

La «Carta de derechos digitales» de los trabajadores ya es ley: menos claros que oscuros en la nueva regulación

Margarita Miñarro Yanini

Secretaria

1. El análisis de actualidad sociolaboral del número 424 de esta revista, correspondiente al mes de julio de 2018, concluía con el deseo de que el título X del proyecto de Ley orgánica de protección de datos, fruto de la tramitación de una enmienda del Grupo Socialista, prosperase, puesto que incorporaba novedosamente una «carta de derechos digitales» en el ámbito laboral. El favor expresado no se basaba en las bondades de su contenido, pues como se apuntaba, presentaba más sombras que luces, sino en la necesidad de disponer de un mínimo tratamiento legislativo respecto de cuestión tan trascendental para el mundo del trabajo actual. Aportaba así, en última instancia, datos legislativos que permitirían al intérprete superar los vicios jurídicos y reconstruir sobre fundamentos avanzados el equilibrio perdido, en una materia que se ha venido configurando hasta ahora como «una encrucijada en la que confluyen líneas de fuerza en tensión y múltiples cuestiones en que la jurisprudencia no siempre ha ofrecido respuestas uniformes o coincidentes», según apunta la muy reciente e importante Sentencia del Tribunal Supremo (STS) (Sala de lo Penal) 489/2018, de 23 de octubre.

La «Carta de derechos digitales laborales» ya se ha convertido en ley (LO 3/2018). Ello ha supuesto, además, que el ET tenga un nuevo precepto, artículo 20 bis, rubricado «Derechos de los trabajadores a la intimidad en relación con el entorno digital y a la desconexión»

Ese deseo se ha materializado y la «Carta de derechos digitales laborales» ya se ha convertido en ley (LO 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales –LOPDGDD–). Ello ha supuesto, además, que el Estatuto de los Trabajadores (ET), al igual que el Estatuto Básico del Empleado Público (nueva letra j) bis del art. 14), tenga un nuevo precepto, artículo 20 bis, rubricado «Derechos de los trabajadores a la intimidad en relación con el entorno digital y a la desconexión». Este precepto dispone que:

Los trabajadores tienen derecho a la intimidad en el uso de los dispositivos digitales puestos a su disposición por el empleador, a la desconexión digital y a la intimidad frente al uso de dispositivos de videovigilancia y geolocalización en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales.

De la relectura del [análisis de actualidad](#) referido se evidencia que hay un notable cambio, al menos de formato, entre la versión que fue examinada en este y la que ha quedado plasmada en la ley. La diferencia se percibe claramente en su extensión, pues mientras que el precepto aprobado, con sus poco más de cuatro líneas, es muy breve, el originariamente propuesto y estudiado en el trabajo citado era notablemente más extenso, incluyendo seis apartados. Ciertamente es que, como observación general, el recorte en la extensión no tiene por qué suponer necesariamente empeoramiento de la regulación, aunque, sin duda, tampoco mejora. Asimismo, hay que tener presente que las previsiones normativas contenidas en la ley tienen por objetivo mejorar las garantías de los derechos de los ciudadanos en el entorno digital, con especial referencia al ámbito laboral, por lo que sería paradójico que su enflaquecimiento pudiera suponer el debilitamiento de las garantías reconocidas por el Tribunal Europeo de Derechos Humanos (TEDH).

Aun sin relación directa con temas laborales, en este sentido resulta ilustrativo traer a colación la polémica generada por la inclusión por la LOPDGDD del [artículo 58 bis en la Ley orgánica de régimen electoral general](#), que permite a los partidos políticos recabar datos personales de páginas web para organizar y realizar acciones políticas durante las campañas electorales. [Esta revisión ha despertado tantas reticencias que la Agencia Española de Protección de Datos \(AEPD\) se ha visto obligada a intervenir](#) para recordar que la nueva ley es garantista y no dismantela la protección precedente, a fin de acallar las críticas y temores.

Las previsiones normativas contenidas en la ley tienen por objetivo mejorar las garantías de los derechos de los ciudadanos en el entorno digital, con especial referencia al ámbito laboral, por lo que sería paradójico que su enflaquecimiento pudiera suponer el debilitamiento de las garantías reconocidas por el TEDH

Sin llegar a tal extremo, la experiencia laboral y la práctica judicial revelan la necesidad de contar con un marco regulador seguro de referencia para ponderar los derechos e intereses que entran en juego, que dé confianza tanto a empleadores y trabajadores. Ello es así por cuanto la falta de uniformidad de criterios, expresada en la [sentencia penal citada](#) y que se aprecia igualmente en el orden social, ha sido una constante hasta ahora.

Muestra de esta inseguridad es el [Auto del Tribunal Supremo \(ATS\) de 14 de junio de 2018 \(rec. 4200/2016\)](#), que inadmite el recurso, no ya por falta de superación del juicio de contradicción, sino porque la sentencia recurrida aplica la doctrina de su tiempo, reflejando la jurisprudencia introducida por la sala a raíz del cambio en la doctrina constitucional (Sentencia del Tribunal Constitucional –[STC– 39/2016, de 3 de marzo](#)) que relajó la exigencia de transparencia de las empresas. Con todo, la evolución de la jurisprudencia del TEDH –célebre [asunto Barbulescu](#), tantas veces referido en las páginas de esta revista– parece que corregiría esa doctrina constitucional, y, por lo tanto, esa jurisprudencia social,

lanzando nuevos mensajes garantistas a las empresas. No obstante, lecturas más sombrías de la nueva norma parecen no ir en dicha dirección.

De hecho, a finales del 2018, con gran eco mediático, se difundía en la prensa económica el titular, en relación con el [ATS de 19 de julio de 2017 \(rec. 3945/2017\)](#), de que «el [Supremo valida utilizar los datos del GPS para justificar el despido](#)». Es cierto que en el texto del artículo se precisaba que ello exigía la condición de que se hubiera informado previamente al trabajador sobre el dispositivo y su finalidad eventualmente disciplinaria. No obstante, el titular ponía énfasis en la actitud relativamente permisiva de los tribunales en esta materia, que el órgano autor del auto corroboraría, pues la información dada por el empresario no alcanzaba «la finalidad exacta que se le ha asignado a ese control». En consecuencia, el enfoque que se transmitía con ello es el de protección del interés legítimo del empleador a controlar los incumplimientos de los trabajadores. La cuestión es dilucidar si este es también el que prima una norma «de garantías» como es la LOPDGDD, que trata de exhibir su finalidad garantista incluyendo tal término en su propia denominación.

En las siguientes páginas se tratará de apuntar respuestas a tales cuestiones, a través del esbozo del contenido de los preceptos a los que remite el nuevo [artículo 20 bis del ET](#), con objeto de fijar los términos en que han de entenderse delimitados los derechos a la intimidad digital, incluido el «derecho a la desconexión digital» fuera de la jornada de trabajo. Estos preceptos de referencia son los nuevos artículos [87](#) a [91](#) de la LOPDGDD.

2. El primer precepto al que el nuevo precepto estatutario reenvía es el [artículo 87 de la LOPDGDD](#), rubricado «Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral». No obstante, este artículo no aporta ninguna novedad relevante desde el punto de vista práctico. Así, el apartado 1 es meramente declarativo del derecho de los trabajadores a la protección de su intimidad en el uso de dispositivos digitales proporcionados por la empresa, que ya estaba reconocido, aun no de forma totalmente clara, por el Tribunal Constitucional –*vid.* [STS 119/2018, de 8 de febrero](#), y [STS \(Sala de lo Penal\) de 23 de octubre de 2018](#), citada–.

El nuevo precepto estatutario reenvía, en primer lugar, al artículo 87 de la Ley orgánica 3/2018, rubricado «Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral», artículo que no aporta ninguna novedad relevante desde el punto de vista práctico

