

EL DERECHO A LA VIDA PRIVADA DEL TRABAJADOR EN EL TRIBUNAL EUROPEO DE DERECHOS HUMANOS: ¿DIÁLOGO O CONFLICTO CON LA JURISPRUDENCIA NACIONAL?

CRISTÓBAL MOLINA NAVARRETE

Catedrático de Derecho del Trabajo y de la Seguridad Social

Universidad de Jaén

“(…) tengo la impresión de que existe, y he intentado mostrarlo, una perpetua articulación del poder sobre el saber y del saber sobre el poder. No basta decir que el poder tiene necesidad de este o aquel descubrimiento, de esta o aquella forma de saber, sino que ejercer el poder crea objetos de saber, los hace emerger, acumula informaciones, las utiliza. (…). El ejercicio del poder crea perpetuamente saber e, inversamente, el saber conlleva efectos de poder”

M. FOUCAULT. “Entrevista sobre la prisión: El libro y su método”, en *Microfísica del Poder*. ed. La Piqueta. Madrid.1980, p. 99.

EXTRACTO

Palabras Clave: privacidad del trabajador, control tecnológico empresarial, ciudadanía digital

El Tribunal Europeo de Derechos Humanos (TEDH) ha experimentado una notable evolución en su jurisprudencia sobre la protección de la vida privada del trabajador en la empresa, dotándolo de un sentido social expansivo. La doctrina constitucional y la jurisprudencia social españolas mantienen, sin embargo, una posición más favorable a la defensa del poder de control tecnológico empresarial. Consecuentemente, asistimos a un evidente conflicto entre estos diferentes niveles jurisdiccionales que requiere corrección, si bien el Tribunal Supremo español parece resistirse a ello. El resultado es una extrema desazón interpretativa y una extremada inseguridad jurídica. El legislador español parece que, esta vez sí, pronto tomará cartas en el asunto convirtiendo en palabra de ley la palabra del TEDH

ABSTRACT

Key Words: worker privacy, business technology control, European Court of Human Rights, digital citizenship

The European Court of Human Rights (ECHR) offers a remarkable evolution in its legal cases on the protection of the worker's privacy, giving it an expansive social meaning. However, the Spanish constitutional doctrine and social jurisprudence maintain a more favorable position to defend the power of corporate technological control. Consequently, we are witnessing an evident conflict between these different jurisdictional levels. This judicial tension creates legal loopholes and contradictions, which require correction. However, the Spanish Supreme Court seems to resist rectification. The result is extreme interpretative distress and extreme legal uncertainty. The Spanish legislator seems that, this time, he will soon take up the matter by converting the word of the ECHR into a word of law.

ÍNDICE

1. INTRODUCCIÓN: CEDH, UNA LEY “RUDIMENTARIA”, TEDH, UNA JURISPRUDENCIA ABANDERADA
2. EL “MÉTODO (JUDICIAL) ENSAYO Y ERROR?”: UN ESCENARIO COMPLEJO E INCIERTO EN ESPERA DE NORMA ESPECÍFICA
3. EVOLUCIÓN JURISPRUDENCIAL DEL TEDH: APERTURA HACIA LA DIMENSIÓN SOCIAL DE LA PRIVACIDAD EN EL TRABAJO
 - 3.1. Planteamiento general: dinamismo y carácter expansivo de la protección de la privacidad del trabajador por TEDH
 - 3.2. Una historia de garantías en 7 hitos: breve recorrido por las sentencias del TEDH en materia de protