# Internet, Derecho y Política. Una década de transformaciones

Actas del X Congreso Internacional Internet, Derecho y Política. Universitat Oberta de Catalunya, Barcelona, 3-4 de julio de 2014

# *Internet, Law & Politics. A Decade of Transformations*

*Proceedings of the 10th International Conference on Internet, Law & Politics. Universitat Oberta de Catalunya, Barcelona, 3-4 July, 2014*

2014

UOC
Universitat Oberta de Catalunya
www.uoc.edu

HUYGENS EDITORIAL

# FACULTAD DE CONTROL EMPRESARIAL Y EL DERECHO A LA LIBERTAD INFORMÁTICA DE LOS TRABAJADORES: UN DERECHO FUNDAMENTAL (INEXPLICABLEMENTE) OLVIDADO

Ignasi Beltran de Heredia Ruiz
*Profesor Agregado y TU acreditado de Derecho del Trabajo y de la Seguridad Social*
*Universitat Oberta de Catalunya (UOC)*

RESUMEN: El estudio analiza el conflicto que suscita la capacidad de control del empresario sobre la actividad de los trabajadores y, particularmente, sobre el uso de los medios electrónicos propiedad de la empresa y su derecho a la libertad informática. Ante la ausencia de normas laborales que explícitamente den respuesta a este conflicto, el ensayo que se propone pretende exponer los criterios hermenéuticos empleados por los órganos jurisdiccionales laborales para resolver estas situaciones. En este sentido, la jurisprudencia ha establecido una amplia capacidad de control por parte del empresario. De modo que únicamente la existencia de una expectativa fundada y razonable de confidencialidad por parte del trabajador puede deslegitimar el posible examen de los medios informáticos de titularidad empresarial puestos a su alcance.

El ensayo defiende que, en ocasiones, la recopilación de datos efectuada por el empresario para poder evidenciar conductas inadecuadas de los trabajadores se ha desarrollado vulnerando el derecho a la libertad informática. Convirtiéndose en una dimensión constitucional del conflicto que inexplicablemente es omitida por los Tribunales y, en el mejor de los casos, queda en un plano secundario.

PALABRAS CLAVE: Poder de dirección y control empresarial, derecho a la libertad informática, privacidad, intimidad, medios informáticos propiedad empresa, internet.

## 1. CONTRATO DE TRABAJO, CONTROL EMPRESARIAL Y LIBERTAD INFORMÁTICA: UN ESPACIO CON UN ALTO POTENCIAL INTRUSIVO (PLANTEAMIENTO)

En una relación laboral son múltiples les datos que el trabajador debe suministrar al empresario. Más allá de los supuestos de transmisión expresa y consentida de datos de carácter personal o los que el empresario pueda exigir para la perfección del contrato y el desarrollo ordinario de la relación laboral, el uso intensivo de dispositivos electrónicos/digitales describe en este ámbito un escenario particularmente amenazador. Y esto es así, especialmente porque, como es bien sabido, permite (sin excesiva dificultad) el rastreo de un conjunto heterogéneo de datos que, pese a tener un carácter intrascendente (o poco relevante) si se analizan aisladamente, en cambio, si se almacenan, combinan y se

someten globalmente a un tratamiento mecanizado, pueden permitir una reconstrucción profunda y detallada del perfil individual del trabajador.

Este escenario resulta particularmente intrusivo, especialmente, porque el empleado, a través del uso de estos dispositivos en el quehacer ordinario de su labor profesional, inconscientemente, puede estar contribuyendo a configurar un perfil detallado de su personalidad y/o su conducta (o una particular dimensión de ambas)[1].

Siguiendo el criterio de la STSJ Cantabria 18 de enero 2007[2], «existen ciertas diferencias entre las nuevas tecnologías y los (…) medios audiovisuales y de comunicación; así, a diferencia de la video-vigilancia, en la ciber-vigilancia es posible distinguir dos momentos distintos, un primer momento de recogida de datos y un segundo momento de tratamiento de los datos obtenidos; es decir, aunque la informática permite un control directo del comportamiento laboral del trabajador, el verdadero conocimiento sobre el comportamiento del trabajador no se obtiene sino mediante la recogida sistemática de datos, su almacenamiento y su posterior tratamiento; de ahí que los limites que se derivan del respeto al derecho de la intimidad han de operar en dos momentos distintos: en el momento de la recogida de los datos y de la información, que ha de ser adecuados al fin perseguido, que no podrá ser otro que la verificación del cumplimiento de sus obligaciones laborales por el trabajador, y, además, en el momento del posterior registro físico para el tratamiento de los datos capturados».