El apartado 2 de este precepto no merece valoración más positiva. Este permite al empleador, de forma genérica, acceder a los contenidos de la comunicación digital de los trabajadores, remitiendo al [artículo 20.3 del ET](#). No se entiende, en consecuencia, la utilidad de este apartado, por cuanto el [artículo 20 bis del ET](#) remite al [87.2 de la LOPDGDD](#) y, este, a su vez, al [artículo 20.3 del ET](#). De este modo, el interés legítimo del empleador al control

sigue garantizándose, con respeto «en todo caso [a] los estándares mínimos de protección de su intimidad de acuerdo con los usos sociales y los derechos reconocidos constitucional y legalmente». La cuestión es que es la LOPDGDD, precisamente, el instrumento que debería haber fijado tales estándares de protección. Se recuerda, en este sentido, que la ausencia de concreción legislativa fue lo que devaluó el valor práctico del criterio establecido en la [STC 29/2013, de 11 de febrero](#), que fue involucionando en las Sentencias [170/2013, de 7 de octubre](#), y [39/2016, de 3 de marzo](#). Tal previsión ni tan siquiera clarifica si el empleador puede establecer una «prohibición absoluta» de uso extralaboral o si debe respetar cierto uso privado. En este punto, parece que el TEDH ha evolucionado en la dirección de admitir un uso privado mínimo –asuntos [Bărbulescu](#) y [Libert](#)–. Con todo, el Documento de Trabajo del Grupo de Trabajo del artículo 29 (GT29), relativo al control o vigilancia de las comunicaciones electrónicas en el trabajo ([WP 55, de 29 de mayo de 2002](#)), parece reconocer potestad al empresario para prohibir a los trabajadores todo uso privado de estos dispositivos digitales.

La cuestión es relevante, pues, si no se acepta que sea posible el establecimiento de tal prohibición absoluta, decaería la posibilidad de realizar «controles ocultos», sin mediar información previa. Si bien la jurisprudencia nacional admitió tal posibilidad de vetar todo uso particular ([STS de 6 de octubre de 2011, rec. 4053/2010](#)), y esta posición ha tenido algún apoyo en la práctica administrativa (AEPD, procedimiento E-01017/2015), se considera que debe descartarse atendiendo a la línea marcada por la [Sentencia Bărbulescu](#). Al margen de que debe aceptarse cierto uso mínimo extralaboral, la garantía de transparencia debe ser un elemento esencial para superar todo juicio previo de legitimidad –[STS \(Sala de lo Penal\) de 23 de octubre de 2018](#), citada–.

Con todo, la valoración aún puede ser menos favorable desde la perspectiva laboral. Así, la versión definitiva de la norma establece un «derecho de participación» de la representación de los trabajadores en el establecimiento de la política de uso de los dispositivos digitales en la empresa, aunque sin concretar la modalidad –información, audiencia, consulta–. De este modo, esta garantía colectiva se ha devaluado durante el proceso de tramitación parlamentaria, pues la versión originaria se refería al «derecho a acordar» el protocolo de uso razonable de los dispositivos digitales, si bien preveía la posibilidad de que este no existiera, permitiendo la aprobación unilateral con un deber de información a los trabajadores del contenido de las pautas adoptadas, como se apuntaba en la [actualidad del número 424 de esta revista](#). Se reduce, además, el contenido obligatorio del protocolo, pues en la versión originaria se incluían indicaciones sobre cómo debería hacerse, así como su contenido mínimo, mientras que en la versión adoptada se per-

La versión definitiva de la norma establece un «derecho de participación» de la representación de los trabajadores en el establecimiento de la política de uso de los dispositivos digitales en la empresa, aunque sin concretar la modalidad, devaluándose esa garantía colectiva durante el proceso de tramitación parlamentaria

mite que sea fijado libremente por el empresario. El cambio es evidente, suponiendo una transacción que ha provocado la devaluación de la garantía colectiva. En consecuencia, este aspecto, que podría haber implicado un avance, se ha diluido durante el trámite parlamentario. Por lo demás, carece de novedad que se reconozca el deber de información previa –AEPD, informe 0464/2013; [Recomendación \(2015\) 5, del Consejo de Europa](#), punto 10–, a la par que sorprende que se prescinda de la más mínima referencia al principio de proporcionalidad, exigido por el acervo normativo –[Dictamen del GT29 2/2017](#); [Recomendación \(2015\) 5, del Consejo de Europa](#), punto 14–.

