La articulación de controles sobre el acceso a internet de los empleados públicos

Alejandra Boto Álvarez*

I. Introducción[1]

Nos encontramos aquí con una cuestión de inteligibilidad casi automática, que casi no precisa de mayores explicaciones. En efecto, parece cuestión de Perogrullo afirmar que el hecho de que un empleado utilice medios materiales de la empresa, como son los ordenadores, para una finalidad encaminada a una actividad privada repercute de forma negativa en el trabajo prestado, reduciendo el tiempo que debe dedicar a la actividad laboral y ocasionando con ello un perjuicio a los intereses del empleador. Cuando además nos encontramos en el ámbito de las Administraciones públicas, valores como la eficiencia y la eficacia en la gestión de los intereses generales no hacen sino exacerbar la relevancia palmaria de los efectos dañinos de estos abusos.

* Profesora Titular de Derecho Administrativo, Universidad de Oviedo, botoalejandra@uniovi.es.

[1] El presente trabajo ha sido elaborado en el marco del proyecto de investigación de referencia IDI/2018/000219 correspondiente a una ayuda a organismos públicos de investigación para apoyar las actividades de grupos de investigación en el Principado de Asturias concedida por el Gobierno de este al grupo SPAG (Servicios Públicos, Administraciones y Garantías) que coordina el profesor Tolivar Alas en la Universidad de Oviedo. Su perspectiva aúna los aspectos laborales y administrativos del tema, analizando la situación en el ordenamiento jurídico español en el marco del derecho de la Unión Europea a la protección de datos de carácter personal y del respeto a la vida privada del Convenio Europeo de Derechos Humanos.

Ahora bien, resulta asimismo bastante evidente que frente a estos valores existen también otros susceptibles de entrar en colisión. Nos referimos al secreto de las comunicaciones[2] y a la intimidad de los trabajadores,[3] sobre todo. Pero también es relevante la protección de la imagen y de los datos personales.[4] Incluso otros atributos como la propia voz[5], han sido analizados como bienes jurídicos de los trabajadores potencialmente afectados por los controles empresariales a través de las nuevas tecnologías. En ocasiones, incluso, se trae a colación el ejercicio de la libertad sindical, porque lo cierto es que los representantes de los trabajadores ven en los medios informáticos un canal idóneo y privilegiado para la difusión e implementación de su actividad reivindicativa. En el contexto actual, la propia regulación positiva se refiere ya a los derechos digitales de los trabajadores.[6]

En España, la ausencia de previsiones legales de corte específico sobre el uso de las nuevas tecnologías por parte de los trabajadores, y la carencia de criterios definidos para determinar hasta dónde puede llegar el ejercicio del poder de vigilancia y control empresarial sobre estos extremos, hacen preciso acudir a la

[2] Garantizado con carácter general, y en especial de las postales, telegráficas y telefónicas, salvo resolución judicial, en el artículo 18.3 de la Constitución Española. De manera monográfica sobre su juego véase, por todos, el estudio de Marín Alonso, Inmaculada, *El poder de control empresarial sobre el uso del correo electrónico en la empresa. Su limitación en base al secreto de las comunicaciones*, Valencia, Tirant lo Blanch, 2005.

[3] El artículo 18.1 de la Constitución Española no sólo garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen, sino que también dispone que la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos (artículo 18.4). Este último inciso ha sido visto como el fundamento que en el Derecho español permitiría hablar de un derecho fundamental a la protección de datos, que como tal no está recogido en la Constitución y tampoco en el Convenio Europeo de Derechos Humanos. Sí en cambio en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea. Sobre su génesis es sumamente ilustrativa la lectura de Murillo de la Cueva, Pablo Lucas y Piñar Mañas, José Luis, *El Derecho a la autodeterminación informativa*, Madrid, Fundación Coloquio Jurídico Europeo, 2009.

[4] Estos aspectos vienen regulados, como se ha visto en la nota precedente, en el mismo artículo de la Constitución. La protección de la propia imagen se presenta de particular importancia en el caso de la video vigilancia y, precisamente un caso planteado en relación con el control por ese medio a un empleado en una Universidad pública fue el que en su momento supuso un avance crucial en la interacción entre ambos derechos. Al respecto, *véase*, Jiménez-Castellanos Ballesteros, Inmaculada, "Videovigilancia laboral y derecho fundamental a la protección de datos", en: *Temas laborales: Revista andaluza de trabajo y bienestar social*, núm. 136, 2017, pp. 129-156, en particular pp. 136 y ss.

[5] Sorzano Volart, Mª Carmen y Núñez-Cortés Contreras, Pilar, "Medios de control empresarial y vulneración de derechos de los trabajadores", en: Herrán, Ana I., Emaldi Cirión, Aitziber y Enciso, Marta (coord.), *Derecho y Nuevas Tecnologías*, Bilbao, Universidad de Deusto, 2011, pp. 207-218.

[6] La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

regulación general: el Estatuto de los Trabajadores[7] (y en el campo particular de la Administración, el Estatuto Básico del Empleado Público);[8] el contenido de los convenios colectivos y lo establecido por la jurisprudencia. Esto último no siempre resulta de sencilla aplicación, porque existen muchos pronunciamientos dispares y extravagantes[9] y, además, cuando el sujeto empleador es la Administración topamos con una dificultad añadida porque, hasta ahora, la actividad litigiosa en la materia se ha producido mayoritariamente en el orden social.[10] Por ello se impone

[7] Cuyo texto refundido vigente fue aprobado por el Real Decreto Legislativo 2/2015, de 23 de octubre.

[8] Cuyo texto refundido vigente fue aprobado por el Real Decreto Legislativo 5/2015, de 30 de octubre.

[9] Una muestra de los vaivenes jurisprudenciales en la materia puede consultarse en Martínez Fons, Daniel, "El control empresarial del uso de las nuevas tecnologías en la empresa", en: Luque Parra, Manuel (coord.), *Relaciones laborales y nuevas tecnologías*, Madrid, La Ley, 2005, pp. 185 y ss. *Véase también*, Montoya Melgar, Alfredo, "Nuevas tecnologías y buena fe contractual (buenos y malos usos del ordenador en la empresa)", en: *Relaciones laborales*, núm. 1, 2009, pp. 31-57.

[10] En el Derecho español la categoría general de los empleados públicos comprende a los funcionarios de carrera; los funcionarios interinos; el personal laboral, ya sea fijo, por tiempo indefinido o temporal; y el personal eventual. Son funcionarios de carrera quienes, en virtud de nombramiento legal, están vinculados a una Administración Pública por una relación estatutaria regulada por el Derecho Administrativo para el desempeño de servicios profesionales retribuidos de carácter permanente. Son funcionarios interinos los que, por razones expresamente justificadas de necesidad y urgencia, son nombrados como tales para el desempeño de funciones propias de funcionarios de carrera cuando se dan una serie de causas tasadas. Por su parte, es personal laboral el que en virtud de contrato de trabajo formalizado por escrito, en cualquiera de las modalidades de contratación de personal previstas en la legislación laboral, presta servicios retribuidos por las Administraciones Públicas. Finalmente, el personal eventual es el que, en virtud de nombramiento y con carácter no permanente, sólo realiza funciones expresamente calificadas como de confianza o asesoramiento especial, siendo retribuido con cargo a los créditos presupuestarios consignados para este fin. Para aproximarse con más detalle a la estructura del sistema es de inestimable ayuda la guía de Sánchez Morón, Miguel, *Derecho de la función pública*, Madrid, Tecnos, 11ª ed., 2018. La convivencia de todas estas categorías de empleados públicos conlleva también distinto foro jurisdiccional competente para discutir el régimen jurídico de cada uno de los colectivos indicados. El punto de partida que es necesario conocer es que los juzgados y tribunales del orden contencioso-administrativo conocen de las pretensiones que se deduzcan en relación con la actuación de las Administraciones públicas sujeta al Derecho Administrativo, pero el personal laboral de la Administración en su régimen jurídico se rige por la legislación laboral y por las demás normas convencionalmente aplicables, mientras que el Estatuto Básico del Empleado Público sólo resulta de aplicación en aquellos preceptos que así lo dispongan. A su vez, la competencia de la jurisdicción social tiene en su Ley reguladora una formulación bastante prolija. La respuesta rápida es que el contrato de trabajo del personal laboral es competencia de los juzgados y tribunales del orden social, pero las incidencias previas a la constitución del vínculo, como son las relativas al proceso de selección -desde los actos relativos a la oferta de empleo, la convocatoria y sus bases, las pruebas y su desarrollo, la dotación, etc.-, en la medida en que se rigen por el Derecho Administrativo, se han de plantear ante el orden contencioso administrativo, al menos cuando se realizan directamente por un sujeto con personalidad jurídico-pública y no por personificaciones instrumentales de Derecho privado. Sobre el tema, con profusas

un estudio previo de la doctrina laboral sobre estos aspectos para luego analizar las posibilidades de su traspaso al ámbito administrativo de la función pública.

En relación con este último punto debe hacerse otra precisión. El extremo que con mayor frecuencia se debate ante la jurisdicción social gira entorno a saber si el abuso de internet y del correo electrónico en el trabajo puede ser causa de despido. Normalmente, en el ámbito privado, no llegan hasta los tribunales casos en que como consecuencia del abuso en las nuevas herramientas de trabajo se apliquen otras medidas disciplinarias menos graves; sin embargo, este es un aspecto muy importante en el ámbito concreto de los empleados públicos, en particular cuando hablamos de funcionarios de carrera, dado el juego de su inamovilidad.[11]

Por las limitaciones evidentes de un trabajo de corte como el presente, aquí no se puede aspirar a presentar todo el impacto de la creciente digitalización en la esfera de los derechos de los empleados públicos,[12] ni tampoco se puede pretender esbozar siquiera todas las vertientes del uso de tecnologías de la información y la comunicación al servicio del genérico poder de vigilancia del empleador.[13] Se prestará atención exclusiva, en coherencia con el intitulado del artículo, al control directo de este sobre el uso de internet por parte de los trabajadores. No se trata, pues, de estudiar el control empresarial sobre los trabajadores *a través* de las TIC, sino el control empresarial *sobre* las TIC que emplean los trabajadores; lógicamente, eso sí, la mayor parte de las veces el control se realiza precisamente a través asimismo de TIC, dándose la conjunción de ambas preposiciones.

referencias jurisprudenciales, puede verse el trabajo de Nores Torres, Luis Enrique, "La competencia para resolver los conflictos del personal laboral al servicio de las AA.PP., en particular, los relacionados con las bolsas de trabajo", *Elderecho.com* (tribuna), 1 de junio de 2014. También cabe señalar que la garantía del cumplimiento de la legislación de prevención de riesgos laborales es competencia del orden social, y que en relación con la tecnología está aceptada la existencia clara de riesgos de estrés (*véase*, Rodríguez Escanciano, Susana, *Derechos laborales digitales: garantías e interrogantes*, Valencia, Tirant lo Blanch, Valencia, 2019, pp. 242 y ss.). La delimitación competencial no siempre es sencilla, como demuestra la reciente sentencia, con un interesante voto particular, del Tribunal Superior de Justicia del País Vasco, sala de lo social, de 2 de abril de 2019, recurso núm. 350/2019.

[11] La inamovilidad en la condición de funcionario de carrera es un fundamento de la propia regulación administrativa de su régimen jurídico de conformidad con lo dispuesto en el artículo 1.3.e) del Estatuto Básico del Empleado Público y es un derecho individual propio de su relación de servicio según el artículo 14.a) del mismo texto legal.

[12] Que es innegable a nivel global y que afecta a cuestiones que van desde el reclutamiento, a sus nuevas obligaciones como empleados digitales como las relativas a la utilización de determinadas plataformas administrativas internas para la gestión de sus derechos, o a la de sostener una firma digital del órgano cuya titularidad ostentan. Sobre el tema resulta de cita ineludible el trabajo de Arroyo Yanes, Luis Miguel, "La digitalización de las Administraciones públicas y su impacto sobre el régimen jurídico de los empleados públicos", en: *Revista vasca de gestión de personas y organizaciones públicas*, núm. 15, 2018, pp. 82-89.

[13] Geolocalización, lectores corporales, obligación de portar dispositivos electrónicos activos, aplicación de algoritmos e inteligencia artificial, etc.

II. El estado de la cuestión en el orden laboral español: activismo judicial

A la hora de evaluar las posibilidades de articular un control empresarial sobre el uso de las nuevas tecnologías por parte de los trabajadores, parece esencial distinguir entre el acceso a través del ordenador de la empresa a páginas web y el uso del correo electrónico. Y es que el acceso a páginas web no está protegido por el artículo 18.3 de la Constitución, ya que en este caso no hay comunicación privada que proteger. Doctrina y jurisprudencia son pacíficos al respecto.[14]

Así las cosas, podría pensarse que la primera dimensión del ejercicio del poder de dirección y vigilancia del empresario no choca con ningún Derecho fundamental de los trabajadores. Excluida, conforme a lo que se acaba de exponer, la aplicación del artículo 18.3 de la Constitución a este supuesto, cabe sin embargo pensar que, aun así, esta última actividad (la "navegación" por internet) puede recaer en el ámbito objetivo de protección de la intimidad del trabajador.

Como se verá más adelante, el argumento ha tenido predicamento ante el Tribunal Europeo de Derechos Humanos y así se ha acabado recepcionado en España. No obstante, en este punto es esencial tener presente que, a pesar de ciertas vacilaciones iniciales, abundante jurisprudencia ha considerado que los ordenadores puestos a disposición de los trabajadores para su actividad profesional no son "efectos personales" suyos (clara diferencia, pues, con el supuesto en que lo que se procede a registrar es una taquilla, por ejemplo). Este extremo fue definitivamente confirmado por la sentencia del Tribunal Supremo de 26 de septiembre de 2007.[15]

En todo caso, este tipo de controles tiene que realizarse siempre con respeto a la dignidad del trabajador. Esto no implica que éste tenga que estar presente cuando se realice la actividad inspectora, pero sí que esté expresamente advertido de la posibilidad de que tal cosa ocurra. Y es que existe un hábito social generalizado

[14] *Vid.* Sánchez-Rodas Navarro, Cristina, "Información y derecho: restricciones en el uso del correo electrónico e internet por parte de los trabajadores por cuenta ajena", en: Vidal Climent, Vicente y García Manglano, Miguel (coords.), *Información, libertad y derechos humanos: la enseñanza de la ética y el derecho de la información*, Valencia, Fundación COSO, 2004, p. 315.

[15] Extracto del Fundamento de Derecho tercero de la sentencia citada: "(…) las medidas de control sobre los medios informáticos puestos a disposición de los trabajadores se encuentran, en principio, dentro del ámbito normal de esos poderes: el ordenador es un instrumento de producción del que es titular el empresario 'como propietario o por otro título' y éste tiene, por tanto, facultades de control de la utilización, que incluyen lógicamente su examen. (…) El empresario tiene que controlar el uso del ordenador, porque en él se cumple la prestación laboral y, por tanto, ha de comprobar si su uso se ajusta a las finalidades que lo justifican, ya que en otro caso estaría retribuyendo como tiempo de trabajo el dedicado a actividades extralaborales. Tiene que controlar también los contenidos y resultados de esa prestación". Al respecto puede verse el comentario a la sentencia de Manteca Velarde, Víctor, "Control del empresario sobre el uso del ordenador por los trabajadores: alcance, contenido y límites", en: *Actualidad jurídica Aranzadi*, núm. 749, 2008.

de tolerancia con ciertos usos personales moderados de los medios informáticos y de comunicación facilitados por la empresa a los trabajadores. Esa tolerancia crea una expectativa también general de confidencialidad en esos usos.[16]

Diversa jurisprudencia ha sentado desde entonces que el hecho de que los ordenadores no tengan clave personal de acceso, o estén ubicados en despachos sin llave, no implica que los trabajadores hayan asumido de forma tácita la posibilidad de dichas inspecciones; tampoco puede utilizarse un examen antivirus con dicho propósito. En cualquier caso no es sencillo construir una síntesis de resumen para la cuestión, pues la práctica judicial demuestra lo complicado que resulta trazar la línea de frontera entre un uso socialmente tolerable y lo que en cambio es un abuso.[17] Las discrepancias en la materia se han manifestado también, en la práctica judicial española, entre distintos órdenes jurisdiccionales. Ha sucedido así que, para el mismo caso, el Tribunal Supremo entiende suficiente o no la información previa del control empresarial para surtir efectos según se esté pronunciado en el orden laboral o en el penal.[18] Existen algunos ordenamientos europeos que han tratado de regular específicamente esta cuestión, pero en España, son los jueces y tribunales los que han de cubrir lagunas legales, dando lugar a lo que la mejor doctrina ha denominado el "activismo judicial",[19] expresión que se ha tomado prestada para el intitulado de esta sección.

Por último, cuando lo que se pretende controlar por el empresario es el correo electrónico, la indudable afectación al derecho fundamental hace que las cautelas se exacerben, aumentando la falta de concreción y la confusión. Existen pronunciamientos judiciales muy dispares en función de si lo que se

[16] El argumento fue por primera vez utilizado en el contexto español por el Tribunal Constitucional en su sentencia 241/2012, de 17 de diciembre. Sobre su génesis y evolución pueden consultarse los trabajos de de Rodríguez Lainz, José Luis, "El principio de expectativa razonable de confidencialidad en la STC 241/2012, de 17 de diciembre", en: *Diario La Ley*, núm. 8122, 2013 y Talens Visconti, Eduardo Enrique, "La expectativa razonable de confidencialidad como presupuesto de vulneración de derechos fundamentales en la fiscalización informática llevada a cabo por el empresario", en: *Aranzadi Social: Revista Doctrinal*, vol. 6, núm. 8, 2013, pp. 271-276.

[17] Algunos ejemplos concretos, con la recomendación de prácticas para evitar la nulidad probatoria del control empresarial de los medios informáticos pueden encontrarse en Picó i Junoy, Joan, "El control empresarial de las TIC y sus límites", en: Herrán, Emaldi Cirión y Enciso, *supra* nota 5, pp. 193-203.