---

1 El TC ha afirmado que «el que un sistema normativo que, autorizando la recogida de datos incluso con fines legítimos, y de contenido aparentemente neutro, no incluyese garantías adecuadas frente a su uso potencialmente invasor de la vida privada del ciudadano, a través de su tratamiento técnico, vulneraría el derecho a la intimidad de la misma manera en que lo harían las intromisiones directas en el contenido nuclear de ésta» (STC 143/1994).
En paralelo, la STC 292/2000 declara que «el objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal. Por consiguiente, también alcanza a aquellos datos personales públicos que, por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos. También por ello, el que los datos sean de carácter personal no significa que sólo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo».

2 AS 2007\1030.

En definitiva, su «privacidad»[3] (o una dimensión de la misma) puede llegar a ser (totalmente) transparente para el empresario.

La llamada 'libertad informática' (o «autodeterminación informativa»), precisamente, confiere el derecho a controlar el uso de los mismos datos insertos en un programa informático –habeas data– y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención (STC 254/1993).

Llegados a este estadio, la distinción entre el derecho a la intimidad y el derecho a la libertad informática es relevante, por cuanto que mientras que el primero se protege desde la propia abstención de los sujetos que eventualmente pueden lesionar el derecho; la tutela informática requiere, además, la adecuación de su comportamiento con una acción concreta: suprimir datos, modificarlos, restringir su uso, emplearlos para fines legítimos, etc. (Arias Domínguez y Rubio Sánchez, 2006, versión digital)[4].

Sin embargo, esta es una circunstancia que ha sido analizada profusamente por la doctrina laboral y, sin duda, su exposición excede, con mucho, el espacio reservado para un ensayo de estas características. Apartándonos de este propósito, el objeto de este breve trabajo consiste precisamente en analizar (brevemente) el tratamiento que los Tribunales laborales están dispensando a esta dimensión de los derechos fundamentales. Especialmente, porque, adelantando las conclusiones, no parece que esté recibiendo el tratamiento aplicativo e interpretativo adecuado por parte de los órganos jurisdiccionales laborales. Veamos, a continuación, estos extremos.

---

3 Según la Exposición de Motivos de la LO 5/1992, 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, afirma que «la privacidad constituye un conjunto, más amplio, más global, de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado».

4 Como afirma la STSJ País Vasco 17 de abril 2012 (AS 1676): «el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre datos personales que faculta a la persona para decidir cuales de esos datos proporciona a un tercero o cuales puede este tercero recabar y también permiten al individuo saber quien posee esos datos y para que se poseen pudiéndose oponerse a lo mismo. Por ello esos poderes de disposición y control que constituyen parte del contenido del Derecho Fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida obtención de acceso a los datos personales y su posterior almacenamiento y tratamiento así como su uso o posibles usos por terceros. Los complementos indispensables son, por un lado, la facultad de saber en todo momento quien dispone de esos datos y por otro a que uso los está sometiendo, para poder oponerse a esa posesión y usos».

## 2. CONTROL EMPRESARIAL, INTIMIDAD Y LIBERTAD INFORMÁTICA EN EL ÁMBITO LABORAL: OMISIONES RELEVANTES

La jurisdicción laboral ha prestado especial atención al uso extralaboral de los medios TIC propiedad de la empresa por parte del trabajador durante el tiempo de trabajo. Especialmente, desde el prisma de la capacidad de control que ostenta el empresario, de la transgresión o no de la buena fe contractual por parte del trabajador y de su derecho a la intimidad y al secreto de las comunicaciones. Como es bien sabido, la ausencia de disposiciones normativas específicas al respecto, ha llevado a la doctrina constitucional[5] y a la jurisprudencia a establecer algunos criterios hermenéuticos (la ausencia de una regulación interna o convencional regulando el uso extralaboral de estos dispositivos comunicada fehacientemente, crea una expectativa de confidencialidad en esos usos), hoy en día, consolidados por los propios Tribunales y la comunidad científica[6].

En este sentido, sorprende que el Legislador Laboral en alguno de los «arrebatos» reformadores que ha tenido en los últimos años no haya tomado la decisión de «normativizar» estos criterios a fin de dar una mayor seguridad a los operadores jurídicos (y aliviar a los órganos jurisdiccionales de una labor que en absoluto les corresponde). De hecho, como botón de muestra, el principal instrumento normativo para dar respuesta a estas cuestiones, el art. 18 ET, sigue refiriéndose al control de las «taquillas» del trabajador.

En paralelo, como recoge la STSJ Cantabria 18 de enero 2007[7], «después de establecer en el art. 20.3 que «El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana y teniendo en cuenta la capacidad real de los trabajadores disminuidos, en su caso», no hace ninguna referencia a esta novedosa forma de vigilancia, lo cual es tanto como decir que el ET no prohíbe el control empresarial mediante al utilización de las nuevas tecnologías de la información; en este sentido la

5 STC 170/2013. Pronunciamiento, en virtud del cual, siguiendo la síntesis de Monereo Pérez y López Insua (2014, versión digital) sostiene – adoptando un criterio muy restrictivo del derecho a la intimidad de los trabajadores - que «la mera «sospecha» acerca de si un trabajador transmite o no indebidamente información confidencial de su empresa a otra entidad mercantil, constituirá causa suficiente para que el empresario esté legitimado para comprobar tanto el contenido de los mensajes «SMS» del móvil profesional del trabajador, como del disco duro del portátil proporcionado por su empresa».

6 SSTS 26 de septiembre 2007 (RJ 7514); y 8 de marzo 2011 (RJ 932); 6 octubre 2011 (RJ 7699); y en la doctrina judicial, entre otras, SSTSJ Castilla-La Mancha 14 de abril 2011 (núm. 450/2011); y Galicia 25 de enero 2011 (núm. 503/2011). Y en la doctrina, vid. al respecto, entre otros, Beltran de Heredia Ruiz (2010), p. 617 y ss.; y Calvo Gallego (2012), versión digital.

7 AS 2007/1030.

Agencia de Protección de Datos tiene establecido que "... en principio y de modo general, siempre que el correo electrónico, archivo informático etc. o cualquier otra comunicación formen parte de la actividad laboral del trabajador y se realicen en tiempo de trabajo puede ser analizadas y supervisadas por el empresario dado que entrarían dentro de la potestad de control que puede ejercer legalmente"».

El foco de atención en estos casos acostumbra a girar en torno a la intensidad con la que debe protegerse la intimidad de los trabajadores o, dicho de otro modo, en qué circunstancias prevalece la capacidad de control por parte del empresario. Sin embargo, éste no es el único derecho fundamental que puede verse vulnerado, pues, si se prevé un control de estos instrumentos informáticos es probable que también se esté procediendo a una recogida sistemática y exhaustiva de datos memorizados sobre aspectos del comportamiento del trabajador. Y, por consiguiente, el derecho a la libertad informática puede verse afectado.

De todos modos, como es bien sabido, no existe una norma que atienda específicamente a las particularidades que presenta la relación laboral, debiéndonos remitir a la Ley Orgánica 15/1999, de Protección de Datos (en adelante, LOPD). Los elementos conceptuales sobre los que se sustenta esta normativa son el principio de congruencia y racionalidad[8], por un lado; y el principio de consentimiento o autodeterminación[9], por otro.

8 En primer lugar, que no se proceda a una recolección de datos excesivos, en relación con el ámbito y las finalidades para las que se hayan obtenido (principio de pertinencia); exigiéndose la veracidad y actualización de los mismos (principio de veracidad) – vid. al respecto STC 94/1998. Además, el art. 4.2 LOPD, dispone que «los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos» (principio de finalidad); prohibiéndose en el art. 4.7 LOPD «la recogida de datos por medios fraudulentos, desleales o ilícitos» (principio de legalidad). Por otra parte, debe garantizarse la accesibilidad a los mismos, así como su posible cancelación, sin que puedan ser conservados durante un tiempo superior al necesario para los fines que justificaron su recogida (principios de accesibilidad, cancelación y descontextualización). Sin olvidar los denominados «datos sensibles», que según su tipología exigen un consentimiento expreso y por escrito (art. 7.2 LOPD), o bien, un consentimiento expreso (7.3 LOPD) –sin olvidar las excepciones previstas en el art. 7.6 LOPD. En todo caso, debe tenerse en cuenta que el empresario en todo caso debe abstenerse de indagar, almacenar, procesar o retener informaciones de tal naturaleza.

9 Esto es, el consentimiento consciente e informado (principio de autodeterminación), salvo que la Ley disponga otra cosa (art. 6.1 LOPD) –como se prevé para el ámbito laboral en el art. 6.2 LOPD– datos estrictamente necesarios para el desarrollo de la relación laboral; y los arts. 22 LPRL y 12.4 TRLISOS –para datos relativos a la salud. Para el resto de datos que no tengan esta naturaleza o los particularmente protegidos (ideología, salud, origen racial, etc.) deberá exigirse el consentimiento del trabajador. Y para el caso de que el responsable del fichero pretenda ceder determinados datos legalmente obtenidos a un tercero, también deberá recabar el consenti-

La incardinación del primero de estos principios en el ámbito laboral implica que el empresario, en el ejercicio de sus facultades, está habilitado legalmente para recabar información de diversa naturaleza de sus trabajadores, siempre que la emplee para las finalidades específicamente descritas en la normativa laboral, sin que en ningún caso, pueda destinarla a otros usos, pues, de otro modo, estaría incurriendo en una práctica ilícita[10].

Y, en relación al segundo de los principios, es importante reparar que a pesar de que el empresario, según los casos, pueda estar eximido de requerir el consentimiento del trabajador, esto no obsta a que éste tenga derecho a saber sobre su existencia y el tratamiento que se está llevando a cabo. De modo que, siempre que los datos hayan sido obtenidos de un modo lícito, una vez creado el fichero, el sistema de garantías debe prevalecer. Esto es, el responsable del mismo o su representante, dentro de los tres meses siguientes al momento del registro de los datos (salvo que ya hubiera sido informado con anterioridad), deberá informar al trabajador previamente de modo expreso, preciso e inequívoco sobre el contenido del tratamiento y la procedencia de los datos y de los siguientes extremos (art. 5.4 LOPD):

- de la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información;
- de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición;
- y de la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

De modo que si el trabajador no ha sido informado sobre las circunstancias particulares que justifican la existencia de un fichero, así como del alcance y ámbito de aplicación del mismo debe calificarse como ilegal.

Sin olvidar, finalmente, que los datos registrados no pueden permanecer en posesión del responsable del fichero de un modo indefinido, sino que una vez cese la finalidad para la cual los datos fueron recogidos y registrados deben suprimirse (art. 4.5 LOPD).

Y esta matriz (brevemente expuesta) describe, precisamente, la clave de bóveda del conflicto entre el derecho a la libertad informática y el poder de control por parte del empresario, pues, la digitalización de gran parte de los dispositivos a disposición de los trabajadores y de sus comunicaciones y, en particular, la extraordinaria facilidad para su eventual almacenamiento coloca al empresario ante la necesidad de dar cumplimiento

---

miento del trabajador afectado (art. 11.1 LOPD), salvo que concurra algunas de las excepciones previstas en el art. 11.2 LOPD.

10 La jurisprudencia constitucional ha tenido ocasión de pronunciarse en dos supuestos al respecto: SSTC 11/1998; y 202/1999.

de los deberes descritos en la LOPD. En caso contrario, debería considerarse que se ha vulnerado los derechos fundamentales de los trabajadores.

Por ejemplo, a pesar del contenido del art. 20.3 ET, debe entenderse que el tratamiento de datos emitidos por el sistema de GPS instalados en los vehículos debe cumplir con lo dispuesto en la LOPD. Esto es, debe informarse al trabajador según lo previsto en el art. 5.1 LOPD[11].

Lo «curioso» (y/o –a nuestro entender– sorprendente) del caso es que, si bien es (relativamente) frecuente que el derecho a la intimidad del trabajador en el uso extralaboral de estos dispositivos ceda frente a la capacidad de control del empresario y, por consiguiente, los Tribunales –en base a los datos obtenidos– admiten la resolución del contrato por vulneración de la buena fe contractual, la dimensión de la libertad informática no aparece ni siquiera mencionada. O, mejor dicho, lo hace en contadas ocasiones[12].

