento-de-datos-del-correo-electr-oo-nico-de-los-trabajadores-por-el-empresario.pdf.

bre la vigencia de los criterios previamente asentados en relación con otras herramientas de trabajo, porque en esos casos precedentes –no conocidos por el TC, cierto es– el control no dependía, o al menos no de manera tan evidente, de la existencia de unas previas y precisas instrucciones sobre el uso personal, y, más concretamente, de una prohibición expresa de su utilización con fines particulares. En cambio, el TC, y también el TS, advierten que la prohibición empresarial expresa de uso personal del ordenador elimina la expectativa de privacidad, y por tanto legitima un control más intenso sobre el contenido, inclusive el correo electrónico, porque la supresión de la expectativa de privacidad desactiva la tutela que proporcionan el derecho a la intimidad y el derecho al secreto de las comunicaciones.

En principio, tanto el TC como el TS parecen referirse exclusivamente a los medios informáticos, por lo que no es claro que esta doctrina pueda extrapolarse a otros supuestos distintos. Así, la jurisprudencia relativa a la instalación de cámaras u otros aparatos de control y vigilancia no se ha visto afectada por estas nuevas sentencias, porque es una doctrina que se construye a partir de premisas distintas (no se trata de herramientas de trabajo). También resulta evidente que los registros sobre la persona y efectos del trabajador, e incluso sobre la taquilla, siguen otros parámetros. En el caso de los registros sobre la persona y los efectos del trabajador la expectativa de privacidad es máxima, y por ello deben cumplirse las garantías del art. 18 ET. También ha de llegarse a la misma conclusión respecto de la taquilla, pues, por más que se trate de una propiedad empresarial, el contenido se presupone personal, y no puede considerarse como una herramienta de trabajo susceptible de control ordinario para evitar una mala utilización.

Ahora bien, determinadas herramientas de trabajo distintas del ordenador pueden ser utilizadas con fines personales, y se suscitan dudas acerca de la aplicación analógica de la doctrina antes expuesta. Piénsese en la utilización del teléfono móvil (no sólo en relación con las llamadas o mensajes, pues los *smartphones* disponen de conexión a internet, y acceso por tanto a correo electrónico y redes sociales), o incluso del teléfono fijo en el puesto de trabajo. Entra en juego en estos casos el art. 20 ET, y no el 18 ET, pues se trata del control de la actividad laboral.

En aplicación de la última doctrina jurisprudencial podría defenderse, por ejemplo, que en presencia de una prohibición explícita sobre el uso de medios empresariales con fines personales el empleador está legitimado para grabar todas las llamadas entrantes y salientes desde el teléfono fijo o móvil propiedad de la empresa, de modo que las conversaciones sean grabadas y susceptibles de consulta en cualquier momento. Siguiendo el mismo argumento, el empleador podría acceder a todos los mensajes de correo electrónico, así como a los mensajes enviados o recibidos por SMS o a través de otros programas de

mensajería (como el Whatsapp). En la medida en que el trabajador no dispone de una «expectativa de privacidad», el canal de comunicación debería considerarse «abierto», y susceptible por tanto de control y vigilancia empresarial, al igual que el ordenador.

Sin embargo, una interpretación de esa índole colisiona, en cierta medida, con la respuesta que el TS ofreció para el control de la actividad de *telemarketing*²², pues, aunque admitió la monitorización, valoró especialmente la proporcionalidad de la medida empleada, que implicaba controles aleatorios (un 0,5%) y limitados a las llamadas entrantes –no a las salientes–, y el hecho de que las especiales características de la actividad hacían imprescindible ese control para verificar el correcto cumplimiento de las obligaciones laborales por parte del trabajador. Es razonable suponer que en el caso de trabajadores no dedicados a actividades de venta telefónica, o que no desarrollen el núcleo de su prestación laboral a través del teléfono proporcionado por la empresa, las limitaciones para la monitorización de las conversaciones habrían resultado mayores. En cambio, a partir de la jurisprudencia relativa al uso del ordenador cabría defender, sin mayores dificultades, la legitimidad de la grabación de todas las conversaciones telefónicas en cualquier sector de actividad o puesto de trabajo, con las únicas condiciones de que la herramienta o instrumento utilizado sea propiedad empresarial y haya existido una prohibición expresa de uso personal; el espacio para la «propia esfera de desenvolvimiento del individuo» (STC 98/2000) quedaría, pues, notablemente reducido.

Nótese, asimismo, que la doctrina relativa a la vigilancia del uso del ordenador no se asienta en los criterios que tradicionalmente había manejado la jurisprudencia constitucional. En la construcción de la doctrina relativa a la colisión de los derechos fundamentales con los intereses empresariales el TC siempre había tenido presente que el medio de control no resultase especialmente invasivo, y, a modo de ejemplo, en el caso de la utilización de cámaras distinguía entre la captación exclusiva de la imagen y la captación de imagen y sonido, aduciendo que «la implantación del sistema de audición y grabación

²² «Si el teléfono controlado se ha puesto a disposición de los trabajadores como herramienta de trabajo para que lleven a cabo sus funciones de telemarketing y a la vez disponen de otro teléfono para sus conversaciones particulares, si, como se ha apreciado, los trabajadores conocen que ese teléfono lo tienen sólo para trabajar y conocen igualmente que puede ser intervenido por la empresa, si además la empresa sólo controla las llamadas que recibe el trabajador y no las que hace, si ello lo realiza de forma aleatoria –un 0,5%–, y con la finalidad exclusiva de controlar la buena realización del servicio para su posible mejora, la única conclusión razonable a la que se puede llegar es a la de que se trata de un control proporcionado a la finalidad que con el mismo se pretende, en el sentido antes indicado. En ese mismo sentido se trata de un control que es necesario puesto que no se conoce otro medio 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–»; cfr. STS de 5-12-2003 (rcud. 52/2003).

no ha sido en este caso conforme con los principios de proporcionalidad e intervención mínima que rigen la modulación de los derechos fundamentales por los requerimientos propios del interés de la organización empresarial»²³.

La jurisprudencia relativa a la utilización del ordenador prescinde de ese principio de «intervención mínima», puesto que –al menos en apariencia– permitiría instalar «programas espía», o habilitar medios para el control exhaustivo del uso del ordenador, de modo que el empleador pueda conocer todos los archivos que contiene, las páginas web visitadas, el contenido de los correos electrónicos y, en general, cualquier actividad o interacción del trabajador con el ordenador, lo que resulta difícilmente conciliable con el principio de proporcionalidad²⁴. La doctrina científica ya ha advertido que el test de proporcionalidad no parece necesario «cuando se ha afirmado por un lado la existencia de un derecho de control del empresario, y por otro lado la inexistencia en el caso de un ámbito protegido de intimidad del trabajador»²⁵.

Por consiguiente, el TC parece admitir -implícitamente- que el control y vigilancia empresarial sobre la actividad del trabajador puede revestir grados distintos en función de las circunstancias. Es posible, como ya se ha dicho, que esta última doctrina deba vincularse inescindiblemente a los dos supuestos de hecho que debía resolver el TC, y que deba por tanto renunciarse a crear reglas generales a partir de argumentos elaborados para casos muy particulares. No obstante, la lectura de ambas sentencias permitiría defender que las facultades empresariales se intensifican cuando se pretende controlar el uso de las herramientas empresariales puestas a disposición del trabajador, especialmente si se trata de medios informáticos. La implantación de mayores cautelas parece responder a un temor de uso desviado, con la asunción de que la potencialidad lesiva para los intereses empresariales resulta elevada.

Si esta línea interpretativa se consolida será necesario un rediseño de los contornos tradicionales de los derechos a la intimidad y al secreto de las comunicaciones. Y si el perímetro de tales derechos debe reformularse, la nueva configuración seguramente afectará a la utilización de los medios no informáticos. En último término, si se admite que un empleador puede comprobar el contenido del ordenador utilizado por el trabajador, incluido el correo electrónico, no habría ninguna razón para negar que también puede monitorizar el contenido de todas las conversaciones telefónicas que mantengan sus empleados desde el teléfono fijo o móvil suministrado por la empresa, e incluso los mensajes enviados y recibidos por correo electrónico, SMS o programas

²³ Cfr. STC 98/2000, de 10 de abril.

²⁴ Vid. A.B. Muñoz Ruiz, *Instrumentos informáticos de utilización generalizada en la empresa o medios de uso personal y secreto de las comunicaciones (Comentario a la STC 241-2012, de 17 de diciembre de 2012)*, Justicia Laboral, nº 55, pp. 100 y ss.

²⁵ Cfr. A. Martín Valverde, *Uso extralaboral del correo electrónico empleando medios informáticos de la empresa. Control empresarial: requisitos*, AL, n 2, 2014, pág. 190.

de mensajería instantánea. Hasta el momento, una intervención de ese calibre exigía garantías extraordinarias o adicionales, pero la última jurisprudencia del TC suscita múltiples incertidumbres. No conviene olvidar que el uso personal del teléfono móvil, de una tableta o de un ordenador portátil puede tener lugar fuera del tiempo y lugar de trabajo, y en muchas ocasiones no se genera coste o perjuicio alguno para la empresa. En consecuencia, resulta imprescindible una reflexión detenida sobre el alcance y consecuencias de este nuevo criterio jurisprudencial y, en concreto, sobre los efectos que puede desplegar la prohibición empresarial de uso personal de los medios empresariales.

5. REDISEÑANDO LOS LÍMITES AL CONTROL EMPRESARIAL DEL ORDENADOR: ALCANCE Y EFECTOS DE LA PROHIBICIÓN EMPRESARIAL DE USO PERSONAL DEL ORDENADOR

La jurisprudencia constitucional sobre el control del uso del ordenador pivota, como se ha dicho, sobre dos premisas. En primer lugar, la titularidad empresarial del ordenador. Y en segundo lugar, la existencia de una política empresarial clara en relación con su utilización. En resumen, si el ordenador es propiedad de la empresa y sólo puede ser utilizado como herramienta de trabajo no hay riesgo de que el control revele datos personales o sensibles, por cuanto el trabajador es consciente de que el ordenador podría ser objeto de control, y por consiguiente su contenido conocido por el empleador en cualquier momento, salvo que se demuestre tolerancia empresarial respecto del uso personal.

El argumento, así concebido, podría dar lugar a un resultado desproporcionado, pues llevado al extremo atribuye al empleador unos poderes exorbitantes. Obviamente, no cabe negar que el poder de dirección empresarial permite establecer límites al uso de los medios empresariales con fines personales, pero esa política empresarial no puede legitimar cualesquiera instrumentos de control, máxime cuando en ocasiones tal política, propiamente dicha, no existe, ni se identifican previamente los eventuales medios de control. E incluso cuando la prohibición existe, es frecuente que se admita una utilización “excepcional” de esos medios empresariales con propósito personal²⁶, aunque los tribunales ordinarios suelen mantener que la prohibición general elimina la expectativa de privacidad, a pesar de esos resquicios²⁷.

El argumento elaborado por la jurisprudencia constitucional resulta atractivo, y también operativo en muchas situaciones, pero no conviene olvidar las

²⁶ Así sucede en el supuesto de hecho resuelto por la STSJ de Madrid de 16-12-2013 (recurso 1237/2013), aunque el Tribunal entiende que la prohibición resultaba clara y terminante.

²⁷ Vid. STSJ de Valencia de 25-6-2013 (recurso 1111/2013).

características de los supuestos de hecho que motivaron esa doctrina. Obviamente, el TC no afirma, ni defiende, que la prohibición empresarial previa, por sí sola, pueda tener como resultado la minimización de los derechos fundamentales a la intimidad y al secreto de las comunicaciones. Y a la inversa, la ausencia de una prohibición expresa de uso personal de los medios empresariales no debería justificar una utilización de tales instrumentos sin sujeción a reglas, ni impide desde luego el control empresarial. A la postre, las dos partes ligadas por el contrato de trabajo deben comportarse conforme a la buena fe, principio que el trabajador debe respetar al utilizar los instrumentos o herramientas que pone a su disposición la empresa, pero que también limita las posibilidades de control del empleador.

La doctrina sentada por el TC será a buen seguro enriquecida cuando ese Tribunal conozca de supuestos de hecho con otros rasgos diferentes, y alguna de las afirmaciones que contienen estas sentencias será matizada, porque la interpretación y aplicación del tenor literal podría dar lugar a actuaciones desproporcionadas. En este sentido, la política empresarial previa adquiere una relevancia desmesurada, y sus efectos desbordan su ámbito natural de actuación, que en este contexto debería vincularse a la modulación del poder disciplinario, y no a las facultades de control y vigilancia de la actividad laboral.

Las SSTC 241/2012 y 170/2013, sin embargo, vinculan las facultades de control empresarial con la existencia de una previa prohibición empresarial, con las dudas que ello genera. Por un lado, no sólo se admite el control específico destinado a detectar un incumplimiento, sino un control genérico, ya que el objeto de esa actividad de vigilancia no se concreta. Por otro, se genera la apariencia de que en ausencia de prohibición la utilización de los medios empresariales con fines personales se tolera, seguramente atendiendo a esa doctrina del TEDH en relación con la expectativa de privacidad, doctrina, por cierto, elaborada a partir del concepto de *privacy* anglosajón, que no es exactamente coincidente con el contenido del derecho a la intimidad reconocido por el art. 18 CE, y cuya extrapolación al ordenamiento español habría requerido, seguramente, de mayores matices.

A partir de las sentencias citadas podría entenderse que la prohibición de uso personal de medios empresariales incide tanto en la posibilidad de control como en el objeto y medios para proceder al mismo. Dicho de otro modo, esa prohibición activaría o legitimaría el control, y, además, ampliaría los modos de ejercerlo. Así configurada, la prohibición empresarial despliega efectos hasta ahora desconocidos, porque las facultades de control y vigilancia, y por extensión el poder de dirección, no requerían de advertencias previas, siempre, desde luego, que se respetasen las condiciones mínimas vinculadas al respeto a los derechos fundamentales y a la buena fe.

En verdad, la voluntad empresarial no debería justificar el control del contenido del ordenador, ni ampliar las facultades del empleador con tal finalidad,

de tal forma que pueda comprobar el contenido de los correos electrónicos enviados o recibidos. Ello no cercena, en absoluto, sus facultades de vigilancia. En esta línea, conviene insistir en que el control y vigilancia de la actividad del trabajador no requiere, de ordinario, un aviso previo ni sobre el hecho mismo del control, ni sobre el medio empleado, pues el interés empresarial en la constatación del cumplimiento de las obligaciones laborales es evidente, y los medios de control pueden ser múltiples, aunque debe garantizarse en todo caso el respeto a los derechos fundamentales del trabajador. De ahí que el TC se haya ocupado con mayor intensidad de delimitar los medios de control y vigilancia que pueden ser utilizados lícitamente por el empleador. En cambio, en relación con el ordenador se presta menos atención al método de indagación y más a la constatación real del incumplimiento.

Posiblemente, la necesidad de una prohibición empresarial previa que actúe como presupuesto del control es un criterio jurisprudencial que en origen pretendía proteger al trabajador. Comoquiera que prácticamente ninguna empresa había realizado tales advertencias, los controles se entendían ilegítimos. Sin embargo, la difusión del criterio conllevará, obviamente, que el número de empresas que prohíban expresamente el uso personal de los medios empresariales aumente, siendo previsible que a corto o medio plazo la práctica totalidad de empleadores adopten esa posición, máxime si se entiende, como se desprende de la jurisprudencia constitucional, que la tipificación de una infracción en el convenio equivale a esa política empresarial. Desde esa perspectiva, el criterio jurisprudencial que nació como garantía generará un efecto perverso, pues una mera declaración empresarial permitirá el control indiscriminado de todos los medios puestos a disposición del trabajador, sin que, hasta el momento, se haya perfilado con claridad si el test de constitucionalidad sigue plenamente operativo.

De este modo, el criterio inicialmente garantista podría derivar en la práctica anulación de los efectos de dos derechos fundamentales (intimidad y secreto de las comunicaciones) a partir de una mera declaración de voluntad del empleador, lo que daría lugar a resultados desproporcionados. Parece evidente que la jurisprudencia constitucional seguirá evolucionando, y que no cabe desligar las sentencias citadas del caso concreto. Con las dificultades que conlleva hacer predicciones de futuro, es probable que esa evolución transite por una dirección similar a la que se aprecia en la jurisprudencia ordinaria relativa al finiquito. Recuérdese que en un primer momento el Tribunal Supremo entendía que ese documento de saldo y finiquito tenía carácter liberatorio si la declaración en él plasmada era suficientemente clara y terminante, lo que supuso de inicio sentencias favorables a los trabajadores. No obstante, cuando los documentos se aquilataron con expresiones suficientemente claras y terminantes, el Tribunal Supremo introdujo numerosos matices que han acabado

por desvincular el efecto liberatorio de la literalidad del documento, haciendo primar los aspectos materiales sobre los formales.

Haciendo un paralelismo con ese criterio jurisprudencial, la doctrina relativa al uso personal de los medios empresariales se encuentra, seguramente, en una etapa inicial o embrionaria, que dota de una eficacia inusitadamente elevada a un aspecto meramente formal, como es la prohibición de uso personal de los medios empresariales. Si a raíz de esa declaración unilateral se generalizan prácticas exorbitantes, con controles exhaustivos basados, exclusivamente, en la previa prohibición, el TC introducirá los pertinentes matices, poniendo el acento en la legitimidad de los medios de control. A la postre, los supuestos de hecho que resuelven las sentencias citadas cuentan con tales peculiaridades que no debería interpretarse que la prohibición empresarial permite todo control y por cualquier medio. Ni, a la inversa, que en ausencia de prohibición la tolerancia es absoluta.

A corto o medio plazo, el TC quizás exigirá que la política empresarial sea mucho más precisa, indicando específicamente cómo y cuándo se efectuarán los controles. En presencia de esa mayor concreción, a buen seguro se entenderá que la expectativa de privacidad desaparece, pues el trabajador conoce que el control puede llevarse a cabo y el medio de control empleado. Todo dato, documento o conversación se encontraría en un canal abierto, y por tanto no amparado ni por el secreto de las comunicaciones ni por el derecho a la intimidad.

Pero un argumento de esta índole, aunque proporciona mayor seguridad jurídica, resultaría difícilmente compatible con la protección de los derechos fundamentales, a salvo de que se entienda que la política empresarial previa permite eludir el test de constitucionalidad, y en particular valorar la necesidad y proporcionalidad de la medida. Obviamente, no cabe duda de que el control del ordenador del trabajador resulta habitualmente idóneo para comprobar si se ha producido o no un incumplimiento de ciertas obligaciones laborales, pero el criterio de la necesidad y el de la proporcionalidad exigen un razonamiento más aquilatado, donde la finalidad del control se convierte en esencial.

Cuestión distinta es que mediando prohibición no cabe argumentar tolerancia empresarial, y el mero incumplimiento resultaría sancionable, sin las matizaciones que sin duda proceden cuando la política empresarial no se haya explicitado²⁸. Dicho en otros términos, la prohibición empresarial previa debería conectar con la política empresarial para sancionar, pero no con la política empresarial para vigilar. Las facultades de control y vigilancia no pueden verse mediatizadas por el mero hecho de que el empleador no prohíba expresamente una conducta que naturalmente supone un incumplimiento laboral, pero esas

²⁸ Vid. M. Carrasco Durán, *El Tribunal Constitucional y el uso del correo electrónico y los programas de mensajería en la empresa*, Revista Aranzadi Doctrinal nº 9/2014 (BIB 2013\2695).

advertencias previas pueden resultar determinantes en un estadio posterior, el de la sanción tras el descubrimiento de la infracción. De este modo, la utilización personal de medios empresariales podría no resultar sancionable cuando fuera inocua, por no conllevar un perjuicio para el empleador, ni una disminución de rendimiento apreciable. Obviamente, no cabe defender que el trabajador tenga derecho a utilizar herramientas empresariales con fines personales, pero, en general, los tribunales vienen advirtiendo que determinados incumplimientos de escasa entidad (*v.gr.*, faltas menores de puntualidad) que no generan daño alguno para el empresario no son sancionables si se aprecia cierta tolerancia empresarial con esas conductas, que los usos sociales legitimarían. Por consiguiente, el control empresarial sería posible, pero el uso personal de los medios empresariales no siempre resultaría sancionable.

Por supuesto, el empleador puede modificar ese grado de tolerancia, e incluso suprimir cualquier generosidad, pero para ello debe advertir explícitamente a los trabajadores sobre esa decisión. En esos términos, la prohibición de uso de los medios o herramientas empresariales con fines personales no incidiría en sí misma sobre las posibilidades de control, sino sobre la eventual reacción ante un incumplimiento, ya que permitiría sancionar esa conducta aunque no se originase daño o perjuicio alguno para la empresa. El poder de dirección empresarial permite organizar los recursos, y dar las pertinentes órdenes e instrucciones, sin que el trabajador pueda aducir el uso inocuo o los usos sociales cuando contraviene una orden empresarial directa.

En suma, la vulneración de los derechos a la intimidad y al secreto de las comunicaciones no tiene lugar por el mero control de la actividad del trabajador, sino por el objeto de ese control y la finalidad perseguida con la actuación empresarial. Cuando el medio utilizado resulte especialmente invasivo habrá que declarar la vulneración de los correspondientes derechos fundamentales, pero ello no prejuzga el derecho empresarial al control y vigilancia de la actividad, sino únicamente el modo de actuación. La política empresarial previa, así pues, despliega los efectos que le son propios en el marco de las facultades disciplinarias, eliminado el margen de tolerancia, pero no habría de incidir en las posibilidades de control, ni en los medios a disposición del empresario para efectuar tal vigilancia. Las facultades de control derivan, por supuesto, del poder de dirección, y esas facultades deben depender, esencialmente, de la finalidad del control. En este sentido, la existencia o no de sospecha previa resulta determinante.

6. FACULTADES DE CONTROL EMPRESARIAL PARA CONSTATAR LA VERACIDAD DE UNA SOSPECHA

El poder de dirección empresarial atribuye al empleador una serie de facultades, y entre ellas las de control y vigilancia. Ahora bien, es menester encontrar un equilibrio entre las legítimas facultades del empleador y los derechos que mantiene el trabajador, como persona, en el ámbito de la relación laboral. Y para garantizar ese equilibrio parece aconsejable atender, principalmente, a la finalidad perseguida con el control, pues de esa circunstancia dependerán, en buena medida, los modos de actuación lícitos del empleador. En efecto, las posibilidades de control empresarial del ordenador dependen, esencialmente, del fin perseguido con ese control, toda vez que el empresario puede querer comprobar, meramente, si el trabajador ha utilizado las herramientas empresariales con exclusivos fines profesionales, o bien podría contar con una intención más específica, cual es la de constatar una sospecha de incumplimiento. Se trata, sin duda, de controles de diferente naturaleza, que el ordenamiento debería contemplar también de manera distinta. La finalidad perseguida debería resultar determinante en el análisis de la legitimidad de los instrumentos empleados.

Obviamente, se presupone que los controles efectuados se desarrollan por voluntad unilateral del propio empleador, y sin consentimiento por tanto del trabajador. Ese consentimiento, de existir, valida en principio la actuación empresarial, si bien la eficacia del consentimiento del trabajador es una cuestión delicada, porque debería ser expreso, *ad hoc* –la habilitación genérica al empresario en el propio contrato suscita serias dudas de compatibilidad con los derechos fundamentales²⁹-, y no forzado por el temor a eventuales represalias; admitir el consentimiento tácito por la existencia de una previa advertencia empresarial sin oposición manifiesta no concuerda bien con la tutela reforzada que proporcionan los derechos fundamentales³⁰, salvo que de las circunstancias concurrentes pueda estimarse que el trabajador ha realizado actos de disposición sobre una información, en principio, íntima/privada. Pero desde luego no cabe inferir tal consecuencia del mero hecho de que el ordenador sea propiedad de la empresa.

En ausencia de ese consentimiento, debe aceptarse, como premisa de partida, que el empleador está legitimado para efectuar los controles pertinentes en orden a constatar si los trabajadores cumplen sus obligaciones laborales, por cuanto se trata de un componente esencial del poder de dirección. En esos términos, el control y la vigilancia de la actividad laboral no puede condicionarse, en modo alguno, a una previa advertencia empresarial sobre ese control y/o los

²⁹ Vid. P.H. Antonmattei, *NTIC et vie personne au travail*, Droit Social, n° 1, 2002, pág. 40.

³⁰ En sentido contrario, vid. A.V. Sempere Navarro y C. San Martín Mazzucconi, *Nuevas tecnologías y relaciones laborales*, Aranzadi, Pamplona, 2002, pp. 68 y ss.

medios empleados a tal efecto. El empleador puede proceder a esa vigilancia aun en ausencia de advertencias previas, obviamente, pero habrá de utilizar medios adecuados. El problema jurídico, así pues, no consiste en determinar si el empleador puede o no controlar, sino qué medios están a su disposición para efectuar la vigilancia, y esos medios deberán estar directamente conectados con la finalidad perseguida.

En el caso de que el empleador cuente con una sospecha fehaciente de incumplimiento, el control empresarial puede ejercerse de manera más intensa. Resulta imprescindible, desde luego, acreditar la existencia y verosimilitud de esa sospecha, que no puede convertirse en un mero pretexto para un control indiscriminado o exorbitante. Pero ante una sospecha fundada y razonable, la finalidad del control consiste, precisamente, en verificar si el incumplimiento se ha producido efectivamente, y conseguir por tanto las pruebas pertinentes. Si esa es la finalidad, y desde luego parece legítima, es lícito verificar el contenido del ordenador y monitorizar su uso –así como grabar las conversaciones telefónicas-, siempre que la medida resulte necesaria y proporcional.

Es decir, cuando no existan otros medios menos invasivos para constatar tal incumplimiento y cuando la comprobación se limite a datos, documentos o archivos vinculados con esa conducta ilícita, el empleador estará legitimado para constatar el contenido. Pero resulta imprescindible establecer las necesarias cautelas, pues en el caso de que las conversaciones, archivos o documentos no guarden relación alguna con el trabajo y se presenten como inidóneos para el fin pretendido (*v.gr.*, conversaciones telefónicas o telemáticas con familiares, datos bancarios personales del trabajador, según los casos, etc.), la comprobación del contenido no es necesaria para el fin pretendido y, por tanto, no se justifica.

En estos términos, una vez constatada la idoneidad, necesidad y proporcionalidad de la medida resulta admisible un control del contenido del ordenador, o de los correos electrónicos, con independencia de que exista o no política empresarial previa sobre el uso de medios empresariales con fines personales. Aunque el art. 18 ET no resulte en puridad aplicable a estas situaciones, no debe olvidarse que el legislador acepta, mediando las debidas garantías, el registro de las «taquillas y efectos particulares» de los trabajadores sin previas advertencias ni prohibiciones explícitas, por lo que resulta difícil rechazar el control sobre los instrumentos o herramientas de su propiedad puestos a disposición de los empleados, ámbito en el que la potencialidad lesiva del derecho a la intimidad es muy inferior.

Obviamente, el test de proporcionalidad debería efectuarse *a priori*, porque el control empresarial no puede legitimarse en función de que se descubra o no el incumplimiento. La medida puede resultar idónea, necesaria y proporcional aun cuando el resultado sea infructuoso, y podrá ser innecesaria y

desproporcionada –pese a su idoneidad- incluso aunque demuestre el incumplimiento. Desde esta perspectiva, el empleador deberá acreditar, en primer lugar, que existen indicios razonables para la sospecha, y, en segundo término, que la medida de control que pretende utilizar es adecuada para verificar el incumplimiento, y no existe un medio de eficacia similar menos invasivo o con menor riesgo para la intimidad del trabajador. En ese contexto, el control del contenido del ordenador resulta legítimo, con independencia del resultado que proporcione esa vigilancia.

En fin, cuando la medida se muestre como eficaz, pero no se hayan explorado alternativas menos invasivas, aumenta el riesgo de que el empleador acceda a información o datos que no debería conocer, porque deberían estar al margen de sus facultades ordinarias de control, y ese conocimiento injustificado podría conducir a sanciones o acarrear perjuicios al trabajador por motivos diferentes a la finalidad del control. Piénsese, por ejemplo, que a resultados del control el empleador comprueba correos electrónicos del trabajador dirigidos a un familiar cercano en el que critica a sus superiores jerárquicos, sin traspasar la frontera de las ofensas verbales o físicas, o descubre que el trabajador padece una enfermedad o que va a tener un hijo. Es una información que, desde luego, el trabajador no pretendía que el empleador conociera, y la consideración del canal como “abierto” en función de que exista o no prohibición empresarial es un artificio jurídico contrario a las mínimas garantías que deberían rodear al derecho a la intimidad, siempre que se acepte que este derecho mantiene alguna virtualidad en el marco de una relación de trabajo.

7. CONTROLES EN AUSENCIA DE SOSPECHA: LA FINALIDAD COMO ELEMENTO DETERMINANTE DE LAS FACULTADES EMPRESARIALES

La sospecha previa concede al empleador facultades de vigilancia más intensas, por cuanto sólo a través de determinados mecanismos podrá constatar fehacientemente si el trabajador cumple sus obligaciones laborales. En cambio, en ausencia de sospecha el empleador no busca verificar un incumplimiento concreto, sino simplemente cerciorarse sobre el correcto quehacer laboral de los trabajadores. Se trata, por tanto, de controles genéricos, que el empleador puede efectuar en el marco de sus facultades de control y vigilancia ordinarias, advierta o no expresamente a los trabajadores. Lógicamente, esos controles deben respetar las exigencias constitucionales, pero el control no es, ni puede considerarse, ilegítimo por el mero hecho de que no se haya preavisado. Es menester, desde luego, valorar las circunstancias concurrentes en el caso, pero debe admitirse, por un lado, que el empleador conserva sus facultades de con-

trol y vigilancia aunque no haya prohibido el uso de medios empresariales con fines personales, y, en segundo lugar, que muchas medidas de control verían frustrada su finalidad si el interesado es previamente advertido³¹.

Ahora bien, los controles deberían superar en todos los casos el test de constitucionalidad (idoneidad, necesidad y proporcionalidad), de modo que no resultan admisibles cuando no encajen en ese marco, con independencia de la advertencia empresarial previa. La virtualidad de esa política empresarial previa debería vincularse, exclusivamente, con la tolerancia empresarial y el uso inocuo, sin modular o matizar el alcance de los derechos fundamentales a partir de una dudosa conexión con la denominada expectativa de privacidad.

La política empresarial previa de carácter restrictivo, por tanto, no atribuye mayores facultades de control. No es necesario, ni proporcional, que el empleador se arrogue la facultad de control exhaustivo sobre cualquier herramienta o instrumento que utilice el trabajador, pues en tal caso debería admitirse que el empleador puede efectuar un control minucioso y permanente sobre toda la actividad del trabajador en ejecución de su trabajo, inclusive, por ejemplo, a través de cámaras de grabación de video y audio enfocadas al puesto de trabajo con la exclusiva finalidad de control de la actividad laboral. Si se acepta que este último medio es lesivo (de la intimidad, o en su caso de la propia imagen, vinculados ambos derechos con la dignidad), no hay razón para negar que resulta igualmente invasiva la grabación de todas las conversaciones telefónicas o la monitorización absoluta del ordenador que utiliza el trabajador (instalando *keyloggers* o, en general, programas espía, incluso aunque el trabajador esté advertido).

Los medios de control deben, desde luego, vincularse al objetivo y finalidad pretendidos por ese control, y sólo en supuestos excepcionales el empleador puede demostrar un interés legítimo para comprobar el contenido de las conversaciones que el trabajador mantenga a través de programas de mensajería instantánea o de correos electrónicos (asumiendo, obviamente, que el ordenador sea propiedad de la empresa y el correo electrónico corporativo). Cuando el empleador no puede demostrar ese interés legítimo y la finalidad del control puede satisfacerse con medios menos invasivos, los principios de necesidad y proporcionalidad se imponen.

En efecto, el hecho de que el ordenador sea propiedad de la empresa y pueda ser catalogado como una herramienta de trabajo no permite al empresario

³¹ Vid. STSJ de Murcia de 13-5-2013 (recurso 129/2013), que afirma que «tampoco parece razonable que la empresa, ante la comisión de faltas laborales, desvele las medidas de control y de seguridad tendentes a prevenir a disuadir o a posibles infractores, cuando se refieren a vigilancia sobre mercancías, que pueden ser sustraídas, o localización de vehículos en sus rutas laborales en un ámbito que no se puede considerar de intimidad o privacidad o de estricto control de una persona con un fin ilegal».

realizar un control exhaustivo, puesto que el derecho de propiedad no puede imponerse de tal forma a los derechos fundamentales³²; de lo contrario, se llegaría al absurdo de pretender que el empresario está legitimado para conocer el contenido del correo postal si el sobre y/o el sello son de su propiedad³³. Es menester, por tanto, limitar «la intromisión empresarial en los procesos comunicativos» y, posteriormente, adoptar «sistemas de drenaje del resultado»³⁴.

Por ello, las facultades del empleador deben restringirse cuando la finalidad consista, meramente, en constatar si el trabajador hace un uso correcto de los medios empresariales. En efecto, cuando no se pretende comprobar un concreto incumplimiento, sino en general la utilización de esas herramientas, el empresario estaría legitimado para comprobar los destinatarios –y la duración– de las llamadas telefónicas que efectúa el trabajador utilizando medios empresariales (y nunca si el trabajador realiza la llamada desde su propio teléfono³⁵), así como para verificar los destinatarios de los mensajes de correo electrónico enviados por el trabajador (y los remitentes de los mensajes que recibe). En caso de duda, podría instarse al trabajador a que identificara al destinatario y probase el carácter laboral/profesional de la conversación. Lo mismo ocurriría con los archivos o documentos almacenados en el ordenador, así como con los correos electrónicos enviados o recibidos. El empleador no necesita conocer el contenido para averiguar si el trabajador realiza un uso personal, e incluso hay herramientas sencillas y escasamente invasivas para constatar el tiempo que el trabajador ha dedicado a esas tareas personales en horario de trabajo. El control del contenido, así pues, no es necesario para constatar ese uso personal, y desde luego tampoco es proporcional si ese es, exclusivamente, el fin perseguido.

En este sentido, los derechos a la intimidad y al secreto de las comunicaciones (que deben incluir las telemáticas porque el art. 18.3 CE no recoge un *numerus clausus* y la información, al menos habitualmente, se transmite a través de la infraestructura telefónica)³⁶ suponen un límite infranqueable para

³² Vid. A. Desdentado Bonete, *Contrato de trabajo y nuevas tecnologías. Una nota sobre algunas cuestiones de actualidad: prueba electrónica, garantías de la intimidad y uso sindical del correo electrónico*, Revista del Poder Judicial, nº 88, 2009, pp. 250 y ss.; I. Marín Alonso, *El uso por los trabajadores de las comunicaciones electrónicas en la empresa: ¿se encuentran protegidas por el derecho al secreto de las comunicaciones?*, Comunicación presentada al XXIV Congreso Nacional de Derecho del Trabajo y de la Seguridad Social.

³³ Vid. A. V. Sempere Navarro y C. San Martín Mazzucconi, *Nuevas tecnologías y relaciones laborales*, Aranzadi, Pamplona, 2002, pp. 83 y ss.; A. Arias Domínguez y F. Rubio Sánchez, *El derecho de los trabajadores a la intimidad*, Thomson-Aranzadi, Pamplona, 2006, pp. 157 y ss.

³⁴ Cfr. D. Martínez Fons, *El poder de control del empresario en la relación laboral*, CES, Madrid, 2002, pp. 179-180.

³⁵ Vid. C. Radé, *Nouvelles technologies de l'information et de la communication et nouvelles formes de subordination*, Droit Social, nº 1, 2002, pág. 31.

³⁶ Igual posición se defiende en el ordenamiento italiano; vid. S. Fernández Sánchez, *Variaciones sobre el poder de control a distancia: el espejo de la madrastra*, RL, nº 19-20, 2005, pp. 92 y ss.

controlar el contenido de las conversaciones telefónicas³⁷, salvo excepciones, como la atención telefónica, en la que se han admitido controles aleatorios para constatar que se dispensa un trato correcto al cliente, como se dijo. No conviene olvidar que la factura telefónica informa de los números de teléfono a los que el trabajador llama, dato que desde luego el trabajador conoce, por lo que, en este caso, la expectativa de privacidad sobre los interlocutores quiebra. Además, la factura se envía directamente al empleador, que es quien la abona, y no puede generarse tal expectativa de privacidad respecto de documentos (facturas) que nunca han estado a disposición del trabajador ni depositados en su ámbito propio de decisión. No hay, pues, intromisión ilegítima del empleador, porque ni siquiera necesita establecer medidas de control para conseguir esa información, de la que es legítimo poseedor³⁸.

En relación con el correo electrónico, y por analogía, el empleador estaría facultado para comprobar la bandeja de entrada y salida, pero no el contenido de los correos, salvo que los conozca, claro está, porque alguno de los remitentes o destinatarios le proporcione esa información (o porque los reciba directamente)³⁹. La prohibición empresarial previa sobre uso personal de los medios empresariales no supone una apertura del canal de comunicación, ni tampoco que el trabajador, consciente de ese control, renuncie a su intimidad cuando utiliza esa vía. El argumento, que difícilmente podría admitirse para las llamadas telefónicas o correos electrónicos salientes, no puede extenderse en ningún caso para los entrantes, porque el interlocutor –de ordinario alguien ajeno a la empresa- no ha prestado ningún consentimiento, ni explícito, ni implícito; su expectativa de privacidad no se ha roto, porque ni son trabajadores de la empresa, ni utilizan medios empresariales, ni han realizado acto alguno

³⁷ Vid. STS de 10-3-1990 (recurso de casación en interés de ley), en la que se declara no admisible una prueba consistente en «grabar una supuesta conversación telefónica entre el actor y una tercera persona no identificada, en la que aquél le ofrecía una cantidad de langostinos sustraídos a la empresa, mediante precio».

³⁸ Vid. M.F. Fernández López, “La intimidad del trabajador y su tutela en el contrato de trabajo”, en M.E. Casas Baamonde, F. Durán López y J. Cruz Villalón (Coord.), *Las transformaciones del Derecho del Trabajo en el marco de la Constitución Española*, La Ley, Madrid, 2006, pp. 645 y ss.; J. García Viña, *Relaciones laborales e internet*, RTSS (CEF), nº 223, 2001, pp. 54 y ss. En contra, admitiendo el control del contenido del mensaje por parte del empresario para comprobar el uso extralaboral, vid. L. Pacheco Zerga, *La dignidad humana en el Derecho del Trabajo*, Civitas, Madrid, 2007, pp. 267 y ss.

³⁹ Vid. A. Roig Batalla, «El uso de internet en la empresa: aspectos constitucionales», en A. Roig Batalla (Coord.), *El uso laboral y sindical del correo electrónico e internet en la empresa*, Tirant lo Blanch, Valencia, 2007, pp. 71 y ss.; M.N. Martínez Gayoso, *Relación de trabajo y nuevas tecnologías: algunos aspectos problemáticos del uso del correo electrónico por parte de los trabajadores en la empresa*, Tribuna Social, nº 203, 2007, pp. 27 y ss.

de disposición⁴⁰. No se olvide, asimismo, que muchos programas de correo electrónico agrupan los mensajes por conversaciones, de modo que la lectura de uno de esos mensajes permite acceder a los precedentes (tanto entrantes como salientes) con el mismo interlocutor.

El canal, en su caso, podría llegar a contar con un carácter «semiabierto» o con una apertura meramente unidireccional, pero esa es una interpretación demasiado alambicada. Lo relevante, desde luego, no es en sí misma la configuración del canal, sino la adecuación de los medios de control al fin perseguido con cada concreta actuación de vigilancia, toda vez que no cabe negar el carácter netamente privado, y potencialmente íntimo, de ciertos datos, documentos o conversaciones almacenados en el ordenador. Debe insistirse en que la constatación de que el trabajador ha utilizado el ordenador con fines personales no requiere, en modo alguno, una comprobación del contenido de los documentos allí archivados, ni tampoco del contenido de los correos electrónicos. Esa medida de control, aunque idónea, no es necesaria para alcanzar la finalidad perseguida, y desde luego tampoco proporcional.

Por consiguiente, los derechos a la intimidad y al secreto de las comunicaciones, tanto del trabajador como de las personas con las que intercambia mensajes, limitan las facultades empresariales de control del contenido del correo electrónico, que sólo se justificaría ante una sospecha fehaciente de incumplimiento, y respecto de aquellos mensajes en los que pueda presumirse razonablemente que se encontrará la prueba del incumplimiento. Un control generalizado del contenido de los correos electrónicos de todos los trabajadores basado meramente en una prohibición previa del uso del ordenador con fines personales resulta incuestionablemente contrario a los derechos fundamentales a la intimidad y al secreto de las comunicaciones.

En conclusión, a salvo de que concurra una sospecha de incumplimiento en los términos indicados, debe convenirse en que «resulta prácticamente imposible el deslinde *a priori* de lo que es inherente a la esfera personal del trabajador y lo que es estrictamente laboral»⁴¹, y por ello el control empresarial habrá de limitarse a la visualización de la bandeja de entrada (*inbox*), o las relativas a elementos enviados y eliminados (remitente y destinatario, a la postre), y con ello el empresario podrá deducir si se está realizando un uso

⁴⁰ Vid. T. De La Quadra-Salcedo Janini y B. Suárez Corujo, *¿Trabajadores incomunicados?: La deriva de la doctrina constitucional en torno a los márgenes de actuación empresarial en el control de las comunicaciones*, Comunicación presentada al XXIV Congreso Nacional de Derecho del Trabajo y de la Seguridad Social.

⁴¹ Cfr. M.F. Fernández López, “La intimidad del trabajador y su tutela en el contrato de trabajo”, en M.E. Casas Baamonde, F. Durán López y J. Cruz Villalón (Coord.), *Las transformaciones del Derecho del Trabajo en el marco de la Constitución Española*, La Ley, Madrid, 2006, pág. 645.

irregular de los medios empresariales⁴². Es cierto que la STC 114/1984, de 29 de noviembre, advirtió *–obiter dicta*, porque el asunto versaba sobre la licitud de presentar como prueba en el juicio una conversación grabada por uno de los interlocutores sin conocimiento del otro- que el secreto de las comunicaciones «no cubre sólo el contenido de la comunicación, sino también, en su caso, otros aspectos de la misma, como, por ejemplo, la identidad subjetiva de los interlocutores o de los corresponsales», pero llevando tal doctrina al extremo se vaciaría de contenido el poder de dirección, ya que el empresario no contaría con ningún medio fiable de control y vigilancia. Es claro que el empleador no puede indagar en la identidad de los destinatarios o remitentes de los mensajes –porque podría obtener información sensible, como la afiliación sindical, la ideología política o las creencias religiosas⁴³-, pero sí debe poder comprobar si tales destinatarios o remitentes son clientes o usuarios de la empresa, para dilucidar si la comunicación se inserta entre los cometidos profesionales del trabajador.

En relación con la navegación por internet, la diferencia resulta más difusa, pero parece claro que el empresario no sólo está legitimado para conocer la dirección de las páginas que el trabajador visita, sino también para acceder a ellas y comprobar su contenido, pues el secreto de las comunicaciones, o el derecho a la intimidad, no parece entrar en juego en este supuesto⁴⁴. En efecto, la página web no contiene, o al menos no hay razón que haga presuponer lo contrario, información confidencial del trabajador, y en todo caso es de libre acceso, por lo que no sería el empleador quien vulnerase el derecho a la intimidad. Cuestión distinta es que la decisión que el empresario tome debe estar basada en la repercusión laboral del uso no adecuado de internet, y no en que el contenido de las páginas visitadas sea más o menos reprobable a juicio del empleador.

No obstante, el control de la utilización de medios informáticos puede resultar exorbitante cuando la información que se obtiene excede de las páginas visitadas. En particular, los denominados «programas espía» tienen funcionalidades muy diferentes, y algunos de ellos detectan y recuerdan las combinaciones de teclas usadas por el trabajador (*keyloggers*), de modo que permiten averiguar las contraseñas utilizadas para acceder a determinados servicios (in-

⁴² Vid. D. Martínez Fons, “El uso y control del correo electrónico e internet en la empresa: aspectos laborales”, en A. Roig Batalla (Coord.), *El uso laboral y sindical del correo electrónico e internet en la empresa*, Tirant lo Blanch, Valencia, 2007, pp. 219 y ss.

⁴³ Vid. B. Cardona Rubert, *Informática y contrato de trabajo*, Tirant lo Blanch, Valencia, 1999, pág. 81.

⁴⁴ Vid. S. Rodríguez Escanciano, “Vigilancia y control en la relación de trabajo: la incidencia de las nuevas tecnologías”, en A. Farriols I Solá, *La protección de datos de carácter personal en los centros de trabajo*, Cinca, Madrid, 2006, pág. 93.

cluso bancarios)⁴⁵ con información indiscutiblemente protegida por el derecho a la intimidad (*v.gr.*, perfil personal en redes sociales). Esa es una información de la que el empresario no puede disponer (y con menos motivo otras personas como los técnicos informáticos que instalan y manejan dichos programas), porque se inserta indudablemente en la esfera personal del trabajador, y aunque el interés empresarial sea legítimo, el medio utilizado resulta palmariamente desproporcionado⁴⁶. El derecho a la intimidad debe prevalecer⁴⁷.

8. A MODO DE CONCLUSIÓN: EL CONVENIENTE RETORNO AL JUICIO DE PONDERACIÓN Y AL CRITERIO DEL USO INOCUO

El veloz avance de las nuevas tecnologías genera efectos muy diversos, y su implantación en el ámbito del trabajo no sólo permite aumentar la productividad y la eficiencia, sino que también genera riesgos, por el potencial perjuicio para la empresa que supone una utilización desviada. Es probable, no obstante, que esa potencialidad del daño se haya magnificado, y que la novedad haya provocado un relativo deslumbramiento, porque si bien es cierto que esos medios tecnológicos permiten al trabajador un uso personal inadecuado

⁴⁵ Vid. F. Camas Roda, *La influencia del correo electrónico y de internet en el ámbito de las relaciones laborales*, RTSS (CEF), nº 224, 2001, pp. 141 y ss.; R. Tascón López, *El poder de control empresarial en la era tecnológica: visión panorámica de una cuestión inacabada*, RTSS (CEF), nº 267, 2005, pp. 25 y ss.