[18] Por todas: Sentencia del Tribunal Supremo de 16 de junio de 2014 de la sala de lo penal, recurso 2229/2013, que considera ilícita la obtención del medio de prueba que en el orden social se había entendido apto para un despido procedente, y que se pretendía que justificara también un delito de estafa.

[19] Rodríguez Escanciano, Susana, "El poder de control empresarial en un contexto productivo tecnológicamente avanzado", en: López Balaguer, Mercedes (coord.), *Descentralización productiva y transformación del Derecho del Trabajo*, Valencia Tirant lo Blanch, 2018, pp. 217 y ss., en particular pp. 229-247.

planteaba era un acceso a los correos registrados en el ordenador o en el servidor de la empresa, diferenciando en ocasiones entre los elementos externos de la correspondencia electrónica y su contenido.[20] La irrupción en estas cuestiones de la pujante regulación sobre la protección de datos personales y la influencia de la jurisprudencia europea son esenciales para tratar de arrojar luz a la cuestión, y a ello se prestará atención seguidamente.

III. La importancia de la disciplina sobre datos personales

Esta es una dimensión de los controles de acceso a las herramientas de internet que la jurisprudencia laboral tradicionalmente ha relegado a un segundo plano en sus pronunciamientos, cuando no directamente la ha dejado de lado. Sin embargo, no puede negarse que exista y merece también ser analizada.

Y es que, aunque muchas veces los tribunales laborales parezcan no haber recaído en ello, resulta evidente que los datos que se recaban a través de los controles empresariales sobre el acceso a internet tienen la condición de datos personales. Con esa actividad de vigilancia se generan entonces ficheros automatizados de carácter personal que habrá que gestionar de la manera reglamentaria. Así, no es lo mismo visionar en directo la página web que en un determinado momento está viendo en la pantalla un trabajador que grabar toda la información de las páginas a las que se conecta y de la pauta con que lo hace, porque al almacenar y combinar todos esos datos se ofrece un perfil completo del trabajador susceptible de descontextualización (puede por ejemplo contener información ideológica).[21]

Afrontar esta materia desde la particular perspectiva de la protección de los datos de carácter personal fue una construcción propia de la Unión Europea. En efecto, a partir de la Directiva 95/46/CE (del Parlamento europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos), en la Unión Europea se creó un Grupo de Trabajo (el llamado GT29)[22] que venía trabajado en identificar una serie de pautas que deberían respetarse por los empresarios cuando establecen este tipo de control sobre los medios informáticos. Así, deben clarificarse por anticipado las condiciones en las que se autoriza el uso de internet y correo electrónico en el trabajo para fines privados (porque se desaconseja prohibirlo de forma absoluta); la finalidad del control; los sistemas

[20] *Véase,* Sorzano Volart y Núñez-Cortés Contreras, *supra* nota 5, pp. 217 y 218.

[21] Véase, Thibault Aranda, Javier, "La vigilancia del uso de Internet en la empresa y la protección de datos personales", en: *Relaciones laborales: Revista crítica de teoría y práctica*, núm. 1, 2009, págs. 215-226.

[22] Hoy sustituido por el Comité Europeo de Protección de Datos como organismo encargado de velar por el cumplimiento de la normativa y asesorar a la Comisión Europea.

y mecanismos instalados (tales como el tamaño máximo de los archivos que se permitirán enviar como adjuntos, o los filtros); el uso que se hará de los datos recabados y las sanciones disciplinarias previstas; si existen, los casos en los que se permitirá el acceso al correo del trabajo por parte de otra persona (por ejemplo en períodos de vacaciones o baja médica del titular), etc.[23]

Si esto es así, la gestión de los datos a que dé lugar un sistema de vigilancia empresarial del acceso de los trabajadores a la red deberá respetar las disposiciones sobre archivo y tratamiento de datos personales que se fijen en la normativa sectorial de protección de datos. Esto venía suponiendo, en pocas palabras, que la información ha de recabarse con transparencia, que debe existir un motivo explícito y legítimo para ello y que la información ha de ser la oportuna. Además, tiene que permitirse un derecho de acceso a esos registros por parte de los interesados, para la rectificación y en su caso supresión de los datos no pertinentes o erróneos.

Todo ello complicaba la puesta en marcha efectiva de este tipo de controles por parte del empleador, porque no sólo era necesaria la adecuada difusión previa de las políticas e instrucciones de usos informáticos permitidos y prohibidos entre los trabajadores, sino que también se precisaba ofrecer un considerable volumen de información *ex post*. El único elemento de cierta flexibilidad era la consideración general de que no era necesaria una prestación del consentimiento previo expreso del trabajador, por darse el tratamiento de datos en el marco de una relación negocial, laboral o administrativa.[24]

En esta tesitura, vio la luz una actualización de la regulación de la protección de datos a nivel de la Unión Europea, con la aprobación del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE. Véase que el instrumento para acometer esta actualización ya no es una Directiva, instrumento que está sujeto a trasposición de los Estados Miembros y con un efecto directo limitado; sino un Reglamento, de automática aplicación llegado el plazo fijado en el mismo. En todo caso, el Reglamento deja cierto margen de libertad a los Estados para adaptar algunas de sus previsiones, y en España la traslación del nuevo derecho a la protección de datos personales en el ámbito laboral se ha producido con la Ley Orgánica 3/2018, ya citada.

Esta norma prevé en su artículo 87 que los trabajadores, y también los empleados públicos, tienen derecho a la protección de su intimidad en el uso de los dispositivos digitales puestos a su disposición por su empleador. El empleador podrá acceder a los contenidos derivados del uso de medios digitales facilitados a los trabajadores

[23] *Véase* González Tapia, María Luisa, "¿Son necesarias las políticas de uso de internet y correo electrónico en las empresas?", en: *Información laboral (jurisprudencia)*, núm. 1, 2008, pp. LN-2 a LN-5.

