



El control empresarial del uso de las redes sociales en el lugar de trabajo: alcance y confines*

por Roberto Fernández Fernández y Cristina González Vidales

1.- Contexto general

Las opciones vinculadas a la utilización de nuevas herramientas tecnológicas constituyen un avance significativo en las sociedades actuales y permiten unas posibilidades de intercambio hasta ahora desconocidas. De esta manera, las formas de comunicación se han incrementado de manera exponencial como consecuencia de tener al alcance de manera inmediata tanto dispositivos como instrumentos capaces de permitir interactuar con otras personas de manera instantánea y sencilla.

Diversas y heterogéneas pueden ser las nociones que se pueden utilizar a fin de conceptualizar esta nueva realidad, si bien una de las más habituales entre la doctrina especializada al respecto es aquella que define a los “servicios de redes sociales on-line [como] servicios web que permiten a los individuos (1) construir un perfil público o semipúblico partiendo de un modelo de formulario determinado (2) articular una lista de usuarios con los que se va a compartir conexión y (3) visualizar y navegar a través de esa lista de conexiones y de otras establecidas por otros usuarios del sistema”¹.

A partir de la definición precedente es posible extraer los tres elementos fundamentales vinculados a la misma, a saber: “permite al usuario presentar y construir su identidad virtual; relacionarse con otros afines en algún aspecto; y reproducir, consolidar y/o extender su red social off-line creando una comunidad virtual”².

Sobre las premisas anteriores, es posible hablar de una sustancial transformación de las formas de interrelación entre los ciudadanos, lo que ha traído aparejada cuanto se ha venido en denominar “revolución digital”³, y que, conforme ha señalado con gran acierto algún autor, nos lleva hacia una “sociedad hiperconectada” capaz de relevarse en tres grandes manifestaciones: una sociedad “hiperinformada”, hipercomunicada” e “hipervisualizada”⁴.

* Estudio realizado en el marco del Proyecto de Investigación DER2017-82192-C3-1-R “Nuevos lugares, distintos tiempos y modos diversos de trabajar: innovación tecnológica y cambios en el ordenamiento social”, financiado por el Ministerio de Ciencia, Innovación y Universidades.

¹ BOYD, D.M. y ELLISON, N.B.: “Social Network Sites: Definition, History, and Scholarship”, *Journal of Computer-Mediated Communication*, núm. 13, 2008, pág. 211.

² SOLER PRESAS, A.: “Am I in Facebook?”, *InDret*, núm. 3, 2011, pág. 4.

³ “En esencia es un nuevo marco tecnológico al servicio de las relaciones sociales en su sentido más amplio, está suponiendo un nuevo paradigma que trasciende de manera general al entorno social y por ende al jurídico, de modo que su significación va más allá de su incidencia concreta en una u otra institución”, ALONSO UREBA, A.: “Revolución Digital, Derecho y Empresa”, *Base de Datos del Diario La Ley*, 2019, pág. 1.

⁴ “Hiperinformada, en el sentido de que a través de Internet es posible acceder de forma inmediata a una información tendencialmente total y global. Determinados buscadores como Google o Bing son buenos ejemplos de acceso continuo a todo tipo de información y ello no sólo respecto a la información actual, sino también en relación con información pasada. En segundo lugar, que estamos ante una sociedad hipercomunicada, en tanto que a través de determinadas redes

De esta manera, y a diferencia de lo que ocurría con las conversaciones privadas o de bar, la sociedad termina por enfrentarse “a un exceso de información y sus sujetos son incapaces de racionalizar las noticias como es debido y separar convenientemente lo verdadero de lo falso, donde los hechos y las noticias se quedan obsoletas de manera fugaz, donde las corrientes de opinión se generan a golpe de tweet o comentarios en cualquiera de las redes sociales sin dedicar el tiempo suficiente para pensar lo que se dice, donde a golpe de un click puedes conectar al mismo tiempo personas que se encuentran distanciadas a miles de kilómetros, donde tus actuaciones dejan de tener repercusión en un entorno cercano, limitado y controlado para poder ser vistas en cualquier lugar y momento potencialmente por un gran número de personas, más aún si se convierten en acontecimientos virales o, por no seguir, donde la tiranía de la imagen está arrinconando definitivamente el valor de la palabra, otorgando más valor a un golpe de efecto visual y a los eslóganes sencillos y directos en lugar de buscar la profundidad de los argumentos alcanzados tras intensas jornadas de estudio”⁵.

La generalización de redes sociales como twitter, whatsapp, facebook, snapchat, linkedin, instagram, xing, telegram, etcétera⁶, ha traído consigo importantes beneficios pero también retos desde el punto de vista jurídico, tendentes a ordenar las posibles conductas que pueden ser realizadas a través de las mismas.

En este sentido, ya se están comenzado a estudiar determinados comportamientos vinculados al uso de estas redes sociales y que pueden traer aparejadas alteraciones de la salud de quienes las utilizan o sufren sus consecuencias⁷:

-- Adicciones a las redes sociales, de manera que el sujeto no puede dejar de estar continuamente pendiente de ellas, llegando a obsesionarse con las mismas.

-- Ciberacoso a través de las redes sociales.

-- Comisión de delitos a través de las mismas (no solamente económicos, sino también vinculados al derecho al honor, a la intimidad...).

Su masiva, creciente exponencialmente e imparable expansión⁸ permite afirmar sin ambages que la utilización de las herramientas anteriormente descritas, llega, en numerosas ocasiones, a trascender el ámbito privado del usuario, afectando también, al marco de las relaciones laborales⁹.

sociales, es posible no ya buscar información, sino establecer una relación multilateral con múltiples e infinitos sujetos con los objetivos más diversos. Facebook, Twitter, WhatsApp o, con carácter más profesional, LinkedIn, pueden ser ejemplos muy representativos al respecto. Y, en tercer lugar, que vivimos en una sociedad hipervisualizada, puesto que a través de determinados programas, aplicaciones y redes, podemos compartir todo tipo de imágenes y representaciones gráficas, y muy principalmente videos y fotografías (destacan, al respecto, plataformas como Youtube e Instagram). Estas tres manifestaciones se retroalimentan, potenciándose mutuamente”, DEL REY GUANTER, S.: *La empresa hiperconectada y el futuro del trabajo. Conclusiones y recomendaciones del informe “El impacto de la empresa hiperconectada y de las redes sociales en la organización del trabajo, en la gestión de los recursos humanos y en las relaciones laborales*, Madrid (Cuatrecasas. Instituto de Estrategia Legal en RRHH), 2017, pág. 2.

⁵ FERNÁNDEZ FERNÁNDEZ, R.: “Deslocalización productiva y condiciones mínimas de trabajo a nivel mundial en los Acuerdos Marco Internacionales”, *Documentación Laboral*, núm. 118, 2019, pág. 47.