Y, dentro de éstas, resulta particularmente ilustrativa la STSJ Cantabria 18 de enero 2007[13]. Como se sostiene en la misma, es cierto que aunque «no se halle vedada la utilización de las nuevas tecnologías entre los instrumentos disponibles para el control y vigilancia de la actividad laboral, no comporta que su aplicación pueda hacerse de manera omnímoda e indiscriminada, con abstracción de los derechos fundamentales del trabajador, tal como se subraya, en sus diversos considerandos, por la Directiva 1995/46CE». Y, más concretamente, es exigible que se respete el «derecho a una vida privada, en cuya virtud el trabajador debe gozar de una razonable expectativa a un cierto grado de intimidad, dignidad, confidencialidad y autonomía»[14].

A partir de estos parámetros, en este pronunciamiento se declara que, a pesar de que la empresa notificó con carácter previo a los trabajadores la prohibición del uso del ordenador para fines extralaborales, se produjo una vulneración de su derecho a la libertad informática porque se instaló un software para su monitorización que excedía de la finalidad perseguida. En concreto, en la medida que «la recogida de datos no se limitaba a

11 Informe AEPD 2008\193.

12 Como botón de muestra (y con el rigor relativo que se le pueda atribuir a un «experimento» de este tipo), en una búsqueda jurisprudencial en el orden Social en la base de datos «Westlaw-Aranzadi», son muy pocos los resultados que aparecen a los términos «libertad informática» (15); «autodeterminación informativa» (9); «habeas data (4).

13 AS 2007\1030.

14 En la STJS Comunidad Valenciana 16 de febrero 2010 (AS 945) se estima que se ha producido una violación del derecho a la autodeterminación informativa (y a la intimidad), pues, la empresa sin haber establecido previamente un protocolo sobre el uso de los medios informáticos en el tiempo de trabajo, procede unilateralmente a auditar la seguridad del sistema informático, averiguando la utilización de todos los empleados de sus visitas a internet; describiendo no solo su número de visitas sino también las concretas páginas visitadas. En términos similares, STSJ País Vasco 17 de abril 2012 (AS 1676).

realizar una estadística de los accesos a Internet que no fueran los oficiales de la pagina de la [empresa] y los enlaces permitidos por esta, sino que especificaba asimismo los recursos de Internet solicitados (paginas web, gráficos, fotografías...etc.), y tal acopio de datos, en la medida en que entrañaba un control sistemático de los sitios visitados, así como de su frecuencia, tiempo de conexión y navegación, permiten reconstruir aspectos subjetivos relativos a la intimidad del trabajador, y ello excede sin duda de la finalidad declarada: conocer el uso que se hacía de Internet en horas de trabajo, que era el parámetro que debió modular el nivel y la intensidad de la recogida de datos, y que al ser rebasado deslegitima el comportamiento empresarial, pues constituye un principio básico de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, que sólo se podrán recoger datos de carácter personal para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido (art. 4.1), lo que también se deduce del Considerando 28 de la Directiva 1995/46 cuando indica que «todo tratamiento de datos personales debe efectuarse de forma lícita y leal con respecto al interesado; que debe referirse, en particular, a datos adecuados, pertinentes y no excesivos en relación con los objetivos perseguidos; que estos objetivos han de ser explícitos y legítimos, y deben estar determinados en el momento de obtener los datos».

En cambio, en la STSJ Comunidad Valenciana 28 septiembre de 2010[15] se alcanza una solución dispar. Se trata de un supuesto en el que una empresa, tras entregar a todos los trabajadores una carta (que firman) en la que se les comunica que queda terminantemente prohibido el uso de medios de la empresa (ordenadores, móviles, internet, etc.) para fines propios, tanto dentro como fuera del horario de trabajo, procede a la monitorización de dos trabajadores porque tiene sospechas de que están incumpliendo este protocolo. En concreto, realiza un control de sus ordenadores a través de un software que permite realizar capturas de pantalla. En opinión del Tribunal, obviando (por completo) la dimensión relativa al derecho a la libertad informática, se trata de un sistema de control «pasivo o poco agresivo», pues, se «limita» a capturar lo que está en pantalla, para comprobar el uso del ordenador por parte del trabajador. De modo que la medida adoptada necesaria, idónea, justificada y equilibrada. Además, –añade– este sistema no supone una invasión de su intimidad, «toda vez que la contraseña utilizada (…) impedía el acceso a sus archivos y el sofware instalado, como se dijo, sólo permitía la recuperación de pantallas.