[24] Arroyo Yanes, *supra* nota 12, pp. 95 y 96.

a los solos efectos de controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la integridad de dichos dispositivos. Los empleadores deberán establecer criterios de utilización de los dispositivos digitales respetando en todo caso los estándares mínimos de protección de su intimidad de acuerdo con los usos sociales y los derechos reconocidos constitucional y legalmente. En su elaboración deberán participar los representantes de los trabajadores. El acceso por el empleador al contenido de dispositivos digitales respecto de los que haya admitido su uso con fines privados requerirá que se especifiquen de modo preciso los usos autorizados y se establezcan garantías para preservar la intimidad de los trabajadores, tales como, en su caso, la determinación de los períodos en que los dispositivos podrán utilizarse para fines privados. También se dispone específicamente que los trabajadores deberán ser informados de los criterios de utilización a los que se refiere ese precepto.

La misma Ley Orgánica reescribe además el Estatuto de los Trabajadores y el Estatuto Básico del Empleado público para reflejar los derechos a la intimidad en relación con el entorno digital y a la desconexión.

IV. La doctrina del Tribunal Europeo de Derechos Humanos (TEDH)

En el caso *Copland contra Reino Unido* (sentencia de 3 abril 2007), el TEDH dio la razón a una trabajadora que se quejaba del seguimiento de sus llamadas telefónicas, correo electrónico y uso de internet, para comprobar si se utilizaba con fines personales, sin que existiese una política previamente anunciada al respecto. El Tribunal considera que la interceptación y almacenamiento de información sobre utilización para uso personal del teléfono, correos electrónicos y navegación por internet en el lugar de trabajo, sin consentimiento del afectado y sin base en la legislación interna o en las normas que regulan el centro de trabajo, implica una injerencia no prevista por la Ley y vulnera el Derecho al respeto de la vida privada garantizado por el Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales (hecho en Roma en 1950).

Este caso resulta especialmente relevante en nuestro análisis porque entre los argumentos esgrimidos ante el Tribunal estaba el de abuso de autoridad en cargo público, supuestamente por parte del superior jerárquico de la demandante. Y es que los hechos habían tenido lugar en un *college* (organismo administrado por el Estado británico). El ámbito público del establecimiento en el que se produjeron los hechos hace merecedor a este pronunciamiento de una especial atención puesto que, como ya hemos anticipado, el grueso de las sentencias judiciales en esta materia se da en cambio en relaciones de trabajo de sede privada.

El TEDH entiende que la recogida y almacenamiento de información personal relativa a las llamadas telefónicas, correo electrónico y navegación por internet de

la demandante, sin su conocimiento, constituye una intromisión que no respeta su vida privada ni su correspondencia, en el sentido del artículo 8 del Convenio. Se le reconoció por ello a la trabajadora una indemnización de 3.000 € en concepto de daño moral por *estrés, ansiedad, desánimo e incapacidad para conciliar el sueño.*

Esta doctrina induce a pensar que tras ella las cautelas de los tribunales hacia los controles sobre el uso de las herramientas informáticas por parte de los trabajadores serían todavía mayores. El TEDH entendió, incluso, que los denominados "archivos temporales", que son copias que se guardan automáticamente en el disco duro de los lugares visitados a través de internet, también entran dentro de la protección de la intimidad; ello a pesar de que estos archivos son más bien rastros o huellas de la navegación en internet que informaciones personales de carácter reservado.

Sin embargo, tampoco en el marco del Consejo de Europa la posición ha sido siempre unánime. Antes bien lo contrario, pues casos como *Barbulescu contra Rumanía* evidencian la ausencia de un criterio único y la fuerza expansiva de los votos particulares. En efecto, en tan sólo un año, el Tribunal dictó dos sentencias con argumentación contraria, en primera instancia en enero de 2016 y en apelación ante la Gran Sala en septiembre de 2017. La primera sentencia había entendido bastante el comportamiento de la empresa (en este caso privada) para quebrar la expectativa de privacidad del trabajador: una circular general prohibiendo el uso privado del ordenador. Mientras que la segunda corrige la primera haciendo suyo el parecer del voto particular discrepante de uno de los magistrados de la sala juzgadora en la instancia: hubiera sido necesario mayor concreción respecto a los posibles controles. En la primera sentencia el resultado fue de 6 votos a 1, y en la segunda de 11 a 6; los tanteos hablan por sí solos.[25]

Con posterioridad a ese caso, y de nuevo en la esfera de lo público, el TEDH tuvo ocasión de enjuiciar la posible injerencia indebida de la sociedad nacional de ferrocarril francesa (SNCF) en el ejercicio del derecho al respeto de la vida privada y familiar de uno de sus trabajadores, de su domicilio y de su correspondencia, en el caso *Libert contra Francia* (sentencia de 22 de febrero de 2018). En el supuesto, el demandante denunció que tras reincorporarse al puesto de trabajo después de una suspensión de funciones temporal por razones disciplinarias, sus superiores habían incautado su ordenador. Como consecuencia, se abrió contra él nuevo procedimiento disciplinario por haber encontrado en ese equipo documentos que probaban distintas irregularidades, además de un gran número de archivos con imágenes y películas de carácter pornográfico,[26] y fue despedido. El demandante

[25] Es muy abundante la doctrina laboralista que ha comentado estas sentencias, por todos, baste citar aquí el trabajo de Molina Navarrete, Cristóbal, "El Poder empresarial de control digital: ¿'nueva doctrina' del TEDH o mayor rigor aplicativo de la precedente?: A propósito de la STEDH de 5 de septiembre de 2017, caso Barbulescu c. Rumania", en: *Iuslabor*, núm. 3, 2017.