3. Por lo que respecta a las prácticas de videovigilancia y grabación de sonidos en el lugar de trabajo, la valoración tampoco puede ser positiva. El [artículo 89](#), rubricado «Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo», mantiene la misma actitud permisiva para tal tratamiento de datos –imágenes y sonidos– que el precedente, asumiendo el enfoque liberal del [artículo 20.3 del ET](#), al que nuevamente se remite. Resulta sorprendente la nueva remisión «dentro de su marco legal y con los límites inherentes al mismo», pues esta fórmula, vacía de contenido regulador, contrasta con el copioso cuerpo de doctrina administrativa que ilustra perfectamente cómo debe articularse (por ejemplo, AEPD, informes 0495/2009 o 0475/2014).

El artículo 89 («Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo») mantiene la misma actitud permisiva para tal tratamiento de datos –imágenes y sonidos– que el precedente, asumiendo el enfoque liberal del artículo 20.3 del ET, al que nuevamente se remite

Más positiva es la exigencia del deber de información previa «expresa, clara y concisa», que parece neutralizar la involutiva [STC 39/2016, de 3 de marzo](#). Sin embargo, la norma tampoco desconoce la posición de defensa del interés empleador, pues incluye una medida de flexibilización del deber de información previa, para los supuestos de captación de imágenes que revelen «la comisión flagrante de un acto ilícito», en cuyo caso se entiende cumplido el deber con la colocación del dispositivo en lugar visible al que se refiere el [artículo 22.4 de la LOPDGDD](#) –que recoge, a su vez, el art. 12 [Reglamento general de protección de datos \(RGPD\)](#)–. Nuevamente en este punto, los cambios respecto de la versión inicial son notables. Así, el originario artículo 22.5 se refería a la «comisión flagrante de un acto delictivo», en cuyo caso eximía al empleador del deber de información y mantenía su valor probatorio, sin perjuicio de la responsabilidad que pudiera derivarse. No obstante, el [artículo 22.8 de la LOPDGDD](#) se limita a remitirse al [artículo 89](#), que debilita la intensidad informativa, en línea con la [STC 39/2016, de 3 de marzo](#). Más dificultades se presentan para conciliar este debilitado deber de información con el más exigente derivado de la [doctrina López Ribalda](#), en el que, aunque las grabaciones captaron apropiaciones indebidas de productos, no se eximió a la empresa del deber de información previa y precisa.

No clarifica el precepto si «acto ilícito» debe interpretarse como acto delictivo –penal– o como todo incumplimiento grave y culpable del trabajador. Al respecto, se considera que tal concepto no puede restringirse a la dimensión penal, pues el cambio expreso de terminología denota una voluntad de ampliación que así lo avala. No obstante, se entiende que tampoco puede hacerse una interpretación genérica, en el sentido de que se incluye todo incumplimiento, puesto que ello diluiría la garantía del derecho fundamental. Igualmente deja sin respuesta la ley la cuestión de si la invalidación de la prueba de videovigilancia –bien por infringir el deber de información previa, bien por incurrir en otra lesión del derecho a la intimidad– contamina otras posibles pruebas del incumplimiento laboral. La doctrina judicial actual no es unánime en este punto, pues mientras que algunas salas sí las admiten (Sentencia del Tribunal Superior de Justicia –STSJ– del País Vasco 651/2018, de 22 de marzo), no así otras (STSJ de Castilla-La Mancha 25/2018, de 12 de enero), sin que hasta la fecha exista pronunciamiento en unificación de doctrina al respecto. No obstante, tanto la [Sentencia López Ribalda et al.](#), como la reiterada [STS \(Sala de lo Penal\) de 23 de octubre de 2018](#), se inclinan por aceptar la validez de otras pruebas no contaminadas con la tecnológica.

El precepto no clarifica si «acto ilícito» debe interpretarse como acto delictivo –penal– o como todo incumplimiento grave y culpable del trabajador. Al respecto se considera que no puede restringirse a la dimensión penal, pero tampoco hacerse una interpretación genérica que diluya la garantía del derecho fundamental

Por lo demás, la garantía de información-control colectiva también ha resultado claramente devaluada, por cuanto ni siquiera se respeta el mínimo establecido en el [artículo 64 del ET](#).