⁴⁶ Así lo advierte la STSJ de Aragón de 4-12-2007 (recurso de suplicación 1004/2007). El trabajador, que prestaba servicios como técnico auxiliar deportivo de un ayuntamiento, utilizaba el ordenador que había sido puesto a su disposición para descargar películas pornográficas de internet, haciendo un uso abusivo de la conexión, lo que motivó quejas de sus compañeros por las dificultades que ello provocaba para navegar. Con el fin de acceder al material descargado, fue necesario que un técnico informático eludiese la contraseña personal que había establecido el trabajador, lo que permitió asimismo copiar todo el contenido del disco duro, operación en la que ningún momento participó el interesado. La sentencia considera que ese medio de control vulnera el derecho a la intimidad y anula todas las pruebas obtenidas por esa vía.

⁴⁷ Como señala la STSJ de Cataluña de 9-7-2002 (recurso 7878/2001), «la empresa está facultada para ejercer la vigilancia y control del cumplimiento de las obligaciones laborales del trabajador y también a velar por el buen uso del sistema informático que pone a su disposición para el cumplimiento de sus obligaciones laborales así como de la utilización y acceso a las terminales de cada uno de los trabajadores. La empleadora podía lícitamente examinar la procedencia de los E-mails recibidos en los que se le ofrecía la compra de determinada tecnología y en otro se insultaba gravemente a uno de sus socios. Es también lícito y correcto investigar las direcciones de correo electrónico que aparecían como remitentes de los mismos [...], pero no puede aceptarse por constituir una vulneración clara de derecho a la intimidad del actor que las personas contratadas por la empresa averiguaran la dirección personal, particular y privada del demandante [...] y que en ningún caso aprecia como emisor de los correos electrónico tantas veces mencionados para que utilizando claves de acceso que dedujeron en su investigación pero que no les proporcionó dicho trabajador y que eran desconocidas por la empleadora, acceder a su contenido desvelando y llegando a conocer el redactado de los correos electrónico allí archivados».

en el entorno laboral, también lo es que proporcionan al empleador formas de control más sofisticadas y con una capacidad lesiva mucho mayor. Es curioso, no obstante, que hasta el momento se haya considerado más reprobable la utilización de esas herramientas empresariales con fines personales que el medio de control empleado, sin que el principio de proporcionalidad haya tratado de aplicarse verdaderamente en los dos extremos: la conducta del trabajador, por un lado, y medio de vigilancia empleado, por otro⁴⁸.

La jurisprudencia constitucional, y ordinaria, sobre el control y vigilancia del uso de estas herramientas en el entorno laboral trata de resolver casos concretos, pero ofrece para ello reflexiones de cierta generalidad que seguramente pueden dar lugar a interpretaciones desmesuradas, tanto por los tribunales de instancia y suplicación, como por la doctrina científica. La jurisprudencia constitucional se halla todavía en construcción, y requiere un análisis muy apegado al caso concreto. De lo contrario, se corre el riesgo de apostar por criterios netamente formalistas y escasamente garantistas, porque perfilar los contornos de los derechos fundamentales en función exclusivamente de la existencia o no de una política empresarial previa aporta seguridad jurídica –valor constitucional de indudable relevancia–, pero deja en manos del empleador la oportunidad del control y el modo de proceder a él, privando de efectividad a los derechos a la intimidad y al secreto de las comunicaciones, que quedan relegados a un segundo plano con independencia de que el empleador demuestre un interés legítimo. Aunque hasta ahora el control del uso de los medios empresariales parecía contar con más límites, desde esta nueva perspectiva la prohibición previa se erigiría como justificación de cualquier clase de control sobre la utilización del ordenador en la empresa, concediendo facultades adicionales al empleador.

Las consecuencias que derivarían de esas interpretaciones, más bien extremas, de la jurisprudencia expuesta generan riesgos potenciales muy notables, pues la completa monitorización del uso del ordenador –que sólo parece requerir de una previa advertencia, incluso genérica–, permitiría al empleador –al menos potencialmente– acceder a información sensible, como la afiliación sindical o política, el número de tarjeta de crédito del trabajador o sus claves bancarias, por ejemplo. Es claro que el trabajador incumple sus obligaciones si utiliza el ordenador con fines personales en contra de las órdenes del empresario, pero existen medios de control menos invasivos que permiten constatar que se ha producido un incumplimiento sin recabar datos personales, privados y/o íntimos.

Así sucede, por ejemplo, en relación con el correo electrónico. En este sentido, admitir el acceso al contenido de los mensajes por el mero hecho de

⁴⁸ Vid. J.L. Monereo Pérez y M.B. López Insua, *El control empresarial del correo electrónico tras la STC 170/2013*, Revista Doctrinal Aranzadi Social nº 11/2014 (BIB 2014\122).

que se encuentren en el ordenador puesto a disposición del trabajador resulta, sin duda, un exceso, ya que no se valora la proporcionalidad de la medida, ni la afectación a terceros (los remitentes o destinatarios del correo). La casuística resulta muy variada, pero no establecer las pertinentes cautelas en el control dará lugar a resultados desproporcionados, porque con los sistemas actuales de almacenamiento en la “nube” es viable que el empleador pueda comprobar el contenido de correos electrónicos enviados por el trabajador fuera del lugar y tiempo de trabajo, normalmente en su propia casa y en un ordenador propio, pero accesibles desde el ordenador “profesional”. En cualquier caso, aceptar que el empleador puede acceder al contenido de los correos electrónicos sin necesidad de demostrar una sospecha previa de incumplimiento configura un nuevo escenario para los derechos a la intimidad (control del ordenador en sentido estricto) y al secreto de las comunicaciones (control del correo electrónico o de otros programas de mensajería).

La diferencia entre un canal abierto y un canal cerrado es, en principio, razonable, pero los criterios para determinar qué formato adopta el concreto canal requieren, sin lugar a dudas, de mayor precisión técnica, porque el hecho de que la propiedad del ordenador pertenezca a la empresa y que se utilice como herramienta de trabajo no debería configurar el canal como abierto, ni aun cuando la empresa prohíba expresamente un uso personal. Esa posición no respeta, en absoluto, el principio de proporcionalidad, y se genera otro riesgo evidente, cual es que la sanción por el incumplimiento venga determinada por el contenido de la comunicación o la concreta utilización del ordenador, y no en sí misma por el uso con fines personales. Si la conducta sancionable es la utilización de medios empresariales con propósito personal, el control empresarial debería limitarse a constatar tal circunstancia, sin utilizar medios más invasivos, que no resultan necesarios ni proporcionales, por indiscriminados. En sentido contrario, cuando la empresa no prohíbe la utilización del ordenador con fines personales el canal no debería considerarse cerrado, y por tanto protegido por el secreto de las comunicaciones, porque la herramienta sigue siendo propiedad de la empresa, el trabajador tiene obligación de utilizar tal instrumento conforme a la buena fe y el empleador no pierde sus facultades de control y vigilancia.

La jurisprudencia constitucional sobre el control del ordenador es, todavía, embrionaria, pero debe aquilatarse, pues de lo contrario podría cuestionarse si el derecho fundamental a la intimidad sigue teniendo virtualidad en el contexto del trabajo, al menos en lo que se refiere específicamente a la utilización del ordenador, pues difícilmente se admitirá un control de la misma índole respecto de otros medios. Por ejemplo, en caso de utilización de un coche de empresa parece razonable que se instale un GPS para conocer la ubicación del vehículo, pero no resulta proporcional, ni siquiera necesario, que se instale una cámara

que grabe la imagen –y eventualmente el sonido–, porque la empresa puede tener un interés legítimo en comprobar la localización del vehículo, pero resultará difícil demostrar que ese interés exige una medida de control más invasiva. Sin embargo, en relación con el ordenador se han olvidado todas las cautelas que derivarían del principio de proporcionalidad, y seguramente se admita que en aquellos casos donde los correos electrónicos –tanto salientes como entrantes, no se olvide– se almacenan en un servidor propio del empleador, este puede consultar su contenido, medida, sin lugar a dudas, desproporcionada.

