# POSIBILIDADES Y LÍMITES EN EL CONTROL DE LOS CORREOS ELECTRÓNICOS DE LOS EMPLEADOS PÚBLICOS A LA LUZ DE LA NORMATIVA DE PROTECCIÓN DE DATOS*

# POSSIBILITIES AND LIMITS IN THE CONTROL OF ELECTRONIC EMAILS BY PUBLIC EMPLOYEES FROM THE RULES OF DATA PROTECTION LAW

**Susana Rodríguez Escanciano**
Catedrática de Derecho del Trabajo
y de la Seguridad Social. Universidad de León
srode@unileon.es

Recibido: 10/03/2019 Aceptado: 11/04/2019



**Laburpena:** Datuak Babesteko eta Eskubide Digitalak Bermatzeko abenduaren 5eko 3/2018 Lege berriak aitortzen duenez, enplegatu publikoek intimitaterako eskubidea dute Administrazioak lan-tresna gisa beren eskura jarritako gailu digitalak erabiltzean, eta, xede horretarako, bis atal bat sartu da Enplegatu Publikoen Oinarrizko Estatutuaren 14.j) artikulura. Hala ere, eskubidea ez dago termino absolutuetan konfiguratuta, administrazio-arduradunek sartzeko duten ahalaren ondoriozko mugaketak izan baititzake. Bada, ahal horrek bi helburu dauzka: estatutuaren betebeharrak betetzen direla kontrolatzea eta tresna digital horien osotasuna bermatzea. Sakontasun handiagoko lege-edukirik ez egoteak ez du ahaztarazi behar, ordea, oinarrizko eskubideen eta auto-antolaketarako ahalen arteko oreka-puntua bilatu behar dela. Xede horretarako, organo judizialek emandako doktrinari heldu behar zaio, zeina gainbegiratze inbaditzaileenen ingurukoa den; hau da, posta korporatiboen gaineko gainbegiraketei buruzkoa da. Izan ere, eremu horretan ez dago pribatutasunerako eskubidea bakarrik sartuta, komunikazioen sekreturako eskubidea ere jorratzen baita.
*Gako-hitzak: enplegu publikoa, kontrol-ahala, posta korporatiboa, datuen babesa, intimitatea, komunikazioen sekreturako eskubidea*

**Resumen:** La nueva Ley 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, reconoce el derecho a la intimidad de los empleados públicos en el uso de los dispositivos digitales puestos a su disposición por la Administración como instrumentos de trabajo, introduciendo a tal fin un apartado bis en la letra j) del art. 14 del Estatuto Básico del Empleado Público. Ahora bien, tal derecho no está configurado en términos absolutos sino que puede sufrir algunas restricciones derivadas de la potestad de acceso por los responsables administrativos desarrollada al amparo de una doble finalidad: bien controlar el cumplimiento de las obligaciones estatutarias, bien garantizar la integridad de dichas herramientas digitales. La escasez de contenidos legales de mayor calado no debe de hacer olvidar la necesidad de buscar un punto de equilibrio atendiendo a la doctrina sentada por los órganos judiciales, vertida principalmente en las supervisiones más invasivas, esto es, las referidas a los correos corporativos, no en vano en este ámbito ya no está implicado solo el derecho a la privacidad sino también el derecho al secreto de las comunicaciones.
*Palabras clave: empleo público, potestad de control, correo corporativo, protección de datos, intimidad, derecho al secreto de las comunicaciones.*

**Abstract:** The new Law 3/2018, december 5th, on the Protection of Personal Data and the Guarantee of Digital Rights, recognizes the right to privacy of public employees in the use of digital devices placed at their disposal by the Administration as instruments of work, introducing for this purpose a paragraph bis in letter j) of art. 14 of the Basic Statute of the Public Employee. However, this right is not set in absolute terms but may suffer some restrictions derived from the power of access by administrative managers developed under a double purpose: either to control compliance with statutory obligations, or to guarantee the integrity of digital tools. The few legal content of greater importance should not make us forget the need to find a balance point between fundamental rights and the powers of self-organization. To this purpose, it is necessary to attend to the doctrine set by the judicial sentences, mainly in the most invasive supervisions, that is, those referring to corporate mail, because in this area, not only the right to privacy is involved, but also the right to secrecy of communications.
*Keywords: public employment, control power, corporate mail, data protection, privacy, right to secrecy of communications.*

* Este trabajo se ha realizado en el marco del proyecto de investigación LE004P17 («Sostenibilidad económica, social y medioambiental e innovación tecnológica: nuevas coordenadas para las políticas públicas de Castilla y León», 2017-2019), de la Junta de Castilla y León.

**Sumario**



## 1. La preocupante «huella digital» de los empleados públicos

Es una realidad incuestionable que la progresiva y vertiginosa irrupción de la tecnología digital, telemática, robótica, nanotecnología, plataformas, algoritmos, internet de las cosas, comunicaciones máquina a máquina, telefonía 5 G, realidad aumentada o inteligencia artificial, todo ello bajo la denominación de industria 4.0, está permitiendo a las empresas privadas optimizar y agilizar el desarrollo de la prestación profesional aumentando la productividad y competitividad e incrementando los márgenes de beneficios (Mercader, 2018). No es menos verdad que las bondades de las nuevas tecnologías en cuanto a los réditos empresariales no sólo se manifiestan *ad extra*, mejorando su posición estratégica en el mercado, sino *ad intra,* en la gestión ordinaria de los recursos humanos, pues, como fácilmente puede adivinarse, van a posibilitar el almacenamiento de una cantidad enorme de información relativa a la persona del trabajador entremezclada con el quehacer laboral e incorporada a ficheros de fácil manejo (Álvarez Cuesta, 2017).

Este doble cúmulo de circunstancias, contrastadas en el sector privado, pueden ser trasladadas *mutatis mutandis* a las oficinas públicas. Dos razones fundamentales avalan poder llegar a esta conclusión: por una parte, las exigencias de la denominada «administración electrónica» (a la luz de la actualmente derogada Ley 11/2007, de 22 de junio, cuyo contenido ha sido debidamente actualizado por las Leyes 39/2015, de 1 de octubre, de Procedimiento Administrativo Común, y 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público), que provocan un escenario en el que el cumplimiento de los principios de eficacia y eficiencia, unidos al de sostenibilidad presupuestaria, obligan a la tramitación *on line* de los expedientes como regla de actuación habitual de los entes públicos en sus múltiples vertientes con los ciudadanos y de imbricación de aquellos entre sí (Piñar, 2011); por otra, la gestión informatizada del personal facilita que todos los datos concernientes al desarrollo del vínculo funcionarial o laboral, desde el momento de la selección de personal, pasando por el desarrollo de los cometidos profesionales hasta su terminación, sean incluidos en soportes informáticos capaces de unificar de forma instantánea extremos dispersos convenientemente actualizados (Pérez de los Cobos, 1991).

Ahora bien, tampoco cabe ocultar que la aplicación de las modernas tecnologías informáticas en la dirección de los recursos humanos puede provocar ataques frente a los derechos fundamentales de los empleados públicos, no en vano va a permitir el manejo de un gran volumen de datos (formación y cualificación, aptitudes físicas y psíquicas, desempeño, retribuciones, dedicación, horas de entrada y salida, eventuales sanciones disciplinarias, movimientos en el interior de las dependencias administrativas, relaciones con los compañeros, mayor o menor vulnerabilidad a las enfermedades...), que sutilmente tratados a través de herramientas multicriteria, van a resultar de gran utilidad para la creación de perfiles completos sobre la personalidad de los afectados sin que sean conscientes de ello (Mercader, 2001). En otras ocasiones, el propio funcionamiento del servicio requiere la constancia de la «identidad digital» de los empleados públicos, que habitualmente utilizan firma electrónica, se sirven del mail corporativo, manejan plataformas administrativas internas (intranet) o, por no seguir, disponen de claves personales de acceso a los teléfonos u ordenadores (Arroyo Yanes, 2018).

Este peligro se multiplica exponencialmente cuando los datos son proporcionados de forma silente a través de los propios instrumentos de trabajo, que permiten el desempeño de las tareas inherentes al puesto y, al tiempo, mostrar a un empleado público transparente, estrechamente controlado dentro de una estructura organizativa marcadamente rígida y burocratizada (Goñi, 2004). La información proporcionada por estos utillajes puede ser utilizada como medio de prueba para acreditar comportamientos irregulares justificativos de una separación del servicio, de un despido o de otro tipo de sanciones, consecuencias favorecidas por la generalizada ambigüedad de las relaciones de puestos de trabajo, la falta de reglas claras sobre asignación de tareas y la carencia de formación en técnicas de liderazgo. Tan certera como esta afirmación lo es el carácter pluriofensivo del acopio y almacenaje y tratamiento de la información sobre un concreto empleado público, puesto que no sólo lesiona o pone en riesgo el derecho a la intimidad [art. 14 j) bis Real Decreto Legislativo 2/2015, de 30 de octubre, por el que se aprueba el Estatuto Básico del Empleado Público (EBEP)], sino también vulnera otros derechos fundamentales como el de la propia imagen, secreto de las comunicaciones o protección de datos personales (Martín Valverde, 1999).

## 2. El derecho a la protección de datos personales en la transición digital de las administraciones públicas

El interés legítimo del empleado público se circunscribe ahora no tanto a proteger un espacio propio de intimidad, cuanto a controlar sus datos personales insertos en los sistemas de comunicación porque sólo así puede ejercer un seguimiento sobre el uso secundario de esos datos y evitar la afectación negativa o postergación durante la relación de servicios. De la defensa del núcleo básico de la privacidad, entendida como pretensión de no injerencia de terceros, se debe evolucionar hacia una nueva dimensión, que faculta a cada sujeto a mantener el poder de disposición sobre el patrimonio informativo, surgiendo los derechos *on line* de los empleados (Ortega, 2017). Procede identificar, así, un nuevo derecho frente a renovadas formas administrativas de amenaza, el derecho a la libertad informática o el derecho a la autodeterminación informativa, reconocido por el Tribunal de Justicia de la Unión Europea[1] y por el texto constitucional español en el art. 18.4[2], configurado como aquél que tiene por objeto «garantizar la facultad de las personas para conocer y acceder a las informaciones que les conciernen, archivadas en bancos de datos (*habeas data*); controlar su calidad, lo cual implica la posibilidad de corregir o cancelar los asientos inexactos o indebidamente procesados; disponer sobre su transmisión...; en definitiva, este derecho entraña una facultad de decidir sobre la revelación y el uso de los datos personales, en todas las fases de elaboración y utilización de los mismos, es decir, su acumulación, su transmisión, su modificación y cancelación».

Advertida la agresividad de los dispositivos electrónicos frente a la privacidad del individuo en el marco de la relación de servicios, es necesario buscar un punto de equilibrio entre la potestad de auto-organización de la Administración a la hora de optimizar las posibilidades que le ofrecen las nuevas tecnologías, incluida la organización y el control de los efectivos, y la preservación de los derechos y libertades fundamentales del trabajador, singularmente el derecho a la protección de datos, idea sobre la que incide de manera clara el nuevo Reglamento UE 2016/679 del Parlamento europeo y del Consejo de 27 de abril de 2016 (RDP), cuyo art. 88.1 señala que «los Estados miembros podrán, a través de disposiciones legislativas o de convenios colectivos, establecer normas más específicas para garantizar la protección de los derechos y libertades en relación con el tratamiento de datos personales de los trabajadores en el ámbito laboral» (entendido este último en sentido amplio inclusivo del sector público y privado) (Sánchez Rodas, 2002)[3], «en particular a efectos de contratación de personal, ejecución del contrato laboral, incluido el cumplimiento de las obligaciones establecidas por ley o por convenio colectivo, gestión, planificación y organización del trabajo, igualdad y diversidad en el lugar de trabajo, salud y seguridad en el trabajo, protección de los bienes de empleados o clientes, así como a efectos del ejercicio y disfrute individual o colectivo de los derechos y prestaciones relacionadas con el empleo y a efectos de extinción de la relación laboral».

Pese a que el RPD es formalmente una norma europea de vocación uniformadora y armonizadora con aplicación directa[4], mantiene en realidad el espíritu e incluso la forma de Directiva, de manera que no sólo va a permitir sino también a promover la particularizada regulación nacional del derecho a la protección de datos en los centros de trabajo tanto a través de ley como de negociación colectiva. Los Estados miembros están inmersos en tales desarrollos legislativos, habiendo concluido ya algunos tal objetivo —pudiendo citar a Francia como uno de los pioneros

(Boto, 2018)[5]— y encontrándose otros aún en fase de tramitación. Entre los países que tardaron en completar el proceso se encuentra España, donde el primer proyecto de Ley Orgánica de Protección de Datos, de 24 de noviembre de 2017, frustró las expectativas creadas de contar con una legislación específica que diera mayor certeza tanto a las empresas (sobre el alcance y límites de su legítima potestad de utilización de datos) como a los trabajadores (sobre los contornos de sus derechos fundamentales), pues solo realizó una breve referencia, muy superficial, a las condiciones de ejercicio del poder de videovigilancia. Muchas fueron las enmiendas formuladas al proyecto inicial, pero quedaron paralizadas tras el nuevo panorama político, fruto de la moción de censura presentada por el grupo socialista, abriéndose posteriores escenarios legislativos (Miñarro, 2018).

Así, cabe dar cuenta de la novedad introducida por el, actualmente derogado, Real Decreto Ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos, pero carecía de contenido sociolaboral al regular aspectos relacionados con el funcionamiento de las autoridades de inspección y control, el régimen sancionador, el procedimiento a seguir ante posibles vulneraciones del RPD y la designación de la Agencia Española de Protección de Datos como interlocutor ante el Comité Europeo.

Afortunadamente, y siguiendo la estela del RPD, la nueva Ley 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDyGDD), viene a extender su marco de aplicación a las relaciones laborales y funcionariales donde ahora, sin lugar a dudas aunque con alguna matización, rigen los principios y garantías de la protección de datos, que deben de ser respetados por la Administración como responsable del tratamiento: consentimiento, licitud, transparencia, finalidad, adecuación, pertinencia, exactitud y actualización, temporalidad, seguridad a través de la confidencialidad, seudonimización o cifrado, evaluación de impacto y responsabilidad proactiva. A estos parámetros se unen una serie de salvaguardas de la persona, que se configuran como derechos subjetivos encaminados a hacer operativos los postulados genéricos: información, acceso, rectificación, supresión, bloqueo, limitación del tratamiento, portabilidad u oposición (Rodríguez Escanciano, 2018).

Esta Ley establece, al tiempo, límites en el ejercicio del poder de supervisión empresarial para guarecer, entre otros aspectos: el derecho de la intimidad de los trabajadores y empleados públicos tanto en el uso de los dispositivos digitales puestos a disposición por su empresario (art. 87), como frente al recurso a los mecanismos de videovigilancia y de grabación de sonidos en el lugar de trabajo (art. 89) o también a raíz del establecimiento de sistemas de geolocación en el ámbito laboral (art. 90), sin dejar de mencionar la posibilidad de desconexión del trabajador o empleado público para respetar sus tiempos de descanso (art. 88).

Ahora bien, la promulgación de una norma específica en materia de protección de datos aplicable a los recursos humanos del sector público, aunque supone un avance, no resuelve todos los problemas suscitados, lo cual va a obligar a seguir realizando una labor de integración entre: de un lado, el marco jurídico común del *habeas data*, compuesto ahora no sólo por la LOPDyGDD sino también por el propio RPD de aplicación directa y obligatoria en todos sus elementos pudiendo ser invocado por cualquier particular en todo tipo de relación pública o privada en que sea susceptible de materialización (Goñi, 2018); y, de otro, aquellas otras muchas instituciones propias del EBEP que puedan servir para proporcionar protección frente a situaciones concretas de abuso. Como fácilmente puede adivinarse, no resulta sencilla esta tarea de coordinación, máxime cuando las exigencias de transparencia administrativa llevan a que ciertos datos de los empleados puedan no sólo ser recabados sino difundidos a través de la información volcada en la página web corporativa (Gorriti, 2013).

Sea como fuere, buena muestra de tal complejidad hermenéutica obrante puede encontrarse en el acceso al contenido de los dispositivos digitales utilizados por los empleados públicos (hardware) y la inspección del uso de internet y del correo electrónico, que no ha encontrado una respuesta clara y tampoco la va a hallar a la luz de la nueva normativa de protección de datos (Camas, 2001), pues únicamente permite extraer unas pautas de actuación.

## 3. Supervisión de dispositivos digitales

El desarrollo de registros sobre el ordenador, tablet o smartphone, utilizados por el empleado público pero proporcionados por la Administración como instrumentos de trabajo, ha sido una cuestión muy controvertida, pues la realidad a monitorizar no se expone al exterior y tampoco es observable directamente sin entrar en el instrumento, recurriendo muchas veces a mecanismos sofisticados como silentes logueos o programas espías (*web bugs)*, que permiten el acceso subrepticio sin violar el *password,* o «registradores de

teclas» que facilitan la averiguación de las contraseñas, sobre todo para inspeccionar archivos, el sistema de mensajería (correo-e) o los accesos a páginas web. Todos estos supuestos constituyen tratamientos de datos de los servidores públicos, pues se memoriza una información susceptible de ser tratada, que no son convenientemente resueltos por el ordenamiento jurídico.

Partiendo de la obligación de los empleados públicos de «desempeñar con diligencia las tareas que tengan asignadas» (art. 53.1 EBEP), el art. 20.2 EBEP, en sus escuetos términos, dispone que «los sistemas de evaluación del desempeño... se aplicarán sin menoscabo de los derechos de los empleados públicos». A ello hay que añadir dos nuevos pasajes derivados de la promulgación de la LOPDyGDD: de un lado, el ya mencionado párrafo bis de la letra h) del art. 14, que reconoce el derecho subjetivo de los empleados públicos «a la intimidad en el uso de dispositivos digitales puestos a su disposición... así como a la desconexión digital en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales»; por otro, el art. 87.1 LOPDyGDD que reitera el derecho del empleado público a la protección de su intimidad en el uso de los dispositivos digitales puestos a su disposición por la Administración.

Por su parte, el párrafo segundo de este mismo precepto, haciendo referencia a los «trabajadores» y sin mencionar a los «empleados públicos», establece una serie de restricciones a tal derecho derivadas de la potestad de acceso por la Administración a los contenidos derivados de aquellos usos, potestad genéricamente condicionada por una doble finalidad («a los solos efectos de»): por un lado, «controlar el cumplimiento de las obligaciones laborales (o, mejor, estatutarias)» y, de otro, «garantizar la integridad de dichos dispositivos».

A la luz de tal tenor literal, cabe plantear un primer interrogante: si la falta de alusión a los servidores públicos en un pasaje que establece limitaciones a un derecho fundamental debe interpretarse de forma restrictiva, entendiendo que tales intrusiones no se aplican en el ámbito del sector público. Esta conclusión, aunque correcta desde el punto de vista técnico-jurídico, debe ser rechazada, pues generaría una diversidad de tratamiento injustificado derivada únicamente de la naturaleza jurídica pública o privada del empleador.

El análisis del régimen jurídico de las posibilidades de acceso por parte de los gestores de recursos humanos a los dispositivos digitales de los empleados públicos exige descender a los aspectos siguientes.

## 3.1. **Correo electrónico**

Cuando el control afecta al mail u otras formas de comunicación ya no está implicado sólo el derecho fundamental a la intimidad o a la protección de datos, sino también el secreto a las comunicaciones y ello provoca la aparición de un tercero respecto del cual la supervisión ya no puede explicarse en principio a través de las facultades que se atribuyen a la Administración en relación con sus empleados (Desdentado y Desdentado, 2018).

La escasez de contenidos legales y la falta de consideración de estos extremos no debe hacer olvidar la incidencia de la argumentación sentada en la Sentencia del Tribunal Europeo de Derechos Humanos de 5 de septiembre de 2017 (asunto 217/61, caso *Barbulescu II*), que, sin duda, va a provocar un cambio significativo en la doctrina constitucional y jurisprudencial española y ayudará a integrar el contenido del art. 87 LOPDyGDD, pues ya no basta con la prohibición de uso personal para superar la expectativa de confidencialidad, sino que es necesario, además, la advertencia de control clara y previa a la práctica de la supervisión (principio de transparencia), que debe afectar a la intimidad o al secreto de la comunicación en la menor medida posible (principio de proporcionalidad), tanto en lo que se refiere a su intensidad como en relación con los medios técnicos utilizados (principio de minimización).