Es oportuno apuntar que la jurisprudencia del TEDH no ha descartado de forma absoluta la validez de la prueba de videovigilancia, incluso en ausencia de cualquier información previa, siempre que concurren circunstancias especiales –sospecha fundada de incumplimiento, grabación selectiva del trabajador afectado, breve periodo de tiempo–. En ello incide en su [Sentencia López Ribalda](#), con remisión a su [Sentencia de 5 de octubre de 2010, demanda 420/07, asunto Köpke](#).

Ninguna novedad sustancial presenta el apartado segundo, que dispone que «en ningún caso se admitirá la instalación de sistemas de grabación de sonidos ni de videovigilancia en lugares destinados al descanso o esparcimiento de los trabajadores», puesto que reproduce el criterio de la [STC 198/2000, de 24 de julio](#). Por la misma razón, tampoco es novedoso el apartado tercero, pues, aunque la norma legal es más restrictiva respecto del empleador «para la grabación de sonidos en el lugar de trabajo», al considerarla válida «únicamente cuando resulten relevantes los riesgos para la seguridad» y con respeto al «principio de proporcionalidad», la limitación que establece es más aparente que real.

En este sentido, además de que maneja conceptos que se han constatado como flexibles –así, la [STS 77/2017, de 31 de enero](#), reinterpreta el concepto de «seguridad pública» como seguridad patrimonial del empleador–, el [Dictamen 5/2005 del GT29](#) ha exigido mayores precisiones causales.

Queda claro, en cualquier caso, que la carga de la prueba sobre la concurrencia de tal causa corresponde al empleador, que no solo ha de justificar la existencia del riesgo, sino también la proporcionalidad de la medida, eligiendo la que sea menos invasiva para los derechos de los trabajadores afectados. Asimismo, habrá de probar que ha informado adecuadamente de la medida de videovigilancia y/o grabación. En este punto, debe recordarse el exigente test establecido por la [Sentencia del TEDH de 28 de noviembre de 2017 \(caso Antović y Mirković vs. Montenegro\)](#), que concluyó que, salvo razones de suficiente interés, el empleador no puede grabar las clases del profesorado universitario en instalaciones de su propiedad sin el consentimiento específico de este. Por su parte, la [Sentencia de la Audiencia Nacional 87/2017, de 15 de junio](#), consideró que el interés de ciertos clientes por el modo de prestación del servicio no constituye interés empresarial suficiente para validar una cláusula de cesión de datos incluida en los contratos.

Por lo demás, el inciso final del apartado 3 exige la supresión de los sonidos conservados con estos sistemas de grabación, como expresión de las nuevas garantías vinculadas al derecho a la intimidad, si bien con notable autonomía del [artículo 18.4 de la Constitución española](#). A tal efecto, remite a lo previsto en el [artículo 22.3 de la LOPDGDD](#).

4. Respecto del [artículo 90](#), referido al «Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral», la valoración tampoco puede ser favorable, pues nuevamente se omiten referencias a garantías fundamentales, como es el principio de proporcionalidad. Sin atender a la exigencia de motivos específicos para el control expresada en la práctica administrativa consultiva ([Dictamen del GT29 2/2017](#)), este parte, como los anteriores examinados, de la legitimación del empresario para efectuarlo. De nuevo, la única clave garantista que introduce es la traslación a la ley de la exigencia de transparencia concretada en el deber de información previa –expresa, concisa, específica–. No obstante, tal exigencia ya había sido respaldada por la práctica administrativa (AEPD, informes 193/2008 y 090/2009) y por la doctrina judicial –[STSJ de Andalucía/Sevilla de 19 de julio de 2017 \(rec. 2776/2016\)](#), firme por el ATS de 19 de julio de 2018 (rec. 3945/2017)–. En cualquier caso, es cierto que la previsión legal servirá para erradicar doctrinas de su-

Respecto al «Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral» (art. 90), la valoración tampoco puede ser favorable. De nuevo, la única clave garantista que introduce es la traslación a la ley de la exigencia de transparencia concretada en el deber de información previa expresa, concisa y específica

plicación que admiten conocimientos «presuntos» –SSTSJ de [Cataluña 1706/2012, de 5 de marzo](#), y de [Galicia 2348/2017, de 26 de abril](#)–, en línea con la corriente judicial que exige un conocimiento específico –[STSJ de Castilla-La Mancha 487/2015, de 28 de abril](#), aplicando la [STC 29/2013, de 11 de febrero](#)–. Sin embargo, no se atiende a las garantías de información colectiva, por lo que se frustra la recomendación de la práctica consultiva administrativa de generalizarla. Por tanto, aunque la información colectiva debiera ser una exigencia inexcusable en esta materia, habrá que continuar basándose solo en el [artículo 64 del ET](#).