⁶ Algunos de los sitios descritos son predominantemente privados y otros motivados por cuestiones laborales, sin embargo, las funciones de las redes sociales en unos y otros tienen a superponerse, pues un trabajador puede dar información sobre cuestiones laborales en sus redes privadas y hablar de sus aficiones en redes de carácter empresarial, GÖPFERT, B. y WILKE, E.: “Facebook and Employment Law in Germany: Regulating the use of social media through a policy on social networking sites”, *Employment & Industrial Relations Law*, Vol. 21, núm. 2, 2011, pág. 8.

⁷ Un estudio exhaustivo sobre el acoso cibernético laboral y su consideración como riesgo psicosocial emergente en la nueva sociedad digital, por todos, MOLINA NAVARRETE, C.: “Redes sociales digitales y gestión de riesgos profesionales: prevenir el ciberacoso sexual en el trabajo, entre la obligación y el desafío”, *Diario La Ley*, núm. 9452, 2019, págs. 1-19.

⁸ “Se estima que, durante un único día, se envían 500 millones de tweets, 295 mil millones de correos electrónicos, 65 millones de mensajes de WhatsApp, se hacen 5 mil millones de búsquedas en Internet y se crean 4 petabytes de información en Facebook [...] Las estimaciones para el año 2025 indican la creación de 645 exabytes de datos en un solo día”, PALORMO ZURDO, F.J. y REY PAREDES, V.: “Retos e incertidumbres del proceso de transformación digital de la economía y de la sociedad”, *Derecho Digital e Innovación*, núm. 3, 2019, pág. 10.

En efecto, y como no podría ser de otra manera en atención a la dedicación que cualquier persona realiza a su vida profesional¹⁰, “el cambio en las pautas de comportamiento social como consecuencia del uso generalizado de las redes sociales ha acabado incidiendo en el ámbito personal y laboral de la vida de las personas y, por consiguiente, en el funcionamiento de las empresas. Más concretamente, la implantación y desarrollo de las redes sociales tiene un efecto progresivo de cambios sustanciales en la organización del trabajo y en la gestión de recursos humanos que a su vez, tienen una repercusión directa e indirecta en las principales instituciones jurídicas que regulan las relaciones del trabajo”¹¹.

En consecuencia, el Derecho del Trabajo también tiene que afrontar retos importantes en relación con la utilización en el lugar de trabajo de las redes sociales y que abarcan desde los estadios previos a la contratación, se mantienen durante el desarrollo de la relación laboral e incluso pueden tener consecuencias en la finalización del contrato de trabajo.

En esta materia, la regulación legal, al menos en España, va por detrás de la realidad tecnológica que nos rodea¹², debiendo utilizar instituciones clásicas para resolver un problema moderno, aplicando unas reglas no acompañadas a su tiempo, convirtiendo su uso en un “campo de minas”¹³ para la legislación laboral. Es verdad que la falta de regulación descrita se ha intentado paliar con la promulgación a nivel comunitario del Reglamento UE 2016/679, del Parlamento y del Consejo, de 27 de abril de 2016 (RPD), y su recepción a nivel interno por parte de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD), pero que no vienen sino a constituir un parche, al no afrontar de manera global y transversal el problema, poniendo únicamente remedio a determinadas cuestiones consideradas más trascendentes por el legislador.

De esta manera, es necesario resaltar que los pasos emprendidos resultan dignos de elogio, pero (compartiendo la opinión de una de las mayores expertas sobre estos temas en la doctrina científica española) quedan todavía muchos tópicos fuera de ambas regulaciones, habida cuenta de que “la promulgación de una norma específica en materia de protección de datos aplicable a los centros de trabajo, aunque supone un avance, no resuelve, por tanto, todos los problemas suscitados en el ámbito laboral, dadas las situaciones heterogéneas y cambiantes en los diversos sectores productivos y, sobre todo, la constante innovación tecnológica y sus efectos en el seno de la empresa”¹⁴.

Por esta razón, se comparte la opinión de una de las maestras del iuslaboralismo español que considera como imprescindible la actuación legislativa para “cumplir la obligación positiva del Estado en relación con el artículo 8 del CEDH en los términos o con las indicaciones señaladas por la Sentencia *Barbulescu II*, y para proporcionar seguridad jurídica”, incorporando al Estatuto de los

⁹ DE CASTRO MEJUTO, L.F.: “Capítulo XIV. Las nuevas maneras de trabajar y las redes sociales”, en AA.VV. (MELLA MÉNDEZ, L. y NÚÑEZ-CORTÉS CONTRERAS, P., Dirs.): *Nuevas tecnologías y nuevas maneras de trabajar: Estudios desde el Derecho Español y Comparado (Alemania, Reino Unido, Polonia, Portugal y Argentina)*, Madrid (Dykinson), 2016, págs. 302-303.

¹⁰ “Cabe señalar en este punto, que es en el marco de la vida laboral donde la mayoría de la gente tiene muchas, si no la mayoría, de las oportunidades para fortalecer sus lazos con el mundo exterior”, STEDH de 16 de diciembre de 1992, asunto *Niemietz*.

¹¹ DEL REY GUANTER, S.: *La empresa hiperconectada y el futuro del trabajo. Conclusiones y recomendaciones del informe...*, cit., 2017, págs. 2-3.

¹² “La legislación sobre el mundo digital va a remolque no ya sólo de la realidad, sino también de la jurisprudencia. Uno de los retos más complejos planteados por esta nueva era es acompañar el ritmo del Derecho, habitualmente lento, y el del cambio tecnológico, usualmente vertiginoso, a fin de evitar que una norma nazca ya envejecida”, MOLINA NAVARRETE, C.: “El derecho a la vida privada del trabajador en el Tribunal Europeo de Derechos Humanos: ¿Diálogo o conflicto con la jurisprudencia nacional?”, *Temas Laborales*, núm. 145, 2018, pág. 155.

¹³ GÖPFERT, B. y WILKE, E.: “Facebook and Employment Law in Germany: Regulating the use of social media through a policy on social networking sites”, cit., pág. 10.

¹⁴ RODRÍGUEZ ESCANCIANO, S.: *Derechos laborales digitales: garantías e interrogantes*, Cizur Menor (Thomson Reuters – Aranzadi), 2019, pág. 31.

Trabajadores “un nuevo título para regular los derechos fundamentales de los trabajadores en las relaciones laborales, despejando las incertidumbres del ejercicio de dichos derechos fundamentales en igualdad y sin discriminaciones y en relación con las tecnologías de la información y la comunicación, con el entorno tecnológico digital que es una realidad insoslayable, virtualmente ausente del ET”¹⁵.

2.- El control de las redes durante el desarrollo de la relación laboral

No es posible negar la evidencia, las redes sociales si son utilizadas adecuadamente pueden proporcionar múltiples beneficios para las empresas, quienes pueden aprovecharse de las sinergias positivas que su utilización presenta en el desarrollo de los procesos productivos, aumentando su competitividad y con ello su cuenta de resultados.

Pero como casi cualquier actividad humana, su utilización por parte de los empleados durante la jornada laboral puede tener consecuencias negativas para la unidad productiva cuando aquel realiza un uso indebido y abusivo de las mismas, por un lado, poniendo en riesgo la seguridad informática de la empresa y, por otro, afectando a su productividad y rendimiento profesional.

Sin olvidar tampoco como casi todas las semanas es posible encontrar historias nuevas de negocios que ven dañada su reputación como resultado de un tweet viral o una publicación en Facebook de uno de sus empleados, o deben afrontar responsabilidades legales por sus propios intentos de monitorear el uso que hacen sus empleados de las redes sociales o la utilización que las compañías mismas hacen de estas herramientas para examinar a los solicitantes de un empleo¹⁶.

Sobre las premisas anteriores, a nadie puede extrañar que el empleador quiera establecer o mantener cierta clase de controles sobre este asunto; “la experiencia demuestra, empero, cómo el poder tecnológico del empresario pone en peligro y moviliza numerosas libertades públicas, tales como el derecho a la intimidad, el secreto de las comunicaciones, el derecho a la propia imagen o la libertad informática. Y ese poder puede ser adicionalmente utilizado, de manera directa o indirecta, con fines discriminatorios”¹⁷. *Item* más, “los avances tecnológicos son constantes y cada día más sofisticados, de suerte que pueden llegar a incidir en mayor medida en la vida privada de las personas, esfera que no pierde su carácter por el hecho de que la actuación se enmarque en el ámbito de una relación de trabajo por cuenta ajena”¹⁸.

Por las razones expuestas, es menester buscar el necesario equilibrio a fin de cohonestar las legítimas expectativas empresariales de tener cierto control sobre cuantas actuaciones realizan sus trabajadores durante la jornada de trabajo aprovechando las extensas oportunidades que les brinda las nuevas tecnologías y el respeto a prerrogativas tan básicas para los trabajadores en cuanto ciudadanos de un Estado Social y Democrático como son los derechos fundamentales.

A este respecto, una primera cuestión que debe ser planteada es hasta donde llega el poder de dirección de las empresas ordenado en el artículo 20 ET¹⁹ para acceder o solicitar las claves de acceso a las redes sociales de sus trabajadores.

Para quienes suscriben estas líneas, y en el caso de la legislación española, si el hardware y el software son privados, el empresario no puede solicitar las claves privadas del trabajador, ni controlar los mensajes utilizados, a no ser que haya una autorización judicial que permita el acceso a los mismos a fin de controlar un incumplimiento laboral; en efecto, si los tribunales han anulado

¹⁵ CASAS BAAMONDE, M^a.E.: “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*, núm. 2, 2018, págs. 118-119.

¹⁶ ORNSTEIN, D.: “Social media usage in the workplace around the world. Developing law and practices”, *Business Law International*, Vol. 13, núm. 2, 2012, pág. 195.

¹⁷ RODRÍGUEZ ESCANCIANO, S.: *Derechos laborales digitales: garantías e interrogantes*, cit., pág. 17.

¹⁸ STSJ Madrid 21 marzo 2014 (Sta. 260/2014).

¹⁹ “Esta facultad de control prevista en la ley legitima el control empresarial del cumplimiento por los trabajadores de sus tareas profesionales”, STCo 170/2013, de 7 de octubre.

cláusulas genéricas en las cuáles se obligaba al trabajador a facilitar a la empresa, con fines profesionales, el “teléfono, incluso móvil, domicilio, correo electrónico y a comunicar los cambios de estos datos, permitiendo el envío de mensajes por esas vías que estuviesen relacionados con el trabajo”²⁰, mucho menos se va a permitir obtener las contraseñas de protección o acceder a estas redes.

En cambio, si el hardware y el software son de la empresa, el titular del capital podrá establecer dispositivos de control y acceder, no al contenido privado de la red social, pero sí al uso que de la misma se ha hecho, cumpliendo para ello con los condicionantes legales y jurisprudenciales exigidos, habida cuenta de que “si bien el trabajador tiene derecho al respeto de su intimidad, no puede imponer ese respeto de modo absoluto cuando utiliza un medio proporcionado por la Compañía en contra de las instrucciones establecidas por esta para su uso”²¹.

2.1. Los criterios jurisprudenciales: el catalizador de la reforma legal

A dar seguridad en el debate no han contribuido en demasía algunas resoluciones judiciales ampliamente conocidas y comentadas en el ámbito de la doctrina científica y judicial, ni una jurisprudencia interna que parece no ir en la línea marcada por instancias supranacionales.

Cabe dar cuenta aquí, como ejemplo señero, de los conocidos casos *Barbulescu I* y *Barbulescu II* y *López Ribalda I* y *II*, pues en apenas un año y medio la Gran Sala viene a enmendar la plana a una de las Secciones del Tribunal y ofrece una interpretación diferente sobre la utilización por el trabajador de una herramienta informática puesta a su disposición por el empleador.

Respecto a la primera de ellas, encuentra su origen en el despido de un trabajador que había abierto, porque así se lo había solicitado su empresario, una cuenta de Yahoo Messenger con el fin de responder a las peticiones que le pudieran hacer los clientes, de manera tal que tenía un uso profesional. Sin embargo, según señalaba la empresa, el trabajador habría utilizado semejante herramienta para un uso personal lo que contradecía la normativa interna de la compañía en relación con los recursos tecnológicos facilitados por la misma. En julio de 2007, la empleadora había informado al trabajador que sus comunicaciones de Yahoo Messenger habían sido monitoreadas entre el 5 y el 13 de julio de 2007 y que se había descubierto una contravención de la norma interna. El trabajador declaró por escrito que la herramienta de comunicación solamente había sido utilizada para fines profesionales, a lo cual la empresa le mostró una transcripción de 45 páginas en las cuales había intercambiado mensajes con su novia y su hermano teniendo por contenido aspectos de la vida personal del empleado.

En este caso, el tribunal consideró que el trabajador, al usar para fines personales, en contra de la política de la empresa y afirmar por escrito que había utilizado la cuenta únicamente para asesorar a clientes, había cometido una infracción disciplinaria y “por lo tanto, se puede deducir que el empleador actuó de conformidad con sus competencias disciplinarias puesto que, tal y como constataron los tribunales nacionales, accedió a la cuenta de Yahoo Messenger basándose en el supuesto de que la información allí contenida estaba relacionada con actividades profesionales y que, por ende, acceder a ella era legítimo [de manera que] es razonable que un empleador quiera comprobar que sus empleados estén llevando a cabo tareas profesionales durante horarios laborales”²².

Sin embargo, año y medio más tarde, el mismo Tribunal en Gran Sala señala que no basta con tener la creencia o constatar la existencia de un incumplimiento laboral del trabajador y la advertencia realizada a través de la normativa de régimen interno sobre la prohibición de utilizar para fines personales los recursos electrónicos puestos a disposición por la empresa, sino que es necesario una actuación más garantista del derecho a la intimidad del trabajador, a situar en una información

²⁰ STS 10 abril 2019 (Sta. 304/2019).

²¹ STSJ Madrid 10 abril 2015 (Sta. 309/2015).

²² STEDH de 12 de enero de 2016, *Barbulescu I*.

previa a este en torno a que su conducta va a ser objeto de supervisión. De esta manera, para romper la expectativa razonable de privacidad (“las instrucciones de una empresa no pueden anular el ejercicio de la privacidad social en el puesto de trabajo [...] aunque pueden limitarse dentro de las medidas de necesidad”) que el trabajador tiene deben concurrir los siguientes factores²³: una advertencia clara en cuanto a la naturaleza de la vigilancia y en todo caso previa a su establecimiento; justificar el grado de intrusión en la vida privada del trabajador, tomando en consideración si la supervisión se ha realizado sobre la totalidad o sobre aspectos parciales de las comunicaciones, si ha sido limitada o no en el tiempo y el número de personas que han accedido a ellas; explicar con argumentos más fundamentados el método de control, pues la vigilancia de las comunicaciones es *per se* una actividad más invasiva; evaluar, atendiendo a las condiciones específicas de cada caso, si el empresario tiene a su alcance algún medio más idóneo y menos invasivo que el acceso directo a las comunicaciones; en fin, si se ofrecieron garantías adecuadas tendientes a impedir que el empresario tuviera acceso al contenido de las comunicaciones sin que el empleado hubiera sido previamente notificado de tal ejercicio basado en el poder de dirección.

En el segundo de los casos, la empresa, ante las sospechas de robos por irregularidades en los niveles de stocks y las cifras de ventas en el supermercado, decidió instalar una serie de cámaras de vigilancia, tanto visibles como ocultas, con el fin de supervisar la actividad de los trabajadores en las cajas registradoras, si bien informó a estos de las visibles pero de las cámaras ocultas no se informó a ningún trabajador, así como también se instaló una señal de advertencia indicando la existencia de una cámara de vigilancia. Como consecuencia de las grabaciones obtenidas, catorce empleados fueron despedidos por haber robado productos o haber cooperado a que otras personas se llevarán bienes sin abonarlos.

En su primera sentencia, la Sala aplica las conclusiones alcanzadas por la sentencia *Barbulescu II* y considera que la actuación de la empresa ha vulnerado el derecho a la privacidad de los trabajadores, habida cuenta de que “si bien la videovigilancia se había aplicado debido a sospechas legítimas de robo, su alcance era amplio --puesto que no estaba limitado en el tiempo, se dirigía a todos los empleados que trabajaban en las cajas y cubría todas las horas de trabajo-- e incumplía la obligación de la legislación nacional de informar previamente a los afectados por la recogida y tratamiento de sus datos personales de la existencia, finalidad y modalidades de estas medidas”²⁴.

Argumentación que vuelve a reforzar de nuevo la Gran Sala señalando que “si bien tanto la legislación española como las normas internacionales y europeas pertinentes no parecen requerir el consentimiento previo de las personas [...] cuyos datos se han recogido, estas normas establecen que, en principio, es necesario informar a estas personas con claridad y con carácter previo de la existencia y modalidades de dicha recogida, aunque sólo sea de manera general. Considera que la exigencia de transparencia y el derecho a la información que resulta de ello son fundamentales, especialmente en el contexto de las relaciones laborales, donde el empleador tiene poderes importantes sobre los trabajadores y cuyo abuso debe evitarse”²⁵.

²³ Siguiendo los argumentos jurídicos de la STEDH de 5 de septiembre de 2017, asunto *Barbulescu II*.

²⁴ STEDH de 9 de enero de 2018, asunto *López Ribalda I*.

“No está de más recordar, en cualquier caso, que siguen existiendo unos derechos constitucionales y legales en el marco de la relación de trabajo que deben ser efectivamente protegidos, y uno de ellos es el de la privacidad, y mucho más en la sociedad tecnológica del siglo XXI, cuestión que no tiene nada que ver con la sanción que pueda producirse de conductas contrarias a derecho y siempre y cuando los medios utilizados para tener conocimiento del incumplimiento contractual sean lo menos invasivos posibles de la privacidad del trabajador”, ROJO TORRECILLA, E.: “Derecho del trabajador a la privacidad en la empresa y límites a su control por cámaras de vigilancia. Estudio del caso López Ribalda y otras contra España (a propósito de la sentencia del Tribunal Europeo de Derechos Humanos de 9 de enero de 2018)”, *Derecho de las Relaciones Laborales*, núm. 2, 2018, pág. 151.

²⁵ STEDH de 17 de octubre de 2019, asunto *López Ribalda II*.

A pesar de cuanto pudiera derivarse de una lectura apresurada de la sentencia, “no se alteran las líneas generales de la jurisprudencia del TEDH sobre la protección y aplicación del art. 8 del CEDH, aun cuando ciertamente se amplía la posibilidad de la adopción de medidas por parte empresarial para poder controlar, en determinadas circunstancias, la prestación laboral de una o más personas trabajadoras sobre las que se tenga sospechas fundadas, no meros indicios, de

En el ámbito interno, cabe dar cuenta de una jurisprudencia del Tribunal Constitucional en torno a los límites de la videovigilancia empresarial y al control del correo electrónico. Para el Intérprete Máximo de la Carta Magna la valoración debe realizarse tomando en consideración tres elementos de manera consecutiva: el juicio de idoneidad, esto es, el control empresarial deberá adaptarse al objetivo propuesto; posteriormente se traslada al ámbito del juicio de necesidad, examinando si había otra posibilidad de actuación, esto es, otro medio de control menos agresivo que el acceso a las redes sociales; por último, hay que adoptar el juicio de proporcionalidad a través de un análisis de los beneficios y desventajas de la medida de control adoptada²⁶.

Con semejantes criterios como frontispicio, cabe dar cuenta de una sentencia señera del Tribunal Constitucional español, más en la línea de la sentencia *Barbulescu I* que de las posteriores, pues muestra una mayor flexibilidad a la hora de valorar la conducta de vigilancia empresarial y la intromisión en la intimidad del trabajador. Para este fallo, “el empresario no necesita el consentimiento expreso del trabajador para el tratamiento de las imágenes que han sido obtenidas a través de las cámaras instaladas en la empresa con la finalidad de seguridad o control laboral, ya que se trata de una medida dirigida a controlar el cumplimiento de la relación laboral y es conforme con el art. 20.3 TRLET”, de manera que “la exigencia de finalidad legítima en el tratamiento de datos [...] viene dada, en el ámbito de la videovigilancia laboral, por las facultades de control empresarial que reconoce el art. 20.3 TRLET, siempre que esas facultades se ejerzan dentro de su ámbito legal y no lesionen los derechos fundamentales del trabajador. Por ello, como hemos señalado, aunque no se requiere el consentimiento expreso de los trabajadores para adoptar esta medida de vigilancia que implica el tratamiento de datos, persiste el deber de información [...], sin perjuicio de que serán las circunstancias de cada caso las que finalmente determinen si dicha fiscalización llevada a cabo por la empresa ha generado o no la vulneración del derecho fundamental en juego [...] En consecuencia, teniendo la trabajadora información previa de la instalación de las cámaras de videovigilancia a través del correspondiente distintivo informativo, y habiendo sido tratadas las imágenes captadas para el control de la relación laboral, no puede entenderse vulnerado el art. 18.4 CE”²⁷.