Llegar a esta conclusión exige realizar un recorrido previo, si quiera breve, por los principales pronunciamientos anteriormente vertidos al respecto en relación con empresas privadas pero de fácil traslación al sector público, pudiendo dar cuenta de un devenir evolutivo marcado por las siguientes etapas:

### 3.1.1. *La consideración del canal de comunicación como abierto o cerrado*

Aun cuando el Tribunal Constitucional, en su sentencia 114/1984, vino a afirmar que el derecho al secreto de las comunicaciones no sólo era invocable frente al Estado sino que también se aplicaba a las relaciones privadas, de modo que la garantía de privacidad no sólo se extendía al contenido sino también al continente, cuando se vio abocado a reflexionar sobre las peculiaridades del secreto de comunicaciones en el ámbito laboral dicho criterio fue relativizado. Así, la Sentencia del Tribunal Constitucional 241/2012, de 17 de diciembre, prescinde del conocido juicio de proporcionalidad para adoptar ahora el canon de expectativa de intimidad atendiendo al carácter abierto o cerrado del canal de comunicación. La demandante de amparo es una trabajadora que venía desempe-


Núm. 16 zk./2019. Págs. 110-127 or.
ISSN: 2173-6405 e-ISSN: 2531-2103

ñando labores de teleoperadora especialista para la empresa Global Sales Solutions Line, S.L. Dicha empleada y una compañera instalaron un programa informático denominado «Trillian», de mensajería instantánea, en el disco duro de un ordenador, que era de uso indistinto por todos los trabajadores de la empresa y al que se accedía sin clave. La instalación del programa contravenía una orden empresarial expresa. A través de dicho soporte informático, las trabajadoras entablaban conversaciones en las que vertían comentarios despectivos, críticos e insultantes en relación con compañeros de trabajo, superiores y clientes. Dichas apreciaciones fueron descubiertas, por casualidad, por otro empleado que intentó utilizar la unidad «C» de ese ordenador, dando cuenta de ello a la empresa. El Tribunal Constitucional entiende que las conversaciones efectuadas por estas trabajadoras no quedan garantizadas por «el derecho al secreto de las comunicaciones» porque se trata de una forma de correspondencia abierta que permite su interceptación sin censura jurídica en base a las facultades directivas reconocidas al empleador en el ET. No existe en ese caso, a juicio del Máximo Intérprete de la Constitución, una «expectativa razonable de confidencialidad derivada de la utilización del programa instalado», atendiendo al carácter abierto del canal utilizado, una computadora de uso común y a las instrucciones vertidas por el empresario sobre las condiciones de uso (Aparicio, 2014).

### 3.1.2. *Prohibiciones de uso de medios electrónicos para fines privados*

El Tribunal Constitucional da un nuevo giro en la Sentencia 170/2013, de 17 de octubre, pues el derecho a la propiedad empresarial de los instrumentos de trabajo (ordenador) y el poder y control de la actividad laboral salen reforzados. En este caso, la empresa Alcaliber SA procede a interceptar el contenido de los correos electrónicos de un trabajador, registrados en el ordenador facilitado por la empresa, ante las sospechas de un comportamiento irregular derivado de la revelación a terceros de datos empresariales confidenciales, tipificando el convenio colectivo como falta leve la utilización para fines privados de los medios informáticos proporcionados por la empresa. Incidentalmente, el Tribunal entiende, sin perjuicio de lo que después se dirá en cuanto al secreto de las comunicaciones, que tal control empresarial no vulnera el derecho a la intimidad, pues se cumplen los requisitos del juicio de proporcionalidad: es una medida justificada, pues su práctica no resulta arbitraria o caprichosa, sino que se fundó en la sospecha de un comportamiento irregular del trabajador; es una medida idónea para la finalidad de verificar si el empleado cometía efectivamente la irregularidad sospechada (la revelación a terceros de datos empresariales de reserva obligada); es una medida necesaria, dado que el contenido de los correos electrónicos serviría de prueba del comportamiento irregular, no siendo suficiente el mero acceso a otros elementos de la comunicación como la identificación del remitente o destinatarios, que por sí solos no permitían acreditar el ilícito indicado; en fin, es una medida ponderada o equilibrada, pues únicamente se ha accedido al contenido de correos electrónicos que han reflejado información relativa a la actividad empresarial sin reflejar aspectos personales o familiares del trabajador (Santiago, 20114). Recuerda, además, en relación con el secreto a las comunicaciones que el art. 18.3 CE protege únicamente las que se realizan a través de medios o canales cerrados, no extendiéndose a las llamadas comunicaciones abiertas, que por sus circunstancias, se entiende que no pueden incluir correspondencia en régimen de confidencialidad.

Pero lo importante de esta nueva doctrina es que la previsión convencional en virtud de la cual se tipifica como falta leve el uso privado de medios tecnológicos de la empresa legitima el control empresarial sin necesidad de informar al trabajador. Esta tipificación se equipara, por el Tribunal Constitucional, a la existencia de prohibición absoluta del uso extraprofesional del correo electrónico, habilitando a la empresa para desplegar medidas de control al objeto de la verificación de su cumplimiento o no por los trabajadores, entendiendo que el afectado debía saber esta posibilidad de inspección porque, a su vez, debía conocer el convenio colectivo aplicable a la empresa, de modo que no podía existir una expectativa fundada y razonable de confidencialidad ni el secreto de las comunicaciones, no en vano la comunicación se produce en un canal abierto.

Por su parte, la Sentencia del Tribunal Supremo de 6 de octubre de 2011[6] entiende que las órdenes empresariales destinadas a concretar la finalidad de los instrumentos de control no deben someterse a los principios de proporcionalidad, idoneidad y necesidad, si existe una prohibición absoluta que impuso el empresario sobre el uso de medios de la empresa (ordenadores, móviles, internet, etc.) por los trabajadores para fines propios, tanto dentro como fuera del horario de trabajo, y no caprichosamente sino ante las sospechas fundadas de que se estaban desobedeciendo tales órdenes impartidas al respecto. Al objeto de comprobar el cumplimiento de tal prescripción, se instaló un programa espía capaz de captar las pantallas a las que accedía una trabajadora para su posterior visualización. Se trataba de un sistema poco agresivo que no permitía ver los archivos del ordenador que estaban protegidos por las contraseñas de cada uno de los usuarios. El Tribunal Supremo entiende que la orden expresa de prohibición lleva im-


Núm. 16 zk./2019. Págs. 110-127 or.
ISSN: 2173-6405 e-ISSN: 2531-2103

plícita la advertencia sobre la posible instalación de sistemas de control, sin que sea posible admitir que surja un derecho a que se respete la intimidad porque no existe tolerancia empresarial del uso personal sino que éste es ilícito. Tal y como establece este fallo, «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 concurrir una situación de tolerancia del uso personal, tampoco existe ninguna expectativa razonable de intimidad». Se bajan, por tanto, las barreras de la protección de la intimidad o el secreto, pues la tolerancia de la empresa es la que crea una expectativa de confidencialidad, de forma que si hay prohibición de uso personal, deja de haber tolerancia, y ya no existirá esa expectativa, con independencia de la información que la empresa haya podido proporcionar sobre el control y su alcance, que deviene innecesaria (Nores, 2014). Basta, por tanto, que haya prohibición para eliminar la expectativa de confidencialidad, sin que sea necesario que la empresa haya advertido de la posibilidad de control y de su alcance (Desdentado y Desdentado, 2018).

Por otro lado, conviene recordar que la Sala de lo Penal del Tribunal Supremo, en sentencia de 16 de junio de 2014[7], interfiere en la jurisprudencia dictada por la Sala Cuarta en relación a las facultades del empresario para adoptar medidas de control y vigilancia en un triple sentido: de un lado, en relación con los correos electrónicos que estén «sin abrir» por el destinatario rige la protección constitucional que otorga el art. 18.3 CE al secreto de las comunicaciones, siendo necesario contar con autorización judicial, pues no contempla el precepto «ninguna posibilidad, ni supuesto, ni acerca de la titularidad de la herramienta comunicativa (ordenador, teléfono, etc. propiedad de tercero ajeno al comunicante), ni del carácter del tiempo en el que se utiliza (jornada laboral) ni, tan siquiera, de la naturaleza del cauce empleado (correo corporativo), para excepcionar la necesaria e imprescindible reserva jurisdiccional en la autorización de la injerencia»; de otro, las comunicaciones «ya abiertas» por el destinatario que únicamente permanecen en las bandejas de entrada y salida, así como otros aspectos adyacentes (historial de navegación web, acceso al disco duro del ordenador, direcciones, frecuencias...), están tutelados por el art. 18.1 CE, referido al derecho a la intimidad, y por el 18.4 CE, relativo a la protección de datos personales, pero no por el derecho al secreto de las comunicaciones, debiendo estar a la conocida teoría de la proporcionalidad en el acceso; en fin, para el registro de medios electrónicos, propiedad del trabajador (*bring your own technology —BYOT—*), utilizados en el tiempo y lugar de trabajo, es necesario contar con autorización judicial (Miro, 2013).

### 3.1.3. *La teoría sobre la «expectativa razonable de intimidad»*

Es necesario traer a colación la doctrina del Tribunal Europeo de Derechos Humanos vertida en la Sentencia de 3 de abril de 2007, conocida como caso *Copland* (2007/23), que, aplicando el art. 8.1 de la Convención Europea de Derechos Humanos, entiende que los trabajadores conservan su derecho a la intimidad aun cuando los dispositivos electrónicos (teléfono, correo electrónico e internet) sean propiedad del empresario y su utilización se produzca durante el horario de trabajo, de suerte que las injerencias empresariales sobre tal derecho, o bien deben contar con el conocimiento del titular, o bien deben de estar previstas expresamente en una ley que las justifique.

Siguiendo esta pauta, la Sentencia del Tribunal Supremo de 26 de septiembre de 2007[8], enjuicia el despido del Director General de una empresa que prestaba servicios en un despacho sin llave, en el que disponía de un ordenador sin clave de entrada y conectado a la red de la empresa. Un técnico informático comprueba los fallos del ordenador, detectando la existencia de virus informáticos derivados de acceso a páginas poco seguras de internet. Entiende el Tribunal que no es aplicable el art. 18 ET porque el registro del ordenador supone el control de un medio de producción, no de un efecto privado del trabajador (que exigiría el máximo respeto a la intimidad y a la dignidad, contando con la asistencia de un representante legal de los trabajadores o, en su ausencia del centro de trabajo, de otro trabajador de la empresa, siempre que ello fuera posible). Se debe acudir, pues, al art. 20.3 ET, produciéndose un ataque al derecho a la intimidad del empleado al no haber sido avisado sobre la práctica del control ni sobre los límites al uso de este instrumento para fines privados.