En cualquier caso, es oportuno recordar que la AEPD consideró adecuada la divulgación de esta información mediante circulares informativas y la instalación de carteles indicativos en los vehículos equipados con GPS (AEPD, E/00597/2006 y E/6036/2014). Por lo que respecta al deber de cancelar tales datos cuando desaparezca el fin para el que se trataron, la AEPD, en aplicación de la recomendación del GT29, [Dictamen 5/2005](#), fija el periodo de conservación en 2 meses, considerando que, si se quieren conservar más tiempo por razones de gestión de recursos, deben hacerse anónimos (AEPD, informe 613/2009).

La ausencia de referencia expresa al principio de proporcionalidad habrá de ser integrada por el intérprete y el operador jurídicos, pues es condición elemental para que, superado el juicio de transparencia, se supere el de legitimidad. Así lo entienden tanto el GT29 ([Dictámenes 2/2017](#) y [5/2005](#)) como, por adhesión, la AEPD y la doctrina judicial –*vid.* STSJ de Andalucía/Granada 1937/2017, de 18 de septiembre–.

5. Con todo, la previsión de la LOPDGDD que mayor trascendencia mediática ha alcanzado, en buena medida con base en valoraciones más superficiales que de fondo –*vid.* relativizando su impacto, por considerar que deriva del «esnobismo de los derechos cívicos», Molina Navarrete, C. (2017). Jornada laboral y tecnología de la info-comunicación: «desconexión digital», garantía del derecho al descanso. *Temas Laborales. Revista Andaluza de Trabajo y Seguridad Social*, 138, 249-283–, es la contenida en el [artículo 88](#), relativo al «Derecho a la desconexión digital en el ámbito laboral». A él se remite el [artículo 20 bis del ET](#), al reconocer el derecho a la desconexión como garantía de efectividad de los derechos al descanso, a la intimidad y a la conciliación de la vida laboral y familiar.

Si bien su versión definitiva también ha experimentado algunos cambios respecto de la originaria, su trascendencia sustantiva es bastante menor que la de algunos de los reseñados anteriormente, por lo que los

La previsión de la Ley orgánica 3/2018 de mayor trascendencia mediática, con base en valoraciones más superficiales que de fondo, es la del artículo 88: «Derecho a la desconexión digital en el ámbito laboral». A él se remite el artículo 20 bis del ET, al reconocer ese derecho como garantía de efectividad de los derechos al descanso, a la intimidad y a la conciliación de la vida laboral y familiar

comentarios que se realizaron en la [actualidad del número 424 de esta revista](#) son trasladables aquí. No obstante, a fin de que este repaso sea completo, procede referenciar brevemente sus aspectos de mayor relevancia.

Como idea previa, es oportuno recordar que, si bien las facetas del derecho a la intimidad en relación con el poder de control empresarial examinadas tienen regulación orgánica, la regulación de la desconexión digital carece de tal consideración, según indica la [disposición final primera de la LOPDGDD](#).

Si bien ello puede parecer una debilidad, lo cierto es que facilitará posteriores desarrollos, tanto en el ámbito legislativo como en el de la negociación colectiva.

Es, precisamente, la negociación colectiva la que ha de fijar las garantías que den contenido al derecho que reconoce la norma legal. Así, se ha establecido una clara diferencia entre la regulación general de las modalidades de ejercicio de esta garantía, que correspondería a la negociación, y la regulación del concreto aspecto de la prevención de un nuevo riesgo laboral reconocido: la fatiga informática en general, así como en situaciones de especial vulnerabilidad a tal riesgo –trabajo a distancia–, objeto de «política interna» de la empresa. En este punto, la ley debiera haber previsto su inserción en la [Ley de prevención de riesgos laborales](#) (LPRL), puesto que al tratarse de un nuevo riesgo laboral debe activarse el sistema preventivo –evaluación y planificación–. En consecuencia, las previsiones normativas de los [artículos 88 de la LOPDGDD](#) y [20 bis del ET](#) han de vincularse con la LPRL.

No se comparte la crítica a la ausencia de remisión a la negociación colectiva en esta regulación específica de la fatiga informática, que sí se ha efectuado para la reglamentación general del derecho a la desconexión. Ello es así por cuanto una remisión tan abierta como la general hace dudar de su efectividad y de su generalización en todas las empresas y sectores. Además, en esta materia ha de aplicarse un sistema de gestión preventiva de riesgos laborales, correspondiendo el deber de protección al empleador, en el marco de competencias de participación de las representaciones de los trabajadores, que debería resultar más intensa que la mera audiencia –devaluación esta del derecho de participación que sí merece crítica–, desempeñando la negociación colectiva el papel de mejorarla.

6. Esta clásica función de mejora de la regulación es la única que atribuye a la negociación colectiva el [artículo 91](#), relativo a los «Derechos digitales en la negociación colectiva», en su versión definitiva. Así, recuerda que los convenios colectivos «podrán establecer garantías adicionales» para salvaguardar los derechos digitales en la empresa. Comparando el texto

Se ha establecido una clara diferencia entre la regulación general de las modalidades de ejercicio de esta garantía, que correspondería a la negociación, y la regulación del concreto aspecto de la prevención, objeto de «política interna» de la empresa. La ley debiera haber previsto su inserción en la LPRL

vigente con el originario incluido en la enmienda, se aprecia que también ha «adelgazado» sustancialmente. Con todo, el contenido perdido se refería a una función mucho más extensa y compleja de la negociación colectiva que se refleja en el artículo 88.2 del [RGPD](#). En consecuencia, esa función sigue quedando abierta, aunque el legislador de protección de datos se haya abstenido de ir más allá, seguramente por evitar situaciones que la experiencia ha demostrado que son complicadas para los interlocutores sociales.

La nueva Ley orgánica 3/2018 no representa la regulación esperada, ni es la más conveniente para un adecuado equilibrio entre el poder de control empresarial y las garantías de respeto de los derechos fundamentales de los trabajadores

7. Hasta aquí esta breve presentación crítica de la nueva [LOPDGDD](#), cuyo análisis, a buen seguro, ocupará en lo sucesivo numerosas páginas de esta revista. Sin duda, no representa la regulación esperada, ni es la más conveniente para un adecuado equilibrio entre el poder de control empresarial –cuya legitimidad presume– y las garantías de respeto de los derechos fundamentales de los trabajadores. Con todo, se ha de reconocer a esta norma el valor de hacer del control empresarial un espacio más transparente para el trabajador, reduciendo la opacidad actual. Además, con toda seguridad será útil a los efectos de eliminar, o siquiera reducir notablemente, la actual «penuria normativa y los zigzagueos jurisprudenciales» denunciados por la tantas veces citada [STS \(Sala de lo Penal\) de 23 de octubre de 2018](#).

En cualquier caso, la [LOPDGDD](#) constituye un paso legislativo, pero no será el último, puesto que, en el actual contexto, no es concebible que el ET carezca de regulaciones específicas en torno a los derechos de «ciudadanía digital responsable del trabajador» –*vid.*

Con todo, se ha de reconocer el valor de hacer del control empresarial un espacio más transparente para el trabajador, amén de que será útil para eliminar, o reducir notablemente, la actual «penuria normativa y los zigzagueos jurisprudenciales»

Molina Navarrete, C. (2018). Redes sociales, códigos de conducta y ciudadanía digital responsable del trabajador: «cara B» del consentimiento y libertad de expresión crítica. *Revista de Trabajo y Seguridad Social. CEF*, 419, 158-168-. En consecuencia, en tanto aparezca un nuevo referente, se espera que más completo y acertado, habrán de buscarse soluciones óptimas por vía interpretativa con base en el marco normativo recién inaugurado.

Cómo citar: Miñarro Yanini, M. (2019). La «Carta de derechos digitales» de los trabajadores ya es ley: menos claros que oscuros en la nueva regulación. *Revista de Trabajo y Seguridad Social. CEF*, 430, 5-14.