A este respecto, cabría considerar que esta línea del Tribunal Constitucional no parece muy acorde con la argumentación más garantista para el trabajador derivada del Tribunal Europeo de Derechos Humanos a partir del asunto *Barbulescu II*²⁸.

Sin embargo, esa no es la interpretación realizada por alguna resolución judicial interna cuando, en relación con la Sentencia de la Gran Sala de 5 de septiembre de 2017, no tiene duda alguna en afirmar como “sus criterios son sustancialmente coincidentes con los de la jurisprudencia

una actuación contraria a derecho y que pueda tener repercusiones negativas para las personas trabajadoras afectadas no solo en el ámbito laboral sino también en el penal”, ROJO TORRECILLA, E.: “Medias verdades y *fake news* en el mundo jurídico. No cabe todo en la videovigilancia de una persona trabajadora. A propósito de la sentencia ‘López Ribalda’ de la Gran Sala del TEDH de 17 de octubre de 2019 (y recordatorio de la sentencia de Sala de 9 de enero de 2018 y del caso *Barbulescu II*, sentencia de Gran Sala de 5 de septiembre de 2017)”, *Blog: El nuevo y cambiante mundo del trabajo. Una mirada abierta y crítica a las nuevas realidades laborales*, entrada del 23 de octubre de 2019.

²⁶ STCo 186/2000, de 10 de julio.

²⁷ STCo 39/2016, de 3 de marzo.

Muy crítico con la misma, por cuanto la Sala “lleva a invertir las reglas del juego jurídico, de tal manera que será el poder de control empresarial el que legitimará con carácter general la vigilancia de los trabajadores, sin perjuicio de prestar atención obligada a las circunstancias concretas de cada caso para determinar si dicha fiscalización llevada a cabo por la empresa ha generado o no la vulneración del derecho fundamental en juego”, ROJO TORRECILLA, E.: “Medias verdades y *fake news* en el mundo jurídico. No cabe todo en la videovigilancia de una persona trabajadora...”, cit., entrada del 23 de octubre de 2019.

²⁸ En efecto, no cabe “olvidar la incidencia de la doctrina sentada en la Sentencia *Barbulescu II*, que, sin duda, va a provocar un cambio significativo en la doctrina constitucional y jurisprudencial española, 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, que debe afectar a la intimidad o al secreto de la comunicación en la menor posible, tanto en lo que se refiere a su intensidad como en relación con los medios técnicos utilizados”, RODRÍGUEZ ESCANCIANO, S.: *Derechos laborales digitales: garantías e interrogantes*, cit., pág. 190.

constitucional, sino también que --precisamente por ello-- la conducta empresarial de autos pasa holgadamente el filtro de los requisitos que el Alto Tribunal europeo exige para atribuir legitimidad a la actividad de control enjuiciada”. Así, llega a colegir como “la clara y previa prohibición de utilizar el ordenador de la empresa para cuestiones estrictamente personales nos lleva a afirmar 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... [Item más], el ponderado examen del correo electrónico [...] utilizando el servidor de la empresa y parámetros de búsqueda informática orientados a limitar la invasión de la intimidad, evidencia que se han respetado escrupulosamente los requisitos exigidos por la jurisprudencia constitucional y se han superado los juicios de idoneidad, necesidad y proporcionalidad”, de manera tal que los elementos descritos por el Tribunal Europeo de Derechos Humanos de obligada toma en consideración para la ponderación de intereses, pueden ser reconducidos básicamente a los tres sucesivos juicios de “idoneidad”, “necesidad” y “proporcionalidad”²⁹.

Además de los dos reseñados, los tribunales han tenido que interpretar otras materias vinculadas al poder de dirección y las nuevas tecnologías, pero su análisis exhaustivo excedería de los objetivos del presente trabajo. Eso sí, es necesario prestar atención, por las interconexiones que tiene con las redes sociales, a determinadas resoluciones judiciales que han fallado sobre el uso de internet en el lugar de trabajo, pues aunque las situaciones no sean idénticas, ambas herramientas tecnológicas utilizan unos procedimientos de actuación bastante similares.

Así, sin ánimo de exhaustividad, los pronunciamientos españoles vienen a tratar el acceso a internet en el lugar y en el tiempo de trabajo, aplicando la institución básica de las licencias comportamentales en el uso de las herramientas proporcionadas por el empresario, viniendo a dar pautas para considerar cuándo se está en presencia de un uso tolerable y cuándo se comete un abuso que pudiera ser calificado como un incumplimiento contractual.

A este respecto, los Tribunales de Justicia españoles han marcado los siguientes elementos hermenéuticos a tomar en consideración por el operador jurídico a la hora de decidir si el control empresarial de un medio facilitado por la empresa vulnera o no el derecho a la intimidad del trabajador, a saber:

1.- Los conflictos entre la fiscalización empresarial y la intimidad del trabajador surgen en tanto en cuanto se produce una utilización personalizada y no estrictamente profesional de la herramienta facilitada por la empresa, produciéndose dicha actuación habida cuenta las dificultades prácticas para prohibir de forma absoluta el empleo personal de un ordenador, una tablet, un móvil... con acceso a internet, y cabría añadir a las redes sociales, y también como consecuencia de la tolerancia generalizada a un uso moderado de los medios empresariales durante el tiempo de trabajo³⁰.

²⁹ STS 8 febrero 2018 (Sta. 119/2018). En términos similares, STS 15 enero 2019 (Sta. 21/2019).

“Que la Sala conocía, cuando dictó la sentencia, que ya se había pronunciado el TEDH en la sentencia *Barbulescu II*, era claro y manifiesto, y que si no se hubiera manifestado sobre la misma tampoco hubiera afectado al fallo [...] Pero, supongo, y simplemente es eso, una pura apreciación subjetiva, que en los debates sobre la sentencia fue objeto de atención aquella sentencia del TEDH y la Sala consideró conveniente referirse a la misma. Y, no lo hace ciertamente con un afán o perspectiva estrictamente intelectual o de análisis puramente doctrinal, sino que lo lleva a cabo por un objetivo o finalidad mucho más concreta y pragmática, la de intentar, y desde luego a su parecer es claro que lo consigue, evidenciar que sus criterios son sustancialmente coincidentes”, ROJO TORRECILLA, E.: “Sobre la privacidad del trabajador en su vida laboral tras la jurisprudencia *Barbulescu II*, del TEDH. A propósito de la sentencia del TS de 8 de febrero de 2018 (caso *Inditex*) y la ‘recuperación’ de la doctrina del TC en sentencia núm. 170/2013 de 30 de octubre”, *Blog: El nuevo y cambiante mundo del trabajo. Una mirada abierta y crítica a las nuevas realidades laborales*, entrada del 1 de abril de 2018.

³⁰ STS 8 marzo 2011 (Rec. 1826/2010).