En esta misma línea, cabe citar la Sentencia del Tribunal Supremo de 8 de marzo de 2011[9], cuyo relato fáctico consiste en un control empresarial realizado en los meses de enero y febrero sobre las redes de información con el objeto de revisar la seguridad del sistema de la corporación y detectar posibles anomalías en la utilización de los medios puestos a disposición de los empleados, evidenciándose que desde el ordenador utilizado por los jefes de turno se accedió a internet en horas de trabajo con un total de 5.566 «visitas» a páginas referidas al mundo multimedia-vídeos, piratería informática, anuncios, televisión, contactos, etc. La gran mayoría de esas visitas se produjeron en los turnos de trabajo del despedido y en tramos horarios en los que aquél estaba en el despacho. El Tribunal entiende que se ha ocasionado un atentado al derecho a la intimidad del trabajador porque no ha habido advertencia previa por parte de la empresa de

los límites de utilización de estos medios para fines privados ni sobre los controles que se iban a practicar (Sepúlveda, 2013).

El Tribunal Supremo, en sentencia de 13 de mayo de 2014[10], va más allá y considera que el hecho de que el empresario haya establecido unas reglas sobre el manejo de los ordenadores o haya previsto ciertas prohibiciones no significa que esté facultado para fiscalizar de cualquier forma, exigiendo con total rotundidad que los empleadores informen expresamente a sus empleados de la posibilidad de llevar a cabo controles de la actividad laboral con carácter previo a su materialización, no siendo suficiente que estos últimos conozcan la existencia del control del medio técnico por motivos de seguridad empresarial. Es necesario, por tanto, que los trabajadores hayan sido informados de la existencia específica del control de la actividad laboral y de los mecanismos a aplicar en orden a comprobar la corrección de los usos, sin perjuicio del posible diseño de medidas de carácter preventivo, como puede ser la prohibición total o parcial de determinadas conexiones.

Todo ello sin olvidar que el Tribunal Europeo de Derechos Humanos se ha vuelto a pronunciar en sentencia de 16 de enero de 2016 (asunto 61496/08, caso *Barbulescu I*), en virtud de la cual se entiende que la empresa puede monotorizar, previa advertencia, los instrumentos informáticos que utiliza un trabajador. Esta interpretación tiene su origen en un litigio por despido en el que un responsable de ventas de una empresa rumana crea a instancias de la corporación, una cuenta de Yahoo Messenger para la gestión y relaciones con los clientes, pero que utiliza también para entablar conversaciones privadas (con su pareja y con su hermano), circunstancia que se descubre en un control empresarial de la citada cuenta. La compañía había entregado previamente a los trabajadores un protocolo interno por el cual se dejaba clara «la prohibición de usar computadoras, fotocopiadoras, teléfonos, télex y fax para fines personales» (Pérez De los Cobos, 2017). El Tribunal entiende que el empresario en el ejercicio del control de la mensajería instantánea no ha violado *in integrum* el derecho de intimidad del trabajador, dado que ha sido proporcionado y limitado a la finalidad perseguida, que no era otra que analizar si el empleado estaba cumpliendo con las restricciones de la política corporativa aplicada por la empresa. Además, destaca que la vigilancia se ha limitado a la mensajería y no a otros posibles medios de comunicación, entendiendo que, si bien es verdad que el control afecta a la intimidad personal del trabajado, no lo hace de forma suficiente para entender conculcado dicho derecho, ya que del modo en que se ha desarrollado se ha conseguido un balance justo (Blázquez, 2018). No existe, por tanto, al calor del sentir mayoritario de la sala, una «expectativa razonable de privacidad» cuando se ha establecido una prohibición absoluta de uso personal en la política interna de la empresa, sin que concurran obligaciones empresariales adicionales en el sentido de justificar el amplio alcance de dicha prohibición o de informar a los trabajadores de forma precisa acerca de las medidas de control (García y Pastor, 2016). Al tiempo, más allá de la vulneración de derechos relativos a la intimidad y a la vida privada, el Tribunal no analiza la posible vulneración de un derecho fundamental a la protección de datos en el trabajo, que se muestra clara en este caso, pues la empresa no informó al trabajador sobre la creación, almacenamiento y uso de los ficheros de datos relativos a sus comunicaciones a través del correo electrónico y la tampoco sobre su finalidad.

#### 3.1.4. *La sentencia del Tribunal de Justicia de la Unión Europea en el asunto Barbulescu II: información previa y proporcionalidad*

En este pronunciamiento se rectifica el criterio de la anterior sentencia del mismo nombre (Barbulescu I) y se reconoce que los tribunales rumanos no verificaron si, pese a la existencia de instrucciones del empleador sobre el uso de los dispositivos, el trabajador había sido advertido con anterioridad de la vigilancia que iba a llevarse a cabo de las comunicaciones electrónicas efectuadas desde su cuenta profesional, ni tampoco hasta qué punto se ha producido una intromisión en la vida privada del trabajador en el ámbito de la relación de trabajo que hubiera podido alcanzarse por vías menos invasivas (Cuadros, 2007). Considera que no es suficiente, atendiendo al Código de Buenas prácticas para la protección de los datos personales del trabajador de 1999 y a la Recomendación del Comité de Ministros del Consejo de Europa (CM/Rec. 2015), sobre tratamiento de datos personales en el ámbito de la relación laboral, que la empresa hubiera remitido una notificación a sus empleados en la que se ilustraba sobre el despido de una trabajadora por motivos disciplinarios, después de haber utilizado para fines privados el internet, el teléfono y la fotocopiadora, sino que es necesario un aviso previo, antes de que comience la supervisión.

La sentencia viene a afirmar que la mera existencia de una prohibición de uso de los medios telemáticos de la empresa para fines personales no debe legitimar *per se* la vigilancia empresarial. Antes al contrario, para proceder a la fiscalización de estos medios es necesario, según el Tribunal Europeo de Derechos Humanos, que los órganos nacionales evalúen si la medida empresarial supera el siguiente test: a) si existió una información previa y clara a los trabajadores de las medidas de control que pueden utilizarse, de

su alcance y de su puesta en práctica; b) el grado de fiscalización empresarial y su extensión, tanto temporal como material; c) si existe un motivo legítimo que justifique la monitorización, al ser una medida invasiva e intrusiva; d) si concurren otras medidas alternativas menos agresivas y más respetuosas con la vida privada del trabajador y demás derechos fundamentales; e) qué uso proporciona el empresario a los datos obtenidos como consecuencia de la monitorización y si ese uso es legítimo para conseguir la finalidad que se pretenda; f) si se respetan determinadas garantías para el trabajador, de tal modo que si se accede al contenido de sus comunicaciones debe haber sido previamente notificado; g) en fin, si la medida de fiscalización se ha realizado al inicio del procedimiento sancionador y no después.

A la luz de estas pautas, el Tribunal llega a la conclusión de que la empresa vulneró el art. 8 del Convenio Europeo de Derechos Humanos (Blasco, 2018). En definitiva, «los tribunales nacionales deben velar por que el establecimiento por una empresa de medidas para vigilar la correspondencia y otras comunicaciones, sea cual sea su alcance y duración, vaya acompañada de garantías adecuadas y suficientes contra los abusos» (apartado 119) (Ruíz, 2018).

De este pronunciamiento pueden extraerse interesantes conclusiones: a) el trabajador ha de ser informado de las medidas que el empresario adopte a fin de controlar los medios de comunicación; b) es necesario diferenciar los flujos de comunicación de su contenido; c) el segundo control, el de los contenidos, exige justificaciones claras y, de producirse, ha de instrumentarse mediante el establecimiento de unas efectivas garantías a favor del trabajador; d) la información facilitada al trabajador ha de efectuarse con claridad y transparencia; y e) ha de realizarse, adicionalmente, con anterioridad a que se active y comience el control (Valdés, 2017). Muy significativa es la consideración que alerta sobre que «las instrucciones de un empleador no pueden reducir la vida social privada en el lugar de trabajo a cero, el respeto de la vida privada y de la confidencialidad de la correspondencia, que siguen existiendo, aun cuando pudieran estar restringidos en la medida de lo necesario» (Gallardo, 2017)[11].

Por lo tanto, para ser legítimo, el control debe superar, primero el test de transparencia en cuanto a la información previa al afectado, segundo, el de finalidad exigiendo un motivo sólido para la fiscalización; y tercero, el de proporcionalidad en lo que respecta a la preferencia de controles menos invasivos frente a los más intrusivos, sólo admitidos siempre que no exista otra opción real y no una mera comodidad o conveniencia empresarial (Molina, 2017). En definitiva, aunque el Tribunal reconozca que el empleador tiene un interés legítimo en garantizar el buen funcionamiento de la empresa, y que esto puede hacerse mediante el establecimiento de mecanismos para verificar que sus empleados cumplan con sus deberes profesionales de mantera adecuada y con la diligencia necesaria, concluye, que, tras un examen de los factores concurrentes, se vulneró la legislación aplicable internacional y europea en materia de protección de datos y los tribunales nacionales no establecieron un equilibrio justo entre los intereses del empresario y los derechos del trabajador.

Esta sentencia adopta una solución intermedia entre dos posiciones opuestas: por un lado, aquella que sostiene que la prohibición empresarial del uso personal es en sí misma legítima, que el control resulta inherente al contrato de trabajo y que con tal prohibición desaparece la expectativa de confidencialidad, por lo que no habría lesión del derecho a la intimidad ni del derecho al secreto de las comunicaciones[12]; por otro, aquella otra que defiende que la empresa no puede prohibir de forma general a sus empleados el uso del ordenador y de la red de internet en la empresa, considerando inadmisible una política de control general sobre dicho uso[13]. La conclusión componedora que aplica la sentencia Barbulescu II parte del principio de que no es suficiente la prohibición de uso personal para destruir la expectativa de confidencialidad; para ello es necesario, además del impedimento, la advertencia del control previa y clara en cuanto a la naturaleza de la supervisión, la existencia de motivos justificativos de dicho control y, cómo no en tanto materialización del principio de proporcionalidad, la utilización de aquellos medios menos intrusivos para la intimidad o el secreto de las comunicaciones.

#### 3.1.5. *Pronunciamientos judiciales recientes: los «hallazgos casuales»*

No resuelve la Sentencia Barbulescu II los supuestos de controles extraordinarios «ad hoc», esto es, los que se establecen frente a determinadas emergencias relacionadas, en muchos casos, con sospechas de actuaciones ilícitas del trabajador (hurtos, revelaciones de información confidencial, acoso, etc.). Hay que tener en cuenta que en estos casos el desconocimiento del control es la garantía de su eficacia. El problema se agrava porque, a diferencia de lo que ocurre en el ámbito penal, en el ordenamiento social no está prevista una autorización judicial para estos controles. El art. 76.5 Ley 36/2011, de 10 de octubre, reguladora de la Jurisdicción Social (LRJS), sólo diseña este instrumento para la entrada de la Inspección de Trabajo en el domicilio de los afectados; «tampoco cabe recurrir a las diligencias preliminares ni a la prueba anticipada, en los términos de los arts. 76.4 y 90.4 LRJS y art. 256 LEC porque, aparte de que su tramitación comprome-

tería la eficacia de la investigación, son medidas de preparación del proceso que no pueden aplicarse a un control laboral ordinario, ni a la investigación de un hecho futuro sobre el que ni siquiera hay certeza de que vaya a dar origen a un proceso» (Desdentado y Desdentado, 2018). Por tanto, las supervisiones extraordinarias derivadas de fundadas sospechas, es decir, las que excedan del marco normal establecido, tendrán que valorarse en función de los criterios de ponderación (justificación, idoneidad, necesidad y proporcionalidad).

Con posterioridad a la Sentencia Barbulescu II, cabe dar noticia sucinta y ejemplificativa de los siguientes pronunciamientos, capaces de demostrar que la solución dista aún de ser fácil:

1. Sentencia del Tribunal Europeo de Derechos Humanos de 22 de febrero de 2018 (asunto 2018/35, *Libert contra Francia*), en la que, tras una ausencia, el trabajador, jefe de brigada de vigilancia de la empresa nacional de ferrocarriles francesa, comprobó que, sin su consentimiento, la empresa realizó una revisión del ordenador que le había sido asignado después de que su sustituto encontrara documentos que le despertaron sospechas. En tal revisión, la empresa descubrió certificados de cambio de residencia a nombre de terceras personas que parecían falsificados y gran cantidad de material pornográfico, archivos alojados en una parte del disco duro denominado «datos personales», siendo despedido. El código deontológico de la empresa contemplaba expresamente que los medios informáticos puestos a disposición de los trabajadores tenían fines exclusivamente profesionales. En su recurso frente a la decisión extintiva, el trabajador alega la infracción del derecho a la vida privada y familiar, solicitando la nulidad del despido por ausencia de causa real y grave, solicitud desestimada por las dos instancias nacionales al considerar que el trabajador incurrió en incumplimiento manifiesto de las reglas sobre uso de material informático proporcionado por la empresa. El Tribunal Europeo de Derechos Humanos acepta la injerencia de la empresa en la vida privada del trabajador, pues los archivos personales fueron abiertos sin su consentimiento y sin ser informado. No obstante, al no indicar de forma precisa que eran privados sino personales, considera que no existía blindaje total para la empresa, llegando a la conclusión de que la actuación empresarial fue legítima, pues en el derecho francés son compatibles el principio protector de la intimidad con la potestad del empresario para acceder a los ficheros profesionales en ausencia del empleado en caso de que este no identifique tales archivos como privados.
2. Sentencia de la Sala de lo Social del Tribunal Supremo de 8 de febrero de 2018[14], que juzga un supuesto en el que, por un hallazgo casual (fotocopias de las transferencias bancarias encontradas por un compañero), la empresa tuvo indicios de la comisión de irregularidades por un empleado al recibir y aceptar dinero y obsequios de proveedores de su empleadora, actividad ésta expresamente prohibida por el código de conducta de la empresa. Bajo tales premisas, se considera adecuado el registro realizado por la empresa sobre el correo corporativo, alojado en el servidor, no de forma generalizada sino a través de una búsqueda selectiva, utilizando palabras clave y limitándose a los períodos en los que se produjeron las transferencias vinculadas a las sospechas, máxime cuando existe una política de uso estrictamente profesional de los medios de la empresa, que se recuerda a los empleados cada vez que acceden a sus terminales. La Sala entiende 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» (Bartolomé, 2018).
   En definitiva, esta línea jurisprudencial reconoce las facultades empresariales para regular el uso de los medios informáticos en la empresa, incluida las prohibiciones absolutas de su uso personal debidamente conocidas y la no exigencia de advertencia previa para la realización del control cuando hay restricción íntegra de ese uso, bastando, por tanto, la prohibición para eliminar la expectativa de confidencialidad y admitiéndose también la posibilidad de controles extraordinarios «*ad hoc*» en caso de sospecha de infracción (Desdentado y Desdentado, 2018).
3. Sentencia de Sala de lo Penal del Tribunal Supremo de 23 de octubre de 2018[15], que consideró nula la prueba presentada por una empresa demostrativa de un delito de apropiación indebida debido a la carencia del *prius habilitante* del consentimiento del trabajador o, al menos, de la previa advertencia de que


Núm. 16 zk./2019. Págs. 110-127 or.
ISSN: 2173-6405 e-ISSN: 2531-2103

el instrumento de trabajo podría ser examinado por el empresario, de la que podría llegar a derivarse una anuencia tácita al control o el conocimiento de esa potestad de supervisión, no en vano la supervisión empresarial no se rige por los mismos parámetros que la observación de las comunicaciones por los poderes públicos del Estado. El Tribunal de lo Penal entiende ahora que la forma de esa advertencia podría haber sido múltiple: expresa instrucción en orden a la necesidad de limitar el uso del ordenador a tareas profesionales, alguna cláusula conocida por ambas partes autorizando a la empresa a adoptar medidas de observación del entorno digital, la incorporación de alguna previsión en convenio colectivo donde se prohíba el uso personal o la obtención del previo consentimiento de quien venía usando de forma exclusiva el ordenador. La falta de observancia *ex ante* de alguno de estos requisitos genera una expectativa de intimidad que hace que resulte indiferente *ex post* que solo se hubieran buscado elementos que tuvieran relación con la actividad mercantil de la empresa o que se hubiese eludido cuidadosamente adentrarse en cualquier archivo o comunicación en la que se percibiese el más mínimo aroma de vinculación con la intimidad o privacidad. Asimismo, entiende que no es decisivo ni se puede considerar como piedra de toque que traiga la solución la distinción en función de si los mails habían sido ya recepcionados o tuvieron que abrirse, pues «este criterio solo tiene virtualidad en los procesos de comunicación postales donde es relevante la interceptación antes de que se cierre el proceso de comunicación o una vez agotado éste (la carta ya abierta que se guarda en un bolsillo es diferente —muy diferente— a la carta que se abre antes de llegar a su destinatario), pero esos moldes no son trasladables sin más a las comunicaciones vía telemática o telefónica» (Cárdena, 2018). Entiende el tribunal que «podrían existir razones fundadas para sospechar y entender que el examen del ordenador era una medida proporcionada y, además, se buscó una fórmula lo menos invasiva posible, pero faltaba el presupuesto inexcusable», esto es, la advertencia al trabajador, circunstancia que forma parte del contenido esencial del derecho fundamental.

Ante este razonamiento, surgen tres escenarios posibles: uno, si la prueba indebidamente valorada por ser ilícita es prescindible, el pronunciamiento de condena no perdería sustento pese a ser suprimida; dos, si la prueba indebidamente valorada resulta esencial, el pronunciamiento condenatorio perdía todo su apoyo y procedería la absolución; y tres —que es por la que opta el órgano juzgador—, si no puede deducirse de manera indubitada la influencia que pudo tener la prueba anulada en el procedimiento condenatorio, habrá que reenviarse la causa al Tribunal *a quo* para que dicte nueva sentencia o celebre nuevo juicio, en ambos casos, sin contar con ese medio probatorio. Se reenvía así la causa a la Audiencia Provincial para un nuevo enjuiciamiento partiendo de que el examen del ordenador vulneró derechos fundamentales y debiendo determinar qué pruebas no están afectadas por la conexión de antijuiridicidad y cuáles sí lo están, así como si las mismas pueden apoyar o no un pronunciamiento de culpabilidad.

A la luz de esta última sentencia, el principio de transparencia o de información al afectado debe ser respetado en todo caso.

## 3.2. **Páginas web**

A diferencia de lo que sucede en el supuesto anterior (correo-e), la navegación por internet en páginas web no relacionadas con el trabajo (al igual que la participación en chats abiertos o la intervención en foros de discusión o wikis) (Fernández Villazón, 2003) no tiene amparo en el derecho al secreto de las comunicaciones (López Mosteiro, 2001). En este caso, existe un acceso a información, pero no una verdadera interacción personal objetivamente tutelable, razón por la cual el juego de la facultad de inspección será más amplio a la hora de verificar los posibles incumplimientos contractuales del empleado público consistentes en consultar páginas web para fines particulares durante la jornada de trabajo, tal y como sucede con otras comunicaciones que transitan en abierto por el espectro radioeléctrico, cuales son las radiocumunicaciones bajo el tradicional «banda AM», o la más moderna «banda lateral única» —«single side band, SSB»— o las que se producen a través de canales de baja frecuencia, como el «*bluetooth*» o el «*near field comunication*» (Fernández Villazón, 2004).

Desde el punto de vista técnico, las posibilidades que existen en la actualidad para supervisar la navegación por internet pueden dividirse en cuatro grupos: programas de «monitorización» (aplicaciones que se instalan en el ordenador y que permiten saber en tiempo real las páginas visitadas, la duración de la conexión y las veces que se ha accedido sin que el usuario tenga conocimiento de ello), «cortafuegos» (permiten vetar y vigilar a la vez el acceso a determinadas páginas de internet, por lo que se consigue que el uso del ordenador sea exclusivo para fines profesionales), «proxy»

(ayudan a saber los sitios que han sido visitados por el trabajador) y «sniffers» (no se instalan en el equipo informático sino en el servidor, alertando sobre lo que el trabajador realiza a lo largo de la jornada laboral) (Toscani, 2014).

Bajo tales premisas, pese a la facilidad de todas estas variables, no cabe desconocer tampoco su sujeción al límite indeclinable constituido por el derecho a la intimidad, debiendo, por tanto, aunque el art. 87 LOPDyGDD guarda silencio, aplicarse los requisitos de los conocidos principios de información previa y de proporcionalidad. No cabe duda que la visita de determinados lugares web permite conocer directamente información sobre aspectos de la vida personal del empleado público relacionados con su intimidad (aficiones personales, gustos culinarios, preferencias sexuales, políticas, sindicales o religiosas...). Al tiempo, el análisis conjunto de los sitios a los que accedió, así como su frecuencia y tiempo de conexión, permiten reconstruir perfiles subjetivos íntimos (Martínez Fons, 2002).

### 3.3. **Protocolos y directrices internas**

Ante la inseguridad de los términos legales y la falta de respuesta clara de los órganos judiciales, cobra destacado protagonismo lo previsto en el párrafo 3.º del art. 87 LOPDyGDD, que recoge la obligación, como compromisos de responsabilidad social, de los empleadores de establecer criterios de utilización de los dispositivos digitales que respeten estándares mínimos de protección de la intimidad de acuerdo a los usos sociales y a los derechos reconocidos constitucional y legalmente, explicando de forma precisa las posibilidades autorizadas y estableciendo garantías para preservar la intimidad del trabajador, debiendo participar en su elaboración los representantes de los trabajadores (aunque, a falta de previsión legal más contundente, se permite una participación mínima a través de una simple comunicación, otra cosa es lo que deba suceder en la práctica). No basta, por tanto, una prohibición de uso genérica y absoluta, sino que resulta necesario especificar con claridad los contornos de actuación y el procedimiento de control a observar por la empresa (Richard, 2018).

Si el empresario no puede reducir a la nada el ejercicio de la vida privada social en el lugar de trabajo no son legítimas las políticas empresariales prohibitivas de la utilización por los trabajadores de los medios tecnológicos de las empresas, y en concreto de internet, para efectuar comunicaciones privadas. Esa utilización puede ser limitada, pero no absolutamente prohibida, con un requisito adicional, pues debe contar con la notificación al colectivo asalariado (Casas, 2018), sin que, en principio, este deber se module o reduzca ante posibles vestigios de incumplimientos laborales (a no ser ilícitos penales o ilícitos laborales muy graves), y sin que se establezcan tampoco exclusiones al principio de proporcionalidad en el control cuando las sospechas son fundadas en cuanto garantías para evitar que la prueba obtenida haya sido preconfigurada. Lo más adecuado es que en el diseño de estos protocolos participen activamente los representantes.

Ahora bien, si esta solución es clara para las empresas privadas, surge la duda sobre su aplicación en el sector público, pues el art. 87.3 LOPDyGDD no menciona a los empleados al servicio de las Administraciones. Puede entenderse, no obstante, que tal omisión queda suplida por la genérica referencia que en el párrafo primero de este precepto se hace a los empleados públicos. Resulta, además, de gran oportunidad la intervención de los representantes a la hora de evitar concesiones *in peius* (Molina, 2018), actuando como garantía más adecuada para la limitación de los «poderes jurídicos de que disponen las autoridades administrativas en la gestión de los recursos humanos» (Arroyo Yanes, 2018), máxime cuando, de un lado, el derogado art. 9.2 c) Ley 9/1987, de 12 de junio, de órganos de representación, determinación de las condiciones de trabajo y participación del personal al servicio de las Administraciones Públicas, atribuía a los representantes de los funcionarios públicos (juntas de personal y delegados de personal) competencias para la emisión de informe, a solicitud de la Administración Pública correspondiente, sobre «implantación o revisión de sistemas de organización y métodos de trabajo», tenor incorporado al art. 40.1 b) EBEP; y, de otro, el art. 64.5 f) ET atribuye a los representantes de los laborales el derecho a emitir informe sobre «la implantación y revisión de sistemas de organización y control del trabajo».

Ahora bien, tampoco cabe pasar por alto que la exigencia de compromiso con tales códigos de conducta puede conllevar una específica obligación de diligencia cualificada, más allá de los parámetros de los arts. 52, 53 y 54 EBEP. Al ser aceptados expresamente por el empleado público, se consideran como documentos vinculantes para el mismo, lo cual implica una doble consecuencia: de un lado, se presume que el servidor público conoce bien cuáles son los comportamientos o acciones que la Administración no va a tolerar en razón de su código ético; de otro, podrá ser sancionado por no adecuarse a lo indicado en dicho código de conducta siempre de conformidad con los principios y garantías del derecho disciplinario recogidos en los arts. 93 y ss. EBEP.


Núm. 16 zk./2019. Págs. 110-127 or.
ISSN: 2173-6405 e-ISSN: 2531-2103

### 3.4. **Negociación colectiva**

Además de estos instrumentos de *soft law*, nada impide a los interlocutores sociales incorporar al estricto ámbito del convenio colectivo o de los pactos y acuerdos soluciones concretas en materia de protección de datos dentro de la utilización de dispositivos digitales[16], tal y como prevé el art. el propio art. 91 LOPDyGDD, que invita a intervenir a la norma paccionada de forma expresa para pautar los contornos de este derecho, afirmando de forma superflua (por ser de sobra conocido) que los convenios colectivos tienen la posibilidad de establecer garantías adicionales a las legales. Esta conclusión no admite dudas para el sector privado, si bien la tarea no es fácil, pues se trata de una materia sumamente técnica, en la que todavía no hay referentes convencionales consolidados, no en vano las previsiones existentes hasta el momento son escasas y no pasan de meras remisiones a la normativa general, programáticas menciones sobre su aplicación en los procesos de selección o sobre la conveniencia del seguimiento de acciones de formación, inclusiones en el catálogo de infracciones muy graves de los incumplimientos, ampliaciones sobre los derechos de información de los representantes de los trabajadores[17], establecimiento de controles por el empresario de medios informáticos utilizados por el trabajador o, en el mejor de los casos, diseño del régimen jurídico aplicable al teletrabajo (Mercader y De la Puebla, 2018).

Más problemas se plantean en el sector público, pues, por un lado, el art. 91 LOPDyGDD no hace referencia expresa a este ámbito y, por otro, el art. 37.2 d) EBEP excluye del deber de negociación las materias relacionadas con «los poderes de dirección y control propios de la relación jerárquica», derivados de la potestad de organización del servicio, referido al aspecto personal de la relación de jerarquía fundamentado en la existencia de posiciones contrapuestas de superioridad y dependencia. Se habilita así la existencia de un poder unilateral de dirección, control y sanción de la actividad de los funcionarios, fundamentado en una relación de sujeción jerárquica y disciplinada, en función de las prestaciones definidas en los diferentes instrumentos de ordenación del personal (Mauri, 2008). Ahora bien, esta conclusión resulta, sin duda precipitada, pues en realidad debe de realizarse una interpretación no extensiva de esta exclusión, atendiendo a las matizaciones que pueden encontrarse en los dos siguientes pasajes: en el párrafo d) del apartado 1.º del art. 37 EBEP, que recoge entre los contenidos objeto de negociación, «los criterios y mecanismos generales en materia de evaluación del desempeño», esto es, el procedimiento que ha de medir y valorar la conducta profesional y el rendimiento o logro de resultados a efectos de la carrera profesional, la formación, la provisión de puestos de trabajo y la percepción de retribuciones complementarias ligadas al rendimiento o consecución de resultados por parte de los empleados públicos; por otro, y todavía con mayor claridad, en el apartado k) del mismo artículo referido a «condiciones de trabajo» básicas y estructurales (Roqueta, 2007). Haciendo una interpretación conjunta e integradora de estas previsiones, podría entenderse cómo es posible negociar aquellas potestades de autoorganización con manifestación en las condiciones de trabajo en tanto ámbitos típicos de la relación bilateral de servicio entre el funcionario y la Administración (Rivero y Val, 2007). Como ha señalado el Tribunal Supremo, «la potestad de autoorganización no excluye la negociación colectiva en todo aquello que afecte a las condiciones de trabajo, como sucede por regla general con las materias de personal»[18], no en vano «el concepto condiciones de trabajo se refiere a las circunstancias que repercuten en la forma en que se desempeña el trabajo en un puesto determinado»[19], susceptible, *in casu*, de ser controlado mediante dispositivos digitales utilizados como herramientas de trabajo.

## 4. La utilización del sistema de mensajería electrónica como cauce de conectividad permanente: el respeto a los tiempos de descanso

La combinación entre los avances en la digitalización y en la robotización implica una sustancial absorción de los trabajos administrativos directos y rutinarios por las máquinas, lo cual provoca que la presencia continuada del empleado público en las dependencias de la Administración pierda su sentido, pudiendo desarrollar la actividad laboral en cualquier momento y lugar (*anywhere, anytime*) (Alemán, 2017).

Sin ninguna duda, los empleados públicos digitales prolongan su jornada de trabajo más allá de los estándares de los empleados tradicionales sujetos a un horario y a un sistema de distribución de tareas mucho más rígido (Rodríguez y Pérez, 2017). Esta realidad cobra significativa importancia en el denominado teletrabajo, entendido como un modo de organizar la actividad laboral que aligera costes de infraestruc-

tura ante el uso intensivo de medios tecnológicamente avanzados (teléfono, fax, correo electrónico, módems, redes de área local, videoconferencia, etc.), permitiendo la separación física del empleado público de la oficina central o del centro de actividad pero intensificando las exigencias (Sánchez, 2016). En concreto, en la Administración General del Estado se ha desarrollado un programa piloto de implantación de esta modalidad de trabajo a distancia, donde el 31 por 100 de los acogidos percibió un aumento del volumen de trabajo[20].

La comunicación rápida y constante del empleado con su superior jerárquico a través de herramientas de procesamiento electrónico de la información (García Romero, 2012), unida al desarrollo de un quehacer profesional que exige pasar largos períodos de tiempo solo, sin contacto ni con compañeros ni con usuarios de los servicios públicos, se han revelado como una fuente de riesgo para la salud mental, asociado a la depresión y la ansiedad (Poquet, 2012; Purcalla y Preciado, 2013; Díaz, 2012; Sempere, 2013). Al tiempo, la necesidad de rápidas respuestas y las posibilidades de conexión permanente están eliminando todas las fronteras entre lo personal y lo profesional, difuminando las separaciones entre jornada de trabajo y tiempo de descanso ante una necesidad de conectividad permanente (Miró, 2016)[21], lo cual provoca un cierto trastorno compulsivo e involuntario a continuar trabajando, unido a un desinterés general por otro tipo de actividades (*workalcoholism*) y a un marcado sedentarismo (De las Heras, 2016). Ello sin olvidar que siempre es necesaria una fuerte autodisciplina y motivación para realizar las tareas, palpitando además un cierto sentimiento de extrañamiento por distancia, monotonía y aislamiento físico (Díaz, 2012; Sempere, 2013).

Ante esta «disrupción tecnológica» (Mercader, 2017), debe de ir cobrando fuerza, con autonomía propia y complementaria de los tradicionales límites de la jornada, el conocido «derecho de desconexión» del empleado público en aras a no perjudicar el bienestar de su salud neuronal[22]. Sobre esta facultad se pronuncia la LOPDyGDD, en su art. 88, que tomando como referente la Ley 2016-1088, de 8 de agosto, conocida como «Loi Travail» francesa (Vallecillo, 2017), diseña un sistema de tutela del tiempo de descanso. Asimismo, la LOPDyGDD introduce una nueva letra j bis en el art. 14 EBEP para reconocer el derecho de los empleados públicos «a la desconexión digital en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales».