Habría sido recomendable, sin duda, que el Tribunal Constitucional hubiera introducido mayores matices en su argumentación. Por ejemplo, la STC 241/2012 omite que la conversación que dio lugar a la sanción no se mostraba en la pantalla del ordenador automáticamente tras su encendido, sino que se encontraba almacenada en una carpeta específica dentro del disco duro del ordenador. En efecto, muchos programas de mensajería guardan un historial de conversaciones antiguas, pero la consulta requiere de cierta indagación fuera del alcance de un usuario novato o poco avanzado. En tal caso, el canal no parece tan abierto como la sentencia afirma, porque son necesarias pesquisas específicas para localizar el archivo, y una voluntad clara de apertura y lectura. En esos términos, la indagación que permite conocer el contenido concreto de las conversaciones debería ser valorada desde la perspectiva del derecho a la intimidad. Conviene recordar que la empresa había prohibido la instalación de programas, lo que supone, en definitiva, que la sanción debía atender, precisamente, a esa circunstancia, con independencia del contenido de la conversación. Sin embargo, no es claro que la empresa hubiera procedido a sancionar a las trabajadoras de no haber conocido los términos concretos de la conversación, o si en lugar de críticas a la empresa se hubieran descubierto comentarios elogiosos.

La sanción, en realidad, se produce a consecuencia de las ofensas verbales y no por la instalación del programa, o por la merma de productividad debida al tiempo dedicado a la conversación. El Tribunal Constitucional parece aceptar que, en caso de duda sobre el carácter personal o profesional de la actuación del trabajador, el empleador efectúe el control, de modo que si se descubre un uso personal la sanción se valida. Es, sin duda, una forma de actuación peligrosa, pues existen opciones mucho más respetuosas con los derechos fundamentales. La más obvia consiste en preguntar al trabajador si el contenido de las conversaciones, documentos o archivos es personal o profesional. En caso de que el trabajador confirme que el uso es profesional, el empleador puede legítimamente comprobar el contenido, mientras que si el trabajador aduce que es personal el empresario podrá imponer la pertinente sanción, precisamente, por ese incumplimiento, pero no estará legitimado para verificar el contenido concreto.

En efecto, no es razonable conceder al empleador un poder de tal intensidad que le permita monitorizar toda la actividad del trabajador, pues el riesgo de vulneración del derecho a la intimidad resulta inaceptable en tanto que existan opciones menos lesivas. Todo ello a salvo, claro está, de que el empresario trate de comprobar la veracidad de una sospecha no infundada, ni mero pretexto, sino con una base sólida. Así sucede en la STC 170/2013, donde lo relevante habría de ser, precisamente, la sospecha de filtración de información confidencial a la competencia. Una vez que la empresa cuenta con tal sospecha, debe desde luego estar legitimada para poner en marcha instrumentos de control adecuados, que podrían resultar de diversa índole, siendo irrelevante la existencia de una prohibición previa.

El hecho de que la empresa haya prohibido el uso personal de medios empresariales no puede ser el argumento principal que justifique el control del contenido de los mensajes de correo electrónico, máxime en un supuesto de hecho como el conocido por esa sentencia, en el que ni siquiera existía tal prohibición, sino la tipificación de una infracción leve en el convenio colectivo. Establecer una equivalencia entre una infracción leve y una prohibición general, y basar en ella la facultad empresarial de acceder al contenido de las conversaciones del correo electrónico, parece un exceso interpretativo. En cualquier caso, la existencia de prohibición empresarial no debería contar con tanta relevancia. No conviene olvidar que en caso de haber optado por otros medios de control usuales en estos supuestos de constatación de competencia desleal –v.gr., contratación de un detective privado–, no parece que el control pueda condicionarse a que la empresa hubiera prohibido explícitamente filtrar información confidencial a la competencia, ni a la advertencia sobre ese posible medio de control.

La jurisprudencia constitucional, en este momento, admite interpretaciones que conducen a un resultado desproporcionado, porque las conversaciones o comunicaciones a través de internet utilizan la infraestructura telefónica, y en ese ámbito el control y la vigilancia del contenido de las comunicaciones requieren de ordinario de autorización judicial. Sin embargo, el hecho de que el medio utilizado sea propiedad de la empresa permite al empleador determinar unilateralmente el modo de utilización y servirse prácticamente de cualquier medio de control. El resultado no se acomoda bien a la especial protección que deberían merecer los derechos fundamentales⁴⁹.

En último término, tampoco cabe olvidar que la STC 170/2013 concluye afirmando que «no consta en las actuaciones que el contenido de estos mensajes refleje aspectos específicos de la vida personal y familiar del trabajador, sino únicamente información relativa a la actividad empresarial, cuya remisión

⁴⁹ Vid. M.B. Cardona Rubert, *Reinterpretación de los derechos de intimidad y secreto de las comunicaciones en el modelo constitucional de relaciones laborales: un paso atrás*, RDS, nº 60, 2012, pp. 169 y ss.; I. Marín Alonso, *La mensajería electrónica en la empresa: un paso atrás en la protección constitucional del derecho al secreto de las comunicaciones*, RL, nº 3, 2013, pág. 97.

a terceros, conforme a la Sentencia recurrida, implicaba una transgresión de la buena fe contractual». Ello suscita otra clase de preguntas, pues no es claro que la respuesta del Tribunal hubiera sido la misma en caso de que el incumplimiento no hubiera sido probado, y si además se hubieran conocido datos íntimos.

En esta línea, resulta recomendable, más bien imprescindible, distinguir entre la necesidad de verificar el uso personal de la herramienta y el acceso al contenido, pues en función de cuál sea el objetivo empresarial, la justificación del control y el medio elegido han de ser diferentes. En suma, cuando el empleador quiere constatar si el trabajador realiza un uso personal del ordenador será suficiente con una comprobación superficial (destinatario y remitente de correos, nombre de los archivos, etc.), y ese control se justifica en virtud del poder de dirección empresarial.

En cambio, el acceso al contenido concreto debería supeditarse a la concurrencia de una de estas dos circunstancias. En primer lugar, el consentimiento del trabajador, debiendo consultarse al mismo sobre el carácter personal o profesional de los archivos, documentos o conversaciones, especialmente en caso de controles sorpresa o no preavisados con la pertinente antelación (a salvo, lógicamente, de que el trabajador ya hubiera abandonado la empresa, lo que permite presumir que la información contenida en el ordenador no tiene carácter personal, ya que debería haber sido borrada). La empresa debería abstenerse de comprobar el contenido calificado como personal por parte del trabajador, sin perjuicio de la sanción que merezca ese incumplimiento específico. En segundo lugar, la previa sospecha de incumplimiento basada en indicios sólidos. En presencia de tal sospecha el empleador puede servirse de medios de control aptos para constatar la infracción laboral.

Sea cual fuere la opción, la política empresarial sobre el uso de medios empresariales con fines personales debe perder protagonismo a favor del test de constitucionalidad, pues exista o no tal política la legitimidad de la actuación empresarial debe enjuiciarse desde la perspectiva de su idoneidad, necesidad y proporcionalidad. Y, especialmente, la necesidad y la proporcionalidad cuentan con escasa presencia en la jurisprudencia constitucional sobre la utilización del ordenador, que además tampoco valora —excepto en el ámbito sindical— el perjuicio realmente causado al empleador, pues no se utiliza el criterio del uso inocuo. En suma, esa jurisprudencia constitucional debe aquilatarse progresivamente, para permitir que el derecho a la intimidad —más que el secreto de las comunicaciones— conserve cierto espacio en el marco de la relación laboral. Y no debe olvidarse que el mantenimiento de las garantías derivadas de los derechos fundamentales, y con ello los límites al control empresarial, no prejuzgan el eventual incumplimiento del trabajador, ni la licitud de una sanción, sino que el propósito, en última instancia, es que la sanción responda verdaderamente a la infracción cometida, y no dependa del contenido de conversaciones o documentos ilegítimamente conocidos.