Pese a esta disparidad de criterios entre esta doctrina judicial expuesta, posteriormente, la STS 6 de octubre 2011[16] entendió que no se daba la contradicción necesaria para poder entrar en el fondo. No obstante, esta sentencia de TS es muy ilustrativa de la línea interpretativa imperante en la jurisdicción social, pues, se afirma que «En el caso

15 AS 2011\47.

16 RJ 7699.

del uso personal de los medios informáticos de la empresa no puede existir un conflicto de derechos cuando hay una prohibición válida». De modo 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».

Así pues, «sentada la validez de prohibición tan terminante, que lleva implícita la advertencia sobre la posible instalación de sistemas de control del uso del ordenador, no es posible admitir que surja un derecho del trabajador a que se respete su intimidad en el uso del medio informático puesto a su disposición. Tal entendimiento equivaldría a admitir que el trabajador podría crear, a su voluntad y libre albedrío, un reducto de intimidad, utilizando un medio cuya propiedad no le pertenece y en cuyo uso está sujeto a las instrucciones del empresario de acuerdo con lo dispuesto en el art. 20 ET».

Criterios hermenéuticos que quedan consolidados con la STC 170/2013 al afirmar 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».

Sin embargo, a nuestro entender, esta matriz interpretativa expuesta resulta muy preocupante, especialmente, porque con independencia del sentido final de los fallos, los Tribunales están omitiendo el posible impacto de las medidas de monitorización empresarial sobre el derecho a la autodeterminación informativa (y su eventual o no vulneración). Sin obviar que, como afirma el Voto Particular de la STSJ Castilla y León\Valladolid 5 de diciembre 2012[17] esta capacidad de control empresarial admitida por la STS 6 de octubre 2011, «no excluye la posible vulneración del derecho a la intimidad cuando el seguimiento empresarial alcance a determinados aspectos íntimos del trabajador, como pudieran ser conversaciones privadas a través de chats, correos electrónicos y otras aplicaciones, esto es, cuando el seguimiento exceda del criterio genérico de proporcionalidad, con sus tres elementos constitutivos (necesidad, idoneidad y proporcionalidad)». O, siguiendo con el citado voto particular, «El Tribunal Supremo no ha declarado la procedencia de todos los despidos basados en un uso personal del ordenador y de las redes informáticas empresariales, ni creo que haya concedido una habilitación genérica a la dirección de las empresas para llevar a cabo un seguimiento exhaustivo de la actividad de sus empleados en la red. Es más, ni siquiera podía hacerlo en los estrechos márgenes del recurso de casación para la unificación de doctrina. Entenderlo así es una magnificación inasumible».

17 AS 2013\167.

Sin olvidar que «una cosa es que en determinadas circunstancias el empresario quede eximido de requerir el consentimiento del trabajador, y otra muy distinta es que el éste desconozca la existencia de un fichero de datos y el tratamiento que se está haciendo de los mismos»[18]. No obstante, por el momento, esta opinión (lamentablemente) tiene una predicación minoritaria. Ahondando en este enfoque de la jurisprudencia descrita por la STS 6 de octubre 2011[19], la STSJ Andalucía\Granada 13 de noviembre 2013[20] declara que la existencia de una prohibición absoluta y legítima de uso personal de estos medios de la empresa en horario de trabajo, excluye la necesidad por parte de la empresa de informar a los trabajadores de la existencia de un software que permita la monitorización de su uso (a través de un programa que capta un fotograma cada diez segundos y posteriormente es archivado durante un período de seis meses).

Repárese que en este caso, el software instalado permite un control indiscriminado de todos los trabajadores, con independencia de que haya sospecha o no de la existencia de un uso incorrecto o de un incumplimiento del protocolo de la empresa firmado por los trabajadores. Pero, a mayor abundamiento, aunque haya una prohibición de uso extralaboral de tales medios, la potencial violación del derecho a la libertad informática no queda excluida per se. O, dicho de otro modo, la recopilación sistematizada y mecánica de la actividad estrictamente laboral del trabajador (y ajustada al protocolo fijado por la empresa y consentido por empleado) puede ser reveladora de ciertos aspectos de su vida personal que son susceptibles de amparo constitucional. Dimensión, de nuevo, soslayada por los órganos jurisdiccionales.

