**MADRID**
Castellana, 216
28046 Madrid
Tel.: (34) 91 582 91 00

**BARCELONA**
Diagonal, 640 bis
08017 Barcelona
Tel.: (34) 93 415 74 00

**BILBAO**
Alameda Recalde, 36
48009 Bilbao
Tel.: (34) 94 415 70 15

**MÁLAGA**
Marqués de Larios, 3
29015 Málaga
Tel.: (34) 952 12 00 51

**VALENCIA**
Gran Vía Marqués
del Turia, 49
46005 Valencia
Tel.: (34) 96 351 38 35

**VIGO**
Colón, 36
36201 Vigo
Tel.: (34) 986 44 33 80

**BRUSELAS**
Avenue Louise, 267
1050 Bruselas
Tel.: (322) 231 12 20

**LONDRES**
Five Kings House
1 Queen Street Place
EC 4R 1QS Londres
Tel.: +44 (0) 20 7329 5407

**LISBOA**
Avenida da Liberdade, 131
1250-140 Lisboa
Tel.: (351) 213 408 600

# VUELTA DE TUERCA AL CONTROL POR LA EMPRESA DE LAS HERRAMIENTAS INFORMÁTICAS (O LA IMPORTANCIA DE TENER UN BUEN PROTOCOLO)

## [STS de 6 de octubre de 2011 (rec. 4053/2010)]

**Área de Laboral**

## 1. LOS HECHOS

La empresa comunicó por escrito a todos los trabajadores –quedando constancia de la recepción mediante la firma- que quedaba terminantemente prohibido el uso de medios de la empresa (ordenadores, teléfonos móviles, internet, etc.) para fines propios tanto dentro como fuera del horario de trabajo. A los pocos días (menos de 7) se hizo una comprobación sobre el uso de estos medios de trabajo. En concreto, se procedió a la motorización de los ordenadores de dos empleadas de las que sospechaba hacían un uso indebido o irregular. La monitorización se llevó a cabo mediante la instalación de un software "pasivo", es decir, "poco agresivo" al permitir únicamente visualizar lo visto en pantalla por el trabajador, sin poder acceder a los archivos del ordenador protegidos por contraseñas personales. Dos semanas más tarde, se procedió a visualizar el proceso de monitorización del ordenador de una de las trabajadoras en su presencia y también en la de otros testigos (en concreto, los artífices de la monitorización, los representantes de la empresa y dos trabajadores más), quienes firmaron un acta de comparecencia. El acta no fue firmada por la trabajadora, que fue inmediatamente despedida.

## 2. LO QUE YA SABÍAMOS

- La empresa debe respetar los derechos fundamentales de los trabajadores, en concreto, en lo que ahora interesa, la dignidad (personal y profesional) y la intimidad (personal): SSTC 88/1985, 6/1988, 129/1989, 126/1990, 99/1994, 106/1996, 186/1996, 90/1997, 98/2000; 186/2000, 196/2004, 125/2007.

- La empresa tiene la facultad de adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento del trabajador de sus obligaciones laborales, respetando, en todo caso, la dignidad del trabajador [arts. 4.2 c) y 20.3 ET]: STC 186/2000. En otros términos, el empresario no queda apoderado para llevar a cabo, so pretexto de las facultades de vigilancia y control, intromisiones ilegítimas en la intimidad de sus trabajadores. De ahí la importancia de llevar a cabo una ponderación adecuada de los derechos e intereses en juego mediante la aplicación de las reglas de la proporcionalidad, de la idoneidad y de la necesidad (P.I.N.).

- El ordenador no es un "efecto personal del trabajador", sino un medio de trabajo que es propiedad de la empresa. De ahí que el control de su uso no quede supeditado a las garantías (máximas) del art. 18 ET, sino a las más generales del art. 20.3 ET: STS de 26 de septiembre de 2007.

- Un "hábito social generalizado de tolerancia" con ciertos "usos personales moderados" de los medios facilitados por la empresa crea una expectativa general de confidencialidad en su uso.

Sin embargo, esta expectativa no puede convertirse en un impedimento permanente del control empresarial: STS de 26 de septiembre de 2007.

- La empresa puede (y debe, según la STS de 26 de septiembre de 2007):
  - Establecer el modo en que tales medios han de ser utilizados, con aplicación de prohibiciones absolutas o parciales.
  - Informar a los trabajadores de que va existir control, de los medios que se van a aplicar en orden a comprobar la corrección de los usos y, cuando sea preciso, de las medidas que han de adoptarse, en su caso, para garantizar la efectiva utilización laboral del medio.
  - Aplicar otras medidas de carácter preventivo, como la exclusión de determinadas conexiones.
- Cuando no se cumplen las pautas señaladas, la empresa asume el riesgo de que la medida de control se estime inadecuada o desproporcionada: STS de 8 de marzo de 2011.
- El trabajador no puede imponer el respeto a su intimidad cuando actúa en contra de las instrucciones dadas por la empresa: STS de 26 de septiembre de 2007.