2.- En la otra cara de la moneda, no es posible desconocer que los instrumentos habitualmente pertenecen al empresario y son facilitados por este para atender cuestiones de índole profesional, por tanto, entran bajo la égida del poder de dirección del artículo 20.3 ET, de manera que el titular de la unidad productiva tiene facultades de control sobre su utilización, que incluyen lógicamente su examen³¹.

Así, “con la finalidad de garantizar la buena marcha de la organización productiva, puede adoptar las medidas que estime más oportunas para verificar el cumplimiento por parte del trabajador de sus obligaciones laborales (artículo 20.3 del ET). Entre estas medidas se encuentran las de vigilancia y control de la utilización de los ordenadores y demás medios informáticos propiedad de la empresa y puestos a disposición de los trabajadores para utilizarlos en su prestación laboral”³².

3.- Las prerrogativas reconocidas al empresario no son omnímodas, lo que supone el respeto a la dignidad y a la intimidad del empleado. “En este punto es necesario recordar la existencia de un hábito social generalizado de tolerancia con ciertos usos personales moderados de los medios informáticos y de comunicación facilitados por la empresa a los trabajadores. Esta tolerancia crea una expectativa también general de confidencialidad en esos usos; expectativa que no puede ser desconocida, aunque tampoco convertirse en un impedimento permanente del control empresarial, porque, aunque el trabajador tiene derecho al respecto a su intimidad, no puede imponer ese respeto cuando utiliza un medio proporcionado por la empresa en contra de las instrucciones establecidas por esta para su uso y al margen de los controles previstos para esa utilización y para garantizar la permanencia del servicio”³³.

4.- En definitiva, el empresario debe regular el uso de estos medios para evitar contravenir derechos fundamentales del trabajador, de manera que si el instrumento es utilizado con un fin privado en contra de las prohibiciones³⁴ y conociendo los controles y medidas aplicables, el operador jurídico no podrá entender, cuando tenga lugar la fiscalización, que el trabajador ha visto vulnerada una expectativa razonable de intimidad³⁵, pues él mismo con su conducta habrá eliminado la garantía³⁶. Como se ha visto todas las sentencias citadas tratan sobre el control del correo electrónico, la instalación de cámaras de videovigilancia y el uso de internet, y no se refieren de manera expresa a la utilización de las redes sociales, de manera que cabe plantearse si los argumentos vertidos en ellas pueden resultar de aplicación al supuesto analizado con el fin de definir la expansión y límites del poder de dirección empresarial.

En este sentido, no es posible desconocer las advertencias realizadas por algún reputado autor doctrinal de referencia cuando señala que “la aplicación de esta doctrina en el ámbito de las redes

³¹ STSJ Madrid 8 febrero 2012 (Sta. 92/2012).

³² STSJ Comunidad Valenciana 19 noviembre 2018 (Sta. 3390/2018).

³³ STS 8 marzo 2011 (Rec. 1826/2010).

³⁴ Ahora bien, “en aquellos casos en los que la empresa, al margen de las instrucciones emitidas, ha venido mostrando cierta tolerancia hacia el uso indebido de las herramientas informáticas (bien no concediéndole trascendencia, o sólo descontando del salario el coste de las conexiones a internet), no puede sin más cambiar de actitud y perseguir tales conductas, sino que ha de advertir de esta intención, por razones de evidente buena fe”, SAN MARTÍN MAZZUCONI, C.: “Navegar por internet en horas de trabajo... ¿Quién? ¿Yo?”, *Aranzadi Social*, núm. 70, 2010 (BIB 2010/147).

³⁵ STSJ Cataluña 6 abril 2018 (Sta. 2014/2018).

³⁶ “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”, STS 13 septiembre 2016 (Sta. 723/2016).

En efecto, “la actuación de la empresa con respecto a Internet ha sido clara y ha reiterado las prohibiciones de uso del mismo para actividades privadas, con lo cual el actor de forma consciente y voluntaria incumplió prohibiciones empresariales que por otra parte tenían una justificación suficiente y para ello basta con ver que la actuación empresarial devino como consecuencia de las quejas de clientes por la lentitud del sistema lo que supone un perjuicio en forma de mala prestación de servicios por la empresa. Por otra parte el empleo de tiempo de trabajo reiteradamente durante la jornada laboral en actividades ajenas al trabajo supone quebrar la buena fe contractual, pues el uso no es escaso y limitado sino generalizado”, STSJ Castilla y León/Valladolid 5 diciembre 2012 (Sta. 2229/2012).

sociales no es automática, en la medida en que estas presentan particularidades propias: fundamentalmente, que la actividad en las mismas es un acto comunicativo y, por tanto, distinto de la mera navegación a través de Internet, y que su utilización exige un grado de interacción y comunicación mucho mayor que otros medios de comunicación, como el correo electrónico, conformando un auténtico espacio de expresión personal. Además, el establecimiento de límites en el uso de las redes sociales plantea mayores dificultades respecto de otros medios telemáticos, ya que el trabajador, con frecuencia, accede a estas plataformas a través de dispositivos de su propiedad (especialmente, smartphones o tablets)”³⁷.

Sin embargo, y a pesar de tener que tener muy en cuenta las palabras descritas, no parece demasiado descabellado aplicar al caso de las redes sociales las soluciones judiciales previstas para el uso de internet, no en vano “el tipo de mensajería instantánea en Internet no es otra cosa que una forma de comunicación que forma parte del ejercicio de la intimidad social”³⁸.

En efecto, “la navegación por internet en páginas web no relacionados con el trabajo (al igual que la participación en chats o la intervención en foros de discusión, wikis o redes sociales --pues son accesibles para cualquier interesado--) no tiene amparo en el derecho al secreto de las comunicaciones. En este caso, existe un acceso a información, pero no una verdadera comunicación interpersonal objetivamente tutelable, razón por la cual el juego de la facultad empresarial será más amplio a la hora de verificar los posibles incumplimientos contractuales del trabajador consistentes en consultar páginas web para fines particulares durante la jornada de trabajo, si bien no cabe desconocer su sujeción al límite indeclinable constituido por el derecho a la intimidad”³⁹.

Como corolario a lo señalado cabe mentar el literal de alguna sentencia que hace referencia expresa al instrumento aquí analizado y puede constituir un perfecto resumen de cuanto se ha analizado en páginas precedentes: “las empresas pueden vigilar los correos internos y las redes sociales de sus trabajadores, utilizadas desde los dispositivos facilitados, pero teniendo en cuenta especialmente que aquellos deben ser conscientes, mediante un aviso o comunicación previa, de que sus equipos pueden ser monitorizados. A su vez, el control debe ser proporcional, necesario y lo menos invasivo posible, evaluando el equilibrio entre el derecho del interés empresarial y la privacidad del trabajador”⁴⁰.

2.2. La reacción del legislador: la inclusión del control empresarial en la normativa sobre protección de datos

Como consecuencia de la importante jurisprudencia generada por el control empresarial de las nuevas tecnologías, el importante campo de actuación, todavía no explorado en su totalidad en el momento actual, y, la ya aludida, trascendental intromisión en los derechos de los trabajadores que puede provocar una actuación empresarial no acorde con estándares mínimos de protección de derechos fundamentales, la discusión en el foro ha sido tomada en consideración por el legislador, y de forma parcial, como se ha indicado al comienzo del presente trabajo, ha introducido ciertas previsiones en la normativa sobre protección de datos⁴¹.

De esta manera, cabe dar cuenta a nivel comunitario de la entrada en vigor del Reglamento 2016/679, en cuyo artículo 88 viene a posibilitar que los Estados miembros “a través de

³⁷ DEL REY GUANTER, S.: *La empresa hiperconectada y el futuro del trabajo. Conclusiones y recomendaciones del informe...*, cit., pág. 5.

³⁸ STEDH de 5 de septiembre de 2017, asunto *Barbulescu II*.

³⁹ STSJ Madrid 10 abril 2015 (Sta. 309/2015).

⁴⁰ STSJ Cataluña 6 abril 2018 (Sta. 2014/2018).

⁴¹ En efecto, “la regulación no se agota con la legislación de protección de datos, sino debe dar entrada a otras normas ya comentadas que han de disciplinar esa actividad ‘voraz’ de las empresas y corporaciones por extraer y tratar información de las personas sin utilizar políticas comerciales leales y transparentes”, OROZCO PARDO, G.: “Reflexiones acerca de los nuevos retos en el ámbito de la protección de datos en la sociedad digital globalizada”, *Base de Datos del Diario La Ley*, 2019, pág. 8.

disposiciones legislativas o de convenios colectivos, [establezcan] 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, en particular a efectos de contratación de personal, ejecución del contrato laboral, incluido el cumplimiento de las obligaciones establecidas por la ley o por el 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 relacionados con el empleo y a efectos de la extinción de la relación laboral”. A tal fin, las normas que vayan a ser dictadas “incluirán medidas adecuadas y específicas para preservar la dignidad humana de los interesados así como sus intereses legítimos y sus derechos fundamentales, prestando especial atención a la transparencia del tratamiento, a la transferencia de los datos personales dentro de un grupo empresarial o de una unión de empresas dedicadas a una actividad económica conjunta y a los sistemas de supervisión en el lugar de trabajo. A nivel estatal la LO 3/2018 establece una serie de medidas perfectamente aplicables a las redes sociales⁴², pues el artículo 87 LOPDGDD reconoce el derecho de trabajadores y empleados públicos “a la protección de su intimidad en el uso de los dispositivos digitales puestos a su disposición por su empleador”. En términos similares, la norma añade un artículo 20bis en el Estatuto de los Trabajadores en el que se reconoce el mismo derecho, remitiendo a la normativa vigente sobre protección de datos personales y garantía de los derechos digitales.

En el otro reverso de la moneda, además de la clásica definición del poder de dirección del artículo 20.3 ET, el artículo 87.2 LOPDGDD reconoce al empresario la posibilidad de “acceder a los contenidos derivados del uso de medios digitales facilitados a los trabajadores a los solos efectos de controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la integridad de dichos dispositivos”.

La norma viene a corroborar una idea *supra* ya expuesta, la fiscalización únicamente alcanza a aquellos dispositivos facilitados por la empresa, no siendo admisible en ningún caso que el empresario pueda controlar los instrumentos propiedad del trabajador⁴³; a lo sumo, aquel podrá establecer prohibiciones sobre la utilización de los terminales privados durante el tiempo y en el lugar de trabajo, pero siempre de una manera razonada y proporcionada, permitiendo un uso tolerable de los mismos, y llegar a realizar una vigilancia indirecta cuando establezca cauces de inspección sobre las herramientas laborales, como pueden ser mecanismos de control de tiempos, de la actividad laboral, etcétera.

Por su parte, el párrafo 3 de dicho precepto, mandata al titular de la unidad productiva a “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”.

⁴² Sin perjuicio de dar cuenta de otros preceptos con un contenido laboral claro como pueden ser el artículo 88 (derecho a la desconexión digital en el ámbito laboral); el artículo 89 (derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo) o el artículo 90 (derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral).

⁴³ PRECIADO DOMENECH, C.H.: *Los derechos digitales de las personas trabajadoras. Aspectos laborales de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y Garantía de los Derechos Digitales*, Cizur Menor (Aranzadi), 2019, pág. 141.

3.- La solución al control de las redes sociales mediante la implantación de códigos de buena prácticas o reglamentaciones internas

Aunque la norma heterónoma ha ido ganando espacio en la regulación de los derechos digitales, no es posible obviar el papel fundamental que va a seguir teniendo la autonomía colectiva en este ámbito⁴⁴.

A este respecto, cabe señalar como el artículo 40 RPD establece que “los Estados miembros, las autoridades de control, el Comité y la Comisión promoverán la elaboración de códigos de conducta destinados a contribuir a la correcta aplicación del presente Reglamento, teniendo en cuenta las características específicas de los distintos sectores de tratamiento y las necesidades específicas de las microempresas y las pequeñas y medianas empresas”.

Por su parte, la LOPDGDD dedica el artículo 38 a la regulación de los códigos de conducta y el artículo 91 refuerza el cometido de las normas paccionadas, cuando les permite establecer garantías adicionales de los derechos y libertades vinculados con el tratamiento de datos personales y la garantía de los derechos digitales en el ámbito laboral.

Asimismo, muchas de las resoluciones judiciales españolas que se han reseñado anteriormente ponen de manifiesto la importancia de diseñar, establecer y comunicar unas políticas de uso de herramientas informáticas que fijen unas directrices claras para los empleados⁴⁵, mediante la aplicación de prohibiciones parciales, habida cuenta de que “lógicamente, si no existe prohibición y simplemente se tolera un manejo moderado de estos instrumentos para fines privados, se desplaza al empleado la valoración de lo que es o no uso excesivo. Es por ello que cuando la empresa establece una política adecuada, mediante el diseño de protocolos o códigos de conducta, que permite al trabajador un uso social de su correo electrónico y de internet, este suele responder positivamente sujetándose a tales límites”⁴⁶.

En consecuencia, nada impide al empresario establecer limitaciones o la prohibición del uso de dispositivos electrónicos y de las redes sociales durante el tiempo y en el lugar de trabajo, con el fin de que el trabajador no se distraiga de sus actividades productivas, habida cuenta de que “en el marco de las facultades de autoorganización, dirección y control correspondientes a cada empresario, no cabe duda de que es admisible la ordenación y regulación del uso de los medios informáticos de titularidad empresarial por parte del trabajador, así como la facultad empresarial de vigilancia y control del cumplimiento de las obligaciones relativas a la utilización del medio en cuestión, siempre con pleno respeto a los derechos fundamentales”⁴⁷.