Otro ejemplo (a nuestro entender) preocupante: la STSJ Castilla y León\Valladolid 5 de diciembre 2012[21] declara la procedencia del despido de una trabajadora porque lleva a cabo un uso particular de Internet que supera la media de estadística efectuada por la empresa y más de un 70% de las páginas a las que accede durante su jornada laboral corresponden a categorías ajenas a su actividad laboral en contra de la prohibición expresa de la empresa (pero sin que quede verificada la incidencia de tal dedicación extralaboral en el tiempo de trabajo, rendimiento o productividad). En concreto, la empresa a través de su Código de Conducta Telemática establece que «todas las páginas de Internet a las que accedan los trabajadores de IMESAPI, S.A. son registradas y almacenadas por el período legal establecido (dos años). La información almacenada incluye entre otras informaciones: usuario, equipo, fecha, hora, página visitada...».

Sin embargo, como recoge el Voto Particular de este pronunciamiento, debe tenerse en cuenta que conforme a la STJUE 19 de abril 2012 («Bonnier Audio AB y

18 Sagardoy Bengoechea (2005), p. 78.

19 RJ 7699.

20 AS 2013\2935.

21 AS 2013\167.

otros contra Perfect Communication Sweden AB», asunto C-461/10), «la identificación de la persona que se conecta a una red a partir de la dirección IP del correspondiente dispositivo de transmisión de datos (que es lo que consta en hechos probados que se ha hecho en este caso) supone comunicar y tratar datos personales y los Estados miembros deben procurar basarse en una interpretación de las Directivas comunitarias que garantice un justo equilibrio entre los distintos derechos fundamentales protegidos por el ordenamiento jurídico de la Unión y muy especialmente el principio de proporcionalidad, que es interpretado en términos idénticos a los contenidos en la jurisprudencia constitucional española (necesidad, idoneidad y proporcionalidad en sentido estricto) para garantizar un justo equilibrio entre los bienes jurídicos implicados».

## 3. VALORACIÓN FINAL

Los Tribunales están admitiendo un amplio control por parte del empresario de los instrumentos electrónicos propiedad de la empresa puestos a disposición de los trabajadores, siempre que haya directrices (conocidas por los trabajadores) que fijen las condiciones para su uso extralaboral. En este escenario, la intimidad del trabajador queda en un plano secundario, pues de este modo, se entiende que ha quedado disipada toda expectativa razonable de confidencialidad e intimidad.

Sin pretender entrar en la idoneidad o no de esta línea interpretativa (pues, excede del objeto de este estudio), en el presente ensayo hemos tratado de evidenciar que el derecho a la «libertad informática» o «autodeterminación informativa» no debería verse afectado (o subyugado) por esta omnímoda facultad empresarial. Sino todo lo contrario, pues, dependiendo de las circunstancias puede permanece subyacente y de un modo autónomo/independiente en todas estas situaciones.

Lo que significa que, aunque existan estas directrices para el uso extralaboral de los medios electrónicos propiedad de la empresa, el empresario sigue estando obligado a dar cumplimiento a las directrices que marca la LOPD. En caso contrario, existe el riesgo (cierto) de que esté incurriendo en una conducta contraria a un derecho fundamental.

Sin embargo, esta dimensión del problema no está recibiendo, a nuestro entender, un tratamiento adecuado por parte de los tribunales e inexplicablemente es soslayada reiteradamente (salvo contadas ocasiones).

Esperamos que el contenido de este breve trabajo contribuya a sacarlo del ostracismo que padece.

## 4. BIBLIOGRAFIA

Beltran de Heredia Ruiz, I. (2010). Las tecnologías de la información y de la comunicación en el ámbito laboral. En Peguera Poch (coord.), Principios de Derecho de la Sociedad de la Información. Pamplona: Aranzadi – Thomson/Reuters.

Calvo Gallego, J. (2012). TIC y poder de control empresarial: reglas internas de utilización y otras cuestiones relativas al uso de Facebook y redes sociales. Revista Doctrinal Aranzadi Social, 9, versión digital (BIB 2012\56).

Monereo Pérez, J. L. y López Insua, B. M. (2014). El control empresarial del correo electrónico tras la STC 170/2013. Revista Doctrinal Aranzadi Social, 11, versión digital (BIB 2014\122).

Sagardoy Bengoechea, A. (2005). Los derechos fundamentales y el contrato de trabajo. Madrid: Thomson-Civitas.