## 3. LOS CRITERIOS NOVEDOSOS

- Se refuerza el poder de dirección de la empresa: el ordenador es "propiedad de la empresa" y el control de su uso es absolutamente lícito en tanto medio o instrumento para trabajar. La empresa tiene "*ex lege* facultades de control". Esta consideración ha de extenderse a cualquier otro medio o instrumento de trabajo como el teléfono.
- El conflicto puede surgir (y surgirá, sin duda) si existe una situación de tolerancia que permite entender que hay espacio para un uso personal moderado de acuerdo con los usos sociales. Sin embargo, no habrá conflicto si la empresa establece una prohibición o limitación en el uso que resulte lícita.
- La empresa no puede adoptar una actitud pasiva: el margen de tolerancia (si es que lo hay) y el uso debido puede (y debe) establecerse mediante un protocolo.
- Cuando hay un margen de tolerancia, por pequeño que sea, surge una "expectativa razonable de confidencialidad" y, paralelamente, una restricción de la facultad de control empresarial, limitada por los criterios del Tribunal Constitucional: el control debe ser el imprescindible para comprobar que el medio informático había sido utilizado para usos distintos de los de su cometido laboral.
- Es lícito prohibir el uso de las herramientas informáticas para fines particulares (no laborales) de un modo absoluto, es decir, sin espacio alguno para que se desarrollen estos últimos: "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 (o confidencialidad) y porque, si el uso personal es ilícito, no puede exigirse al empresario que lo soporte y que además se abstenga de controlarlo". En otras palabras, "el trabajador afectado sabe que su acción de utilizar para fines personales el ordenador no es correcta y sabe también que está utilizando un medio que, al estar

lícitamente sometido a la vigilancia de otro, ya no constituye un ámbito protegido para su intimidad".

- La prohibición absoluta no siempre es válida ni admisible:
  - No ha de ser caprichosa o arbitraria/ injustificada.
  - Se admite la prohibición total cuando hay sospechas fundadas de que se están desobedeciendo las órdenes impartidas por la empresa.
  - Si el convenio colectivo reconoce el derecho a un uso personal, la empresa debe respetar el criterio convencional. En este caso, la empresa debe respetar la intimidad de los trabajadores y puede aplicar, en su caso, medidas de control que han de ser compatibles con el respeto de los derechos fundamentales.
- Cuando la prohibición (absoluta o relativa) es válida, no puede existir un conflicto de derechos porque no hay un espacio para la protección jurídica de la intimidad ni de la confidencialidad. En este caso –criterio novedoso- es irrelevante "la información que la empresa haya podido proporcionar sobre el control y su alcance", pues el control, aquí, "es inherente a la propia prestación de trabajo y a los medios que para ello se utilicen". Dicho en otros términos, cuando la prohibición es válida "lleva implícita la advertencia sobre la posible instalación de sistemas de control del uso del ordenador".
- En todo caso, la garantía de intimidad no es absoluta sino que su posible afección requiere ponderar circunstancias tales como la naturaleza más o menos pública del medio, el hecho de que esté sujeto o no a la inspección de otra persona, etc.: "quien entra en el ordenador sometido al control de otro, que ha prohibido los usos personales y que tiene *ex lege* facultades de control, sabe que no tiene una garantía de confidencialidad.
- *Da mihi factum … et ius … et iurisprudentia … et argumentum*: el Tribunal está sometido al recurso y, por tanto, ceñido a las denuncias contenidas en él, sin que pueda, de oficio, invocar argumentos o razones "nuevas" que no se contienen en el recurso: "la censura tiene que ceñirse a la denuncia por el exceso de la utilización de un programa espía y a la alegación de que se han incumplido las garantías del art. 18 ET", sin que pueda examinarse si la "falta de advertencia expresa a la actora de la instalación del "software" de monitorización" supuso o no una extralimitación o una actuación inadecuada o poco proporcionada de la empresa.
- La sentencia cuenta con un voto particular de 6 Magistrados en el que se discrepa de la solución dada, estimando que la ausencia de información a los trabajadores acerca del control y de los medios para comprobar la corrección del uso del ordenador supone que se ha vulnerado una expectativa razonable de intimidad, ya que –a juicio de los Magistrados que se separan del voto mayoritario- no es suficiente la prohibición del uso del ordenador para actividades privadas, sino que dicha prohibición ha de ir acompañada de una información sobre la existencia de un control y de los medios que van a aplicarse. Además, se estima que el procedimiento de control (el sistema "no agresivo") supone una vulneración del derecho a la intimidad en tanto permitía visualizar la pantalla.