Sin embargo, “lo que debe hacer la empresa de acuerdo con las exigencias de buena fe es establecer previamente las reglas de uso de esos medios --con aplicación de prohibiciones absolutas o parciales-- e informar a los trabajadores de que va a existir control y de los medios que han de aplicarse en orden a comprobar la corrección de los usos, así como de las medidas que han de adoptarse en su caso para garantizar la efectiva utilización laboral del medio cuando sea preciso, sin perjuicio de la posible aplicación de otras medidas de carácter preventivo”⁴⁸, “como la exclusión de

⁴⁴ En efecto, “dado que muchos de los problemas legales en este área siguen sin resolverse, es aconsejable elaborar disposiciones específicas de la empresa (una ‘política de redes sociales’)”, GÖPFERT, B. y WILKE, E.: “Facebook and Employment Law in Germany: Regulating the use of social media through a policy on social networking sites”, cit., pág. 10.

⁴⁵ Estas resoluciones “ilustran claramente la necesidad de que las empresas y los empleados conozcan sus derechos y posibles responsabilidades en relación con el uso de las redes sociales en el lugar de trabajo, incluso cuando el uso de las redes sociales se realiza fuera del trabajo”, JUNG LEE, E.: “The implications of personal use of social media on employment relationships: An update of Canadian case law”, *Employment & Industrial Relations Law*, Vol. 22, núm. 2, 2012, pág. 8.

⁴⁶ STSJ Madrid 10 abril 2015 (Sta. 309/2015).

⁴⁷ STCo 241/2012, de 17 de diciembre.

⁴⁸ STSJ Madrid 10 abril 2015 (Sta. 309/2015).

conexiones a determinadas páginas web o el control del tráfico de internet o de la mensajería electrónica, pero no el de su contenido”⁴⁹.

De esta manera, “de no existir protocolo, o si existiendo este no prohíbe el uso de los equipos para cuestiones personales, el trabajador disfrutaría de una expectativa razonable de intimidad que anularía cualquier intromisión empresarial en estos equipos, así como también en las cuentas de correo o sistemas de mensajería que use el trabajador para fines particulares”⁵⁰.

Asimismo, para evitar problemas de vulneración de derechos fundamentales, los documentos de buenas prácticas deben hacer hincapié en que en su ejecución, el empleador debe cumplir los requisitos del triple juicio pergeñado, y *supra* mencionado, por el Tribunal Constitucional, a saber: idoneidad, necesidad y proporcionalidad.

En consecuencia, dichas políticas empresariales deben ser absolutamente respetuosas con los derechos fundamentales de los trabajadores, en particular la intimidad, el secreto de las comunicaciones o la dignidad, advirtiendo claramente a los trabajadores sobre los posibles controles y fiscalizaciones de su actividad profesional y la monitorización y utilización adecuada de las herramientas tecnológicas, habida cuenta de que no cumplir con los estándares legales y jurisprudenciales conducirá sin lugar a dudas a la nulidad de la medida empresarial por vulnerar prerrogativas garantizadas al más alto nivel constitucional.

Por los motivos descritos, en España, se están empezando a implantar códigos de conducta o reglamentaciones internas (a pesar de que se encuentren todavía “en estado embrionario”⁵¹) con el fin de pautar la utilización de móviles, tabletas, ordenadores, etcétera y el acceso a las redes sociales durante el tiempo de trabajo⁵².

4.- Breve reflexión final

Las redes sociales han aparecido con gran ímpetu en las actividades cotidianas de los ciudadanos hasta el punto de llegar a convertirse en un medio de socialización de uso masivo en el día a día, que llega a tener, como no podía ser de otra manera, su trascendencia en el ámbito laboral.

Frente a esta realidad el mundo del Derecho, y en particular el sistema de relaciones laborales, no puede quedar ajeno y continuar con la anomia legislativa que suele caracterizar a los modelos jurídicos en la ordenación de cuantas derivas está planteando la revolución digital. En este sentido, son de alabar los intentos regulatorios incorporados en el Reglamento UE 2016/679, del Parlamento y del Consejo, de 27 de abril de 2016 (RPD), y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD).

Sin embargo, se trata de meros remedios parciales, que no plantean una solución global al problema, de ahí de que, desde estas líneas, y sin perjuicio del papel fundamental que ha de jugar la autonomía colectiva de los agentes sociales, se considera oportuno una actuación a nivel heterónomo, en la cual el legislador tome conciencia de la situación y proceda a dictar una norma completa que tenga en cuenta todas y cada una de las materias relacionadas con la implantación en el seno de la empresa de cuanto se ha conocido como revolución digital.

Mientras ello ocurre, habrá que continuar pendientes de las resoluciones judiciales y como, en la práctica forense, van interpretando los importantes desafíos que las nuevas tecnologías presentan en el lugar de trabajo. En este sentido, y a fin de solventar cuantos retos plantea la utilización de las redes sociales en el espacio laboral, es posible aplicar de manera analógica, y *mutatis mutandis*, los

⁴⁹ STSJ Comunidad Valenciana 19 noviembre 2018 (Sta. 3390/2018).

⁵⁰ STSJ Cataluña 6 abril 2018 (Sta. 2014/2018).

⁵¹ NAVARRO NIETO, F.: “El alcance del derecho al respeto de la correspondencia del trabajador en la jurisprudencia del Tribunal Europeo de Derechos Humanos”, *Temas Laborales*, núm. 145, 2018, pág. 162.

⁵² Un análisis exhaustivo de las características básicas que deberían cumplir estos códigos llegando a aconsejar un decálogo de ellas, DEL REY GUANTER, S.: *La empresa hiperconectada y el futuro del trabajo. Conclusiones y recomendaciones del informe...*, cit., págs. 10-13.

razonamientos judiciales establecidos en el marco de otros problemas distintos pero con variadas y amplias interconexiones.

En consecuencia, las empresas están habilitadas para fiscalizar las redes sociales de sus trabajadores, en especial cuando son utilizadas desde las herramientas que aquellas ponen a su disposición, pero deben asegurarse que el empleado conoce previamente los mecanismos y procedimientos de control, y este ha de ser absolutamente respetuoso con el derecho a la intimidad del trabajador, de manera que ha de cumplir los juicios de idoneidad, necesidad y proporcionalidad.

En fin, los códigos o protocolos de buenas prácticas empresariales deben jugar un papel fundamental en el cumplimiento de las obligaciones empresariales, habida cuenta de que son el instrumento idóneo para ordenar los procesos de advertencia y comunicación al trabajador e impedir así cualquier tipo de contravención de los derechos fundamentales ya descritos.

En definitiva, las redes sociales han llegado para quedarse y con el paso del tiempo parece que no van a hacer otra cosa sino aumentar su influencia en los ciudadanos, negar esa evidencia sería no ser conscientes del problema. Por tal razón, es necesario educar en un uso responsable de las mismas y que los sujetos aprendan a utilizarlas de manera adecuada. En el ámbito laboral, se trata de cohonestar los intereses empresariales con los derechos de los trabajadores, alcanzando el adecuado equilibrio entre rendimiento y productividad empresarial y cierta tolerancia hacia el uso moderado de las redes durante el tiempo y lugar de trabajo.

Roberto Fernández Fernández

Profesor Titular de Universidad, Universidad de León (España)

Cristina González Vidales

Contratada predoctoral FPU (Ministerio de Universidades), Universidad de León (España)