En efecto, se reconoce el mencionado derecho a la desconexión digital de los empleados públicos a fin de garantizar, fuera del tiempo de trabajo efectivo, el respeto de su tiempo de descanso, permisos y vacaciones, así como de su intimidad personal y familiar, especialmente afectado «entre quienes ocupan los puestos de mayor nivel administrativo, los más cercanos a los núcleos decisionales de la Administración» (Arroyo Yanes, 2018). No obstante, quizá hubiera sido más conveniente configurar tal extremo como un deber para los responsables de los recursos humanos de no enviar notificaciones y mensajes de contenido laboral fuera de la jornada de trabajo y, en general, durante el tiempo de descanso de los empleados, salvo en casos de urgente necesidad y de guardias domiciliarias consideradas como tiempo efectivo de actividad[23], estando debidamente tipificada su transgresión (Talens, 2018). En este sentido, es de interés mencionar una reciente Sentencia del Tribunal Superior de Justicia de Asturias, de 27 de marzo de 2018[24], que reconoce cómo la empresa está obligada a contar con un procedimiento que permita al trabajador desactivar el sistema de posicionamiento global, de forma que no esté operativo a partir del momento en que finalice la jornada a no ser que el empleado preste su consentimiento, solución que debería trasladarse al marco del empleo público.

En todo caso, las modalidades de ejercicio de este derecho «potenciarán el derecho a la conciliación de la actividad laboral y la vida personal y familiar» y se sujetarán a lo establecido en la negociación colectiva o, en su defecto, a lo acordado entre la empresa y los representantes de los trabajadores (art. 88.2 LOPDyGDD). Esta previsión, sin duda, servirá de acicate para aumentar el número (muy escaso hasta ahora salvo honrosas excepciones)[25] de convenios colectivos o pactos que abordarán de forma específica esta cuestión. Esta previsión no presenta dificultad alguna en su materialización dentro del sector público, atendiendo a lo dispuesto en el art. 37.1.m) EBEP, que incluye entre las materias objeto de negociación aquellas referidas a «calendario laboral, horarios, jornadas, vacaciones, permisos..., así como los criterios generales sobre la planificación estratégica de los recursos humanos, en aquellos aspectos que afecten a condiciones de trabajo de los empleados públicos».

Es más, el art. 88.3 LOPDyGDD establece, como otra posibilidad, que el contenido concreto y las modalidades del ejercicio de este derecho se diseñarán por el empleador, previa audiencia (en principio, no necesariamente acuerdo) de los representantes de los trabajadores, por medio de una política interna que incluirá a los puestos directivos y prestará especial atención a los supuestos de realización total o parcial del trabajo a distancia así como en el domicilio del empleado, estando vinculado al uso con fines laborales de herramientas tecnológicas. Nada impe-


Núm. 16 zk./2019. Págs. 110-127 or.
ISSN: 2173-6405 e-ISSN: 2531-2103

diría, pues, que la Administración, previa audiencia a los representantes diseñara el régimen jurídico de este derecho. No se ha realizado así, empero, en la reciente Resolución de 28 de febrero de 2019, de la Secretaría de Estado de Función Pública, por la que se dictan instrucciones sobre jornada y horario de trabajo.

Con todo, como la finalidad de esta habilitación de este derecho es la de evitar «el riesgo de fatiga informativa», las posibilidades de participación de estos representantes no deben limitarse a una mera audiencia sino que deben de llevarse a cabo de conformidad con lo previsto en los arts. 33 y 34 Ley 31/1995, de 8 de noviembre de Prevención de Riesgos Laborales (LPRL), de aplicación también a las Administraciones Públicas, desarrollada para la Administración General del Estado en el Real Decreto 67/2010, de 19 de enero. Es más, deben ser objeto de negociación aquellas materias que establezca «la normativa de prevención de riesgos laborales» [art. 37.1 j) EBEP], cuyas disposiciones tienen el carácter de normas mínimas mejorables por la negociación colectiva (art. 2.2 LPRL) (Roqueta, 2007).

## 5. Conclusión

La nueva Ley 3/2018 ha extendido su marco de aplicación al empleo público introduciendo un apartado bis en la letra j) del art. 14 EBEP con el fin de establecer límites expresos a las facultades de control ejercidas por los responsables administrativos en relación con el uso de dispositivos digitales bajo la premisa de lograr el respeto debido a los derechos fundamentales. Buena muestra de esta búsqueda de equilibrio entre intereses contrapuestos puede encontrarse en el art. 87 LOPDyGDD, que, además de albergar la impronta de los recientes pronunciamientos judiciales, acoge las prerrogativas y principios tuitivos comunes a cualquier tratamiento automatizado, singularmente «transparencia» (información previa) y «miniminación» (preferencia por las supervisiones menos invasivas frente a las más intrusivas). Ello sin olvidar que la elaboración de unas reglas claras sobre el manejo de los medios informáticos y el conocimiento de tales instrucciones por los empleados públicos se convierte en el primer y principal requisito para legitimar el registro y evitar el riesgo de la vulneración del derecho a la intimidad y del secreto de las comunicaciones.

## 6. Bibliografía

Alemán Páez, F. (2017). El derecho de desconexión digital. Una aproximación conceptual, crítica y contextualizadora al hilo de la Loi travail n.º 2016-1088, *Trabajo y Derecho*, 30, 12-33.

Álvarez Cuesta, H. (2017). *El futuro del trabajo vs. el trabajo del futuro*. Madrid: Colex.

Aparicio Aldana, R.K. (2014). Las nuevas tecnologías en las relaciones laborales. Análisis de la STC 241/2012, de 17 de diciembre. *Revista General de Derecho del Trabajo y de la Seguridad Social*, 36, 379-391.

Arroyo Yanes, L.M. (2018). La digitalización de las Administraciones Públicas y su impacto sobre el régimen jurídico de los empleados públicos. *Revista Vasca de Gestión de Personas y Organizaciones Públicas,* 15, 82-99.

Barrios Baudor, G. (2019). El derecho a la desconexión digital en el ámbito laboral español: primeras aproximaciones. *Revista Aranzadi Doctrinal*, 1 (BIB 2018/14719).

Bartolomé Martín, A. (2018). Control empresarial del uso de medios tecnológicos, ¿caso cerrado?. *Información Laboral*, 6 BIB 2018/10356).

Blasco Jover, C. (2018). Trabajadores «transparentes»: la facultad fiscalizadora del empresario vs derechos fundamentales de los empleados. *Revista Internacional y Comparada de Relaciones Laborales y Derecho del Empleo*, 6, (3), 29-56.

Blázquez Agudo, E.M. (2018). *Aplicación práctica de la protección de datos en las relaciones laborales*. Madrid: Wolters Kluwer.

Boto Álvarez, A. (2018). Tratamiento de datos personales: entre la protección francesa dela vida privada y el mercado digital único. *Revista General de Derecho Administrativo*, 49.

Cadena Serrano, F.A. (2018). El derecho al entorno digital. *Diario La Ley*, 9307, 7.

Camas Roda, F. (2001). La influencia del correo electrónico y de internet en el ámbito de las relaciones laborales. *Revista de Trabajo y Seguridad Social* (Centro de Estudios Financieros), 224, 2001, 139-162.

Casas Baamonde, M.E. (2018). Informar antes de vigilar ¿Tiene el Estado la obligación positiva de garantizar un mínimo de vida privada a los trabajadores en la empresa en la era digital? La necesaria intervención del legislador laboral. *Derecho de las Relaciones Laborales*, 2, 2018, 103-121.

Cuadros Garrido, M.E. (2007). La mensajería instantánea y la STEDH de 5 de septiembre de 2017. *Aranzadi Doctrinal*, 11 (BIB 2017/43157).

De Las Heras García, M.A (2016). *El teletrabajo en España: un análisis crítico de normas y prácticas.* Madrid: CEF.

Desdentado Bonete, A. y Desdentado Daroca, E. (2018). La segunda sentencia del Tribunal Europeo de Derechos Humanos en el caso Barbulescu y sus consecuencias sobre el control del uso laboral del ordenador. *Información Laboral,* 1, 2018, 19-39.

Díaz Franco, J.J. (2012). Psicopatología relacionada con alteraciones por quebrantamiento en la organización del trabajo. En Collantes, M.P. y Marcos, J.I. (Coords.), *La salud mental de los trabajadores,* Madrid: La Ley.

Fernández Villazón, L.A. (2003). Las facultades empresariales de control de la actividad laboral, Pamplona: Aranzadi.

Fernández Villazón, L.A. (2004). A vueltas con el control empresarial sobre la actividad laboral: «test de honestidad», telemarketing, registro de terminales y uso —o abuso— de internet. *Tribuna Social*, 168, 35-40.

Gallardo Moya, R. (2017). Un límite a los límites de la vida privada y de la correspondencia en los lugares de trabajo. Comentario a la sentencia del Tribunal Europeo de Derechos Humanos (gran sala) de 5 de septiembre de 2017 en el caso Barbulescu II c Rumanía. *Revista de Derecho Social*, 79, 141-156.

*García González*, R. y Pastor Merchante, J. (2016). Límites a la necesaria flexibilización de los derechos a la intimidad y al secreto de las comunicaciones en el ámbito laboral: una reflexión tras la sentencia del TEDH de 12 de enero de 2016 en el caso Barbulescu. *La Ley,* 865/2016.

García Romero, B. (2012). *El teletrabajo*, Pamplona: Aranzadi.

Goñi Sein, J.L. (2004). Vulneración de derechos fundamentales en el trabajo mediante instrumentos informáticos, de comunicación y archivo de datos. En Alarcón Caracuel, M.R. y Esteban Legarreta, R. (Coords), *Nuevas tecnologías de la información y la comunicación y Derecho del Trabajo,* Albacete: Bomarzo.

Goñi Sein, J.L. (2018). La nueva regulación europea y española de protección de datos y su aplicación al ámbito de la empresa (incluido el Real Decreto-Ley 5/2018), Albacete: Bomarzo, 15.

Gorriti Bonguiti, M. (2013): Un sistema de reforma del empleo público alternativo a los recortes de personal. *Revista Vasca de Gestión de Personas y Organizaciones Públicas*, 4, 8.

López Mosteiro, R. (2001). Despido por uso de correo electrónico e internet. *Actualidad Laboral*, 41, 2001, 1132.