[26] Se trataba de 1562 archivos de carácter pornográfico representando un volumen de 787 Mb

instó ante la jurisdicción nacional la nulidad de este despido, argumentando que la SNCF había vulnerado su privacidad abriendo, durante su ausencia, elementos identificados como personales en su ordenador, pues los archivos estaban ubicados en un disco duro denominado "D:/ datos personales", dentro de una carpeta titulada "risas". Durante el proceso, la SNCF explicó sin ser contradicha, que la unidad "D" se denomina por defecto "D:/ datos" y se utiliza tradicionalmente por los agentes para almacenar sus documentos de trabajo, y recordó que el manual del usuario establece que "las informaciones de carácter privado deben estar claramente identificadas como tales (opción "privado" en los criterios de *outlook*)" y que es lo mismo en los "soportes receptores de información (repertorio "privado")". Los tribunales laborales franceses, considerando que un empleado no puede utilizar la totalidad de un disco duro, pensada supuestamente para grabar datos de trabajo, para un uso privado, estimaron que la SNCF tenía derecho a considerar que la designación "datos personales" en el disco duro no podría prohibir el acceso a este elemento. También argumentaron que el término genérico de "datos personales"[27] podría relacionarse con asuntos que son gestionados personalmente por el trabajador y por lo tanto no referirse explícitamente a los elementos relativos a su vida privada (de hecho, tal fue el caso, el análisis del disco duro reveló muchos documentos de carácter profesional) y que el término "risas" no designa claramente que un elemento así denominado tenga carácter de privado, que esta designación puede hacer referencia a intercambios entre compañeros de trabajo o a documentos profesionales archivados como "tonterías" por el empleado. Entendieron por todo ello que el despido no era desproporcionado, recordando que tanto el código deontológico de la SNCF como los referenciales internos a su disposición recuerdan que los agentes deben utilizar los medios informáticos a su disposición con fines exclusivamente profesionales, estando tolerada únicamente una utilización puntual de carácter privado. Se llegó a afirmar que las actuaciones del demandante eran más graves si cabe debido a su condición de agente público, lo que le obligaba a mantener un comportamiento ejemplar.

Ante el TEDH, el demandante se quejaba de una violación de su derecho al respeto de su vida privada, invocando el artículo 8 del Convenio.[28] El demandante

durante un periodo de cuatro años.

[27] Incidiendo en que "datos personales" no es lo mismo que "datos privados".

[28] Este dispone que toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia (art. 8.1). No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás (art. 8.2).

admitía haber utilizado con fines personales el ordenador puesto a su disposición por su empleador, pero se oponía al hecho de haber personalizado todo su disco duro, manteniendo que únicamente denominó "D:/datos personales" a una parte de éste. Incidía en que su empleador consultó un fichero titulado "risas" cuando el título no admitía, en su opinión, dudas sobre su carácter no profesional. El demandante consideraba por otra parte que la medida no perseguía un objetivo legítimo. En su opinión, no sería pertinente invocar en su causa la necesidad de dar al empleador la posibilidad de controlar el trabajo de sus empleados y de garantizar que respetaban la reglamentación, puesto que la confiscación de su ordenador y la búsqueda de su contenido se realizó cuando él ya llevaba ausente más de un año, y que, por lo tanto, ese ordenador no se utilizaba desde hacía tiempo. Su empleador tampoco podía argumentar la necesidad de prevenir el delito, ya que la posesión de imágenes eróticas, pornográficas o de contenido humorístico no son contrarias a la legislación francesa.

Frente a ello, el Gobierno francés insistía en que los archivos no estaban correctamente identificados como "privados", por lo que no podría hablarse de injerencia. Sostenía además que en ningún caso la misma hubiera provenido de una autoridad pública, por la naturaleza formalmente privada de la sociedad de ferrocarril.

El TEDH no acoge estos últimos argumentos, entendiendo en cambio que sí se produjo una injerencia, y que esta procedía de una autoridad pública,[29] lo que claramente diferencia este caso de *Barbulescu* y lleva analizar la queja, no al amparo de las obligaciones positivas del Estado, sino al amparo de sus obligaciones negativas. Esto supone que tal injerencia incumpliría el artículo 8 excepto si "estando previsto por la ley", perseguía uno o varios de los objetivos legítimos establecidos en el segundo párrafo de esta disposición, y "era necesaria en una sociedad democrática" para alcanzarlos. Y esta clave en la que se decide sobre el fondo del asunto.

El TEDH entiende finalmente que la injerencia tenía una base legal y un objetivo legítimo (proteger los derechos del empleador, como en el caso *Barbulescu*), y que los tribunales nacionales no se habían excedido en su margen de apreciación.

V. La aplicación de estas enseñanzas a los empleados públicos

En principio, en la traslación de la doctrina social al ámbito administrativo, habrá que realizar las adaptaciones pertinentes a los derechos y deberes recogidos en el Estatuto Básico del Empleado Público y, sobre todo, al Código de conducta del artículo 52 de dicho texto. Éste está configurado por una serie de principios éticos y de conducta inspirados en el cumplimiento diligente de las tareas que

[29] En el sentido lato de la propia doctrina acuñada en el caso *Copland*, antes comentado, entre otros.

esos empleados tengan asignadas, de forma objetiva, íntegra, neutral, responsable, imparcial, confidencial, transparente, ejemplar, austera, eficaz, honrada, etc.

Se trata de un particular compromiso con el interés general y el servicio público que tiene un alcance sustancialmente distinto de la buena fe contractual al que está vinculado el trabajador común por cuenta ajena. Hay que puntualizar, además, que la doctrina de la sujeción especial determina y limita las libertades de los funcionarios y, por lo tanto, habrá que tenerla presente a la hora de aplicar a este ámbito la jurisprudencia de las salas de lo social.

Esto podría llevar a pensar en una posible matización de la doctrina del orden social cuando tuviera que aplicarse sobre empleados públicos. Ésta podría reinterpretarse en clave de mayor flexibilidad; no en vano, la relación de sujeción especial de los funcionarios y el Código de conducta de los empleados públicos les vinculan de forma específica a una gestión diligente, honrada y transparente del interés público. Son, como se puso de manifiesto en el caso *Libert* ante el TEDH, "un personal del que se espera un comportamiento ejemplar".

Así las cosas, no sería descabellado sostener que cabe reconocer ciertos efectos a los resultados de controles no preavisados, sobre todo en la medida en que puedan ser útiles a los efectos menores de amonestación doméstica y de diagnóstico de sinergias perniciosas. Sería el caso, por ejemplo, cuando el abuso en la utilización de los medios técnicos concurra con otro tipo de faltas disciplinarias, o cuando lo que se pretenda es advertir sin incoar un expediente sancionador. Aspecto, este último, que en la práctica puede revelarse muy útil. En todo caso, eso sí, los controles deben articularse con cuidado para evitar que puedan contraponerse argumentos basados en la discriminación.[30]

Ahora bien, la relación de sujeción especial no puede justificar *per se* una merma de garantías de fondo y forma en los Derechos fundamentales de los que también son titulares los funcionarios, como cualquier otro ciudadano.[31] Además, la configuración

[30] Así se apunta en la sentencia *Copland* del TEDH (en dicho caso la demandante había hecho especial hincapié en el hecho de que los controles, además de sorpresivos, habían sido realizados únicamente a ella, por motivos personales, dentro de toda la plantilla). El mismo argumento también subyace en la sentencia del Tribunal Supremo español de 26 de septiembre de 2007, ya tratada en la nota 15, allí de hecho había habido incluso una sanción previa de la Inspección de Trabajo a la empresa por acoso laboral. No es de descartar que, a pesar de tratarse de dos asuntos distintos, en la conciencia del juez que ha de valorar la sanción impuesta a un trabajador en base a pruebas obtenidas de una "emboscada" informática, pueda pesar la sospecha de una persecución individual enquistada. El argumento también se intentó en el caso *Libert*, sosteniendo el demandante que fue descubierto porque exista una sospecha *a priori*; sin embargo, su empleador no pudo conocer el contenido de los archivos en causa si no los hubiera abierto, lo que a su juicio evidenciaba que, en realidad, su empleador habría buscado un pretexto para desembarazarse de un cargo demasiado antiguo. En este caso, como ya se ha visto, el TEDH no acogió el razonamiento.

[31] *Véase,* Castillo Blanco, Federico A., *Función pública y poder disciplinario del Estado*, Granada, Civitas, 1992, pp. 87-153. *Véase también,* Lorenzo de Membiela, Juan B., *Régimen disciplinario*

actual de los derechos y deberes del empleado público es muy general, constituyendo más bien el establecimiento de unas líneas de "buena administración", entendida como un derecho más de la ciudadanía,[32] así que difícilmente podrá utilizarse para sustentar una modulación tan notable como la examinada. La reciente introducción en el Estatuto Básico del Empleado Público del "derecho a la intimidad en el uso de dispositivos digitales puestos a su disposición y frente al uso de dispositivos de videovigilancia y geolocalización, 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",[33] genera una previsión en cierto modo tautológica pero que traduce una clara *mens legislatoris* de refuerzo.

Nos movemos aquí, en suma, en un terreno especialmente pantanoso y la transparencia por parte del superior jerárquico responsable de la actividad inspectora es la única opción plenamente segura a seguir. En la situación actual, sólo se podrán hacer valer a efectos disciplinarios los resultados de controles en el uso de los medios técnicos cuando la posibilidad de éstos hubiera sido de general y previo conocimiento. Lo contrario vulneraría la dignidad del empleado público, quien podría alegar una preconcebida legítima confianza en la confidencialidad de su uso en internet merecedora de tutela por los tribunales, salvo prueba y admisión de un comportamiento abusivo.

Así lo ha reconocido, por ejemplo, el Tribunal Superior de Justicia de Aragón en sentencia de 4 de diciembre de 2007, en un caso en el que el Técnico Auxiliar Deportivo de un Ayuntamiento había sido despedido tras haber constatado la utilización de un puesto informático a su servicio para la descarga de numeroso material pornográfico, habiendo ocupado incluso la totalidad de la banda ancha disponible y dificultando la utilización de la infraestructura por parte del resto de usuarios del establecimiento público. Ante lo palmario de los hechos, el Juzgado de lo Social declaró en primera instancia la validez de la sanción disciplinaria impuesta por Resolución de la Alcaldía; en apelación, el Tribunal Superior, sin embargo, dado que no existía prohibición expresa del Ayuntamiento respecto a la utilización por parte de sus empleados de internet para usos personales, ordena la readmisión del trabajador. No cabe sino resaltar la diferencia de base en los presupuestos fácticos con respecto al caso *Libert*, donde como se ha comentado sí existían reglas respecto al uso privado y a la identificación de los archivos de uso personal en el ordenador del trabajo.

---

de los funcionarios de carrera, Cizur Menor, Thomson-Aranzadi, 2ª ed., 2008, pp. 35 y 36.

[32] *Vid.* Castillo Blanco, Federico A., "Los deberes de los funcionarios públicos" en VV.AA., *Comentarios a la Ley del Estatuto Básico del Empleado Público*, Valladolid, Lex Nova, 2007, pp. 362 y 363.

[33] Artículo 14.j.bis introducido por la disposición final decimocuarta de la Ley Orgánica 3/2018. La previsión es idéntica a la introducida en el Estatuto de los Trabajadores respecto a la intimidad en relación con el entorno digital y a la desconexión.

VI. Conclusiones

En el contexto laboral, a día de hoy, no existe una respuesta única y excluyente que nos permita conocer el alcance disciplinario exacto de un uso indebido de internet y del correo electrónico en el trabajo. Es por ello que muchas empresas han incluido, en sus convenios, códigos de conducta acerca del uso de internet en horas de trabajo. De tal manera que los empleados conocen desde el principio sus obligaciones y límites en cuanto al uso de los medios que la empresa pone a su disposición para llevar a cabo sus funciones. En aquellos casos en los que existe una normativa interna que regule el uso de internet (como también puede establecerse para el caso del teléfono y demás medios técnicos afectados a la actividad laboral), ésta debe ponerse en conocimiento de los trabajadores, para que la acepten y acaten. De esta forma, si el empresario conoce del quebrantamiento de dicha normativa por un trabajador podrá avisarle amonestándole y abriéndole un expediente disciplinario. Pero si algo enseñan las sentencias *Barbulescu* del TEDH es que *the devil is in the details*: en la extensión, los medios admisibles y los requisitos formales de tal información previa.

Aun con esa incertidumbre, esta misma es la solución más segura en el ámbito público: información previa sobre la posibilidad de realizar inspecciones. La decisión de no advertir de la celebración de este tipo de controles siempre contaría con la amenaza de ser declarada contraria a la dignidad personal de los empleados públicos. Existen pronunciamientos jurisprudenciales que lo corroboran, y que aquí se han expuesto en relación con personal laboral.[34]

Para garantizar la eficiencia administrativa por parte de los gestores resulta procedente establecer, por anticipado, filtros que veten el acceso a determinadas páginas web, o aprobar unas directrices que detallen el uso permitido de las herramientas informáticas, correo electrónico, internet y navegación "no corporativa". Si los empleados aceptan esta información, significa que están enterados de las normas y del uso de las herramientas telemáticas. Por tanto, si se constatan después incumplimientos no habría ningún obstáculo para llegar hasta las últimas consecuencias disciplinarias, siempre con medidas proporcionales al daño causado, como ha señalado de nuevo el TEDH en el caso *Libert*.

Además, la gestión de los registros con la información extraída de la referida actividad de control habrá de ser gestionada con todas las cautelas que exige la normativa de protección de datos de carácter personal.

---

[34] Un estudio específico sobre el personal funcionario, que requiere un análisis pormenorizado de la jurisprudencia contencioso-administrativa, en Boto Álvarez, Alejandra, "Control a través de las TIC en el sector público y expectativa razonable de privacidad: la visión del contencioso-administrativo", *Revista General de Derecho del Trabajo y la Seguridad Social*, núm. 54, 2019, pp. 374-389.

VII. Bibliografía

Arroyo Yanes, Luis Miguel, "La digitalización de las Administraciones públicas y su impacto sobre el régimen jurídico de los empleados públicos", en: *Revista vasca de gestión de personas y organizaciones públicas*, núm. 15, 2018, pp. 82 y ss.

Boto Álvarez, Alejandra, "Control a través de las TIC en el sector público y expectativa razonable de privacidad: la visión del contencioso-administrativo", *Revista General de Derecho del Trabajo y la Seguridad Social*, núm. 54, 2019, pp. 374-389.

Castillo Blanco, Federico A., *Función pública y poder disciplinario del Estado*, Granada, Civitas, 1992.

González Tapia, María Luisa, "¿Son necesarias las políticas de uso de internet y correo electrónico en las empresas?", en: *Información laboral (jurisprudencia)*, núm. 1, 2008, pp. 2 y ss.

Herrán, Ana I., Emaldi Cirión, Aitziber y Enciso, Marta (coord.), *Derecho y Nuevas Tecnologías*, Bilbao, Universidad de Deusto, 2011.

Jiménez-Castellanos Ballesteros, Inmaculada, "Videovigilancia laboral y derecho fundamental a la protección de datos", en: *Temas laborales: Revista andaluza de trabajo y bienestar social*, núm. 136, 2017, pp. 129 y ss.

Lorenzo de Membiela, Juan B., *Régimen disciplinario de los funcionarios de carrera*, Cizur Menor, Thomson-Aranzadi, 2ª ed., 2008.

López Balaguer, Mercedes (coord.), *Descentralización productiva y transformación del Derecho del Trabajo*, Valencia Tirant lo Blanch, 2018.

Luque Parra, Manuel (coord.), *Relaciones laborales y nuevas tecnologías*, Madrid, La Ley, 2005.

Manteca Velarde, Víctor, "Control del empresario sobre el uso del ordenador por los trabajadores: alcance, contenido y límites", en: *Actualidad jurídica Aranzadi*, núm. 749, 2008.

Marín Alonso, Inmaculada, *El poder de control empresarial sobre el uso del correo electrónico en la empresa. Su limitación en base al secreto de las comunicaciones*, Valencia, Tirant lo Blanch, 2005.

Molina Navarrete, Cristóbal, "El Poder empresarial de control digital: '¿nueva doctrina del TEDH' o mayor rigor aplicativo de la precedente?: A propósito de la STEDH de 5 de septiembre de 2017, caso Barbulescu c. Rumania", en: *Iuslabor*, núm. 3, 2017, disponible en: https://www.upf.edu/documents/3885005/140470042/9.Molina.pdf/7505da89-5f23-f749-da5b-f3f7988ae417.

Montoya Melgar, Alfredo, "Nuevas tecnologías y buena fe contractual (buenos y malos usos del ordenador en la empresa)", en: *Relaciones laborales*, núm. 1, 2009, pp. 31 y ss.

Murillo de la Cueva, Pablo Lucas y Piñar Mañas, José Luis, *El Derecho a la autodeterminación informativa*, Madrid, Fundación Coloquio Jurídico Europeo, 2009.

Nores Torres, Luis Enrique, "La competencia para resolver los conflictos del personal laboral al servicio de las AA.PP., en particular, los relacionados con las bolsas de trabajo", *Elderecho.com* (tribuna), 1 de junio de 2014, disponible en: https://elderecho.com/la-competencia-para-resolver-los-conflictos-del-personal-laboral-al-servicio-de-las-aa-pp-en-particular-los-relacionados-con-las-bolsas-de-trabajo.

Rodríguez Escanciano, Susana, *Derechos laborales digitales: garantías e interrogantes*, Valencia, Tirant lo Blanch, 2019.

Rodríguez Lainz, José Luis, "El principio de expectativa razonable de confidencialidad en la STC 241/2012, de 17 de diciembre", en: *Diario La Ley*, núm. 8122, 2013.

Sánchez Morón, Miguel, *Derecho de la función pública*, Madrid, Tecnos, 11ª ed., 2018.

Talens Visconti, Eduardo Enrique, "La expectativa razonable de confidencialidad como presupuesto de vulneración de derechos fundamentales en la fiscalización informática llevada a cabo por el empresario", en: *Aranzadi Social: Revista Doctrinal*, vol. 6, núm. 8, 2013, pp. 271 y ss.

Thibault Aranda, Javier, "La vigilancia del uso de Internet en la empresa y la protección de datos personales", en: *Relaciones laborales: Revista crítica de teoría y práctica*, núm. 1, 2009, págs. 215 y ss.

Vidal Climent, Vicente y García Manglano, Miguel (coords.)*, Información, libertad y derechos humanos: la enseñanza de la ética y el derecho de la infor-*

mación, Valencia, Fundación COSO, 2004, disponible en: https://eprints.ucm.es/6128/1/definitivo2.pdf.

VV.AA., *Comentarios a la Ley del Estatuto Básico del Empleado Público*, Valladolid, Lex Nova, 2007.