Martín Valverde, A. (1999). Contrato de trabajo y derechos fundamentales. Revista de Derecho Social, 6, 16.

Martínez Fons, D. (2002). Uso y control de las tecnologías de la información y comunicación en la empresa. *Relaciones Laborales*, 23-24, 200.

Mauri Majos, J. (2008). La negociación colectiva, Del Rey Guanter, S. (Dir.). Comentarios al Estatuto Básico del Empleado Público. Madrid: La Ley.

Mercader Uguina, J.R. (2001). Derechos fundamentales de los trabajadores y nuevas tecnologías: ¿hacia una empresa panóptica? *Relaciones Laborales*, 10, 14.

Mercader Uguina, J.R. (2017). El futuro del trabajo en la era de la digitalización y la robótica. Valencia: Tirant Lo Blanch.

Mercader Uguina, J.R. (2018). *El futuro del trabajo en la era de la digitalización y la robótica*, Valencia: Tirant Lo Blanch.

Mercader Uguina, J.R. y De La Puebla Pinilla, A. (2018). Protección de datos y relaciones colectivas. *Trabajo y Seguridad Social* (Centro de Estudios Financieros), 423, 70.

Miñarro Yanini, M. (2018). La Carta de derechos digitales para los trabajadores del Grupo Socialista en el Congreso: un análisis crítico ante su renovado interés. *Trabajo y Seguridad Social (*Centro de Estudios Financieros), 424, 94.

Miró Morros, D. (2013). El uso del correo electrónico en la empresa: protocolos internos. Actualidad Jurídica Aranzadi, 874 (BIB 2013/2511).

Miró Morros, D. (2016). El control de la jornada y el teletrabajo. Aranzadi Instituciones, BIB 2016/3956.

Molina Navarrete, C. (2017). El poder empresarial de control digital: ¿nueva doctrina del TEDH o mayor rigor aplicativo de la precedente? *IusLabor,* 3/2017, 287-297.

Molina Navarrete, C. (2018). Redes sociales, códigos de conducta y ciudadanía digital responsable del trabajado: cara B del consentimiento y libertad de expresión crítica. *Trabajo y Seguridad Social* (Centro de Estudios Financieros), 424.

Nores Torres, L.E. (2014). Algunas cuestiones sobre la utilización de las redes sociales como medio de prueba en el proceso laboral. *Actualidad Laboral*, 3, 315.

Ortega Giménez, A. (2017). *El nuevo régimen jurídico de la Unión Europea para las empresas en materia de protección de datos de carácter personal*. Pamplona: Aranzadi.

Pérez De Los Cobos Orihuel, F. (1991). *Nuevas tecnologías y relación de trabajo*. Valencia: Tirant Lo Blanch.

Pérez de Los Cobos Orihuel, F. (2017). El control empresarial sobre las comunicaciones electrónicas del trabajador: criterios convergentes de la jurisprudencia del Tribunal Constitucional y del Tribunal Europeo de Derechos Humanos. *Nueva Revista Española de Derecho del Trabajo,* 196 (BIB 2017/814).

Piñar Mañas, J.L., Dir. (2011). *Administración electrónica y ciudadanos*. Valencia: Tirant Lo Blanch.

Poquet Catalá, R. (2012). Teletrabajo y su definitiva configuración jurídica. *Trabajo y Seguridad Social* (Centro de Estudios Financieros), 351, 147.

Purcalla Bonilla, M.A. y Preciado Domenech, C.H. (2013). Trabajo a distancia vs. Teletrabajo: estado de la cuestión a propósito de la reforma laboral de 2012. *Actualidad Laboral*, 2, 217.

Richard González, M. (2018). Reglas para la investigación forense y aportación como prueba al proceso de correos y mensajes electrónicos del trabajador (comentario a la STS sala cuarta de lo social, n.º 119/2018. *Diario La Ley*, 9323, 7.

Rivero Lamas, J. y Val Tena, J.M. (2007). El derecho a la negociación colectiva de los funcionarios. *Revista del Ministerio de Trabajo y Asuntos Sociales*, 68, 219.

Rodríguez Escanciano, S. (2018). El derecho a la protección de datos personales en el contrato de trabajo: reflexiones a la luz del reglamento europeo. *Revista Trabajo y Seguridad Social* (Centro de Estudios Financieros), 423, 19-62.

Rodríguez Fernández, M.L. y Pérez Del Prado, D. (2017). Economía digital: su impacto sobre las condiciones de trabajo y empleo. Madrid: Fundación para el diálogo social, 21-22.

Roqueta Buj, R. (2007a). El ámbito objetivo de la negociación colectiva funcionarial y laboral en las Administraciones Públicas. En Consejo General del Poder Judicial. *La negociación colectiva en las Administraciones Públicas a propósito del Estatuto Básico del Empleado Público*. Madrid: CGPJ.

Roqueta Buj, R. (2007b). *El Derecho a la negociación colectiva en el Estatuto Básico del Empleado Público*. Madrid: La Ley.

Ruíz González, C. (2018). Las nuevas propuestas interpretativas del Tribunal Europeo de Derechos Humanos sobre el control del uso laboral de la tecnología de la empresa: Barbulescu y López Ribalta. *Cuadernos de Derecho Transnacional*, 10, 2.

Sánchez Iglesias, A.L., Coord. (2016). *Situaciones jurídicas fronterizas con la relación laboral*. Pamplona: Aranzadi.

Sánchez Rodas, C. (2002). El concepto de trabajador por cuenta ajena en el Derecho español y comunitario. *Revista Ministerio de Trabajo y Asuntos Sociales*, 37, 37-59.

Santiago Redondo, K.M. (2014). Intimidad, secreto de las comunicaciones y protección de datos de carácter personal. El art. 18 CE. *Relaciones Laborales*, 1, 2014, 119-138.

Sempere Navarro, A.V. y Kahale Carrillo, D.T. (2013): *Teletrabajo*. Madrid: Francis Lefebvre, 28.

Sepúlveda Gómez, M. (2013). Los derechos fundamentales inespecíficos a la intimidad y al secreto de las comunicaciones y el uso del correo electrónico en la relación laboral. Límites y contra límites. *Temas Laborales*, 122, 197-214.

Talens Visconti, E.E. (2018). La desconexión digital en el ámbito laboral: un deber empresarial y una nueva oportunidad de cambio para la negociación colectiva. *Información Laboral*, 4 (BIB 2018/8599).

Toscani Giménez, D. y Calvo Morales, D. (2014). El uso de internet y el correo electrónico en la empresa: límites y garantías. *Nueva Revista Española de Derecho del Trabajo*, 165, 197-224.

Valdés Dal-Re, F. (2017). Doctrina constitucional en materia de videovigilancia y utilización del ordenador por el personal de la empresa. *Revista de Derecho Social*, 79, 15-35.

Vallecillo Gámez, M.R. (2017). El derecho a la desconexión: ¿novedad digital o esnobismo del viejo derecho al descanso? *Trabajo y Seguridad Social* (Centro de Estudios Financieros), 408, 167-178.

## Notas

1 STJUE 8 abril 2014, asunto *Digital Rights Ireland* y 6 octubre 2015, asunto *Schrems*.

2 SSTCo 254/1993, de 20 de julio y 290 y 292/2000, de 30 de noviembre.

3 Sabido es que el concepto comunitario de funcionario se equipara al de trabajador por cuenta ajena. STJUE 24 marzo 1994, asunto *Van Poucke*.

4 Al igual que lo es el Reglamento UE 2018/1725, del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de estos datos.

5 Que contaba con la Ley 1978-7, de 6 de enero, relativa a la informática, los ficheros y las libertades, ha apostado por adaptarla a la nueva regulación a través de una Ley *omnibus*, la 2018-493, de 20 de junio, que a lo largo de 37 artículos introduce constantes modificaciones en la primera, además de innovar también la regulación de otros textos como el código penal, el de consumo, el de patrimonio, el de la educación, el general de las colectividades territoriales o el de defensa.

6 Rec. 4053/2010.

7 Rec. 2229/2013.

8 Rec. 966/2006.

9 Rec. 1826/2010.

10 Rec. 2229/2013.

11 Cfr. Ordinal 80.

12 Sentencia del Tribunal Europeo de Derechos Humanos de 16 de enero de 2016 (asunto 61496/08, caso Barbulescu I). También, STCo 170/2013, de 17 de octubre (caso Alcaliber) y STS 6 octubre 2011 (rec. 4053/2010).

13 SSTS 8 marzo 2011 (rec. 1826/2010) y 13 mayo 2014 (rec. 2229/2013),

14 Rec. 1121/2015.

15 Rec. 1674/2017.

16 Informes de la Agencia de Protección de Datos 252/2006, 0154/2010 y 0384/2010.

17 Posibilidad de ampliación admitida por la doctrina judicial. Vid., SSTSJ Cantabria 29 diciembre 2008 (rec. 1139/2008), Madrid 26 junio 2006 (rec. 2686/2006). Recientemente, STS 7 febrero 2018 (rec. 78/2017).

18 STS, Cont-Admtivo, 10 diciembre 2014 (núm. 5085/2011).

19 STS, Cont-Admtivo, 6 febrero 2007 (rec. 639/2002).

20 www.bci.inap

21 Importante es la STSJ Castilla y León 3 febrero 2016 (rec. 2229/2015), que obliga a una empresa a abonar horas extraordinarias a los teletrabajadores.

22 SAN 17 julio 1997 (Ar. 3370).

23 Tal y como sucede en el supuesto enjuiciado en la STJUE 518/15, de 21 de febrero de 2018, asunto *Matzak*, donde queda claro que «la obligación de permanecer presente físicamente en el lugar determinado por el empresario y la restricción que, desde un punto de vista geográfico y temporal, supone la necesidad de presentarse en el lugar de trabajo en un plazo de ocho minutos limitan de manera objetiva las posibilidades que tiene un trabajador (bombero belga) de dedicarse a sus intereses personales y sociales».

24 Rec. 2241/2017.

25 CC Grupo AXA (BOE, 10 octubre 2017); CC Barcelona Cicle de l'Agua (BOP Barcelona, 16 abril 2018); CC EUI Limitd Sucursal España (BOP Sevilla, 21 agosto 2018). Un estudio sobre tales instrumentos convencionales puede encontrarse en BARRIOS BAUDOR, G.: «El derecho a la desconexión digital en el ámbito laboral español: primeras aproximaciones», *Revista Aranzadi Doctrinal*, núm. 1, 2019 (BIB 2018/14719).


Núm. 16 zk./2019. Págs. 110-127 or.
ISSN: 2173-6405 e-ISSN: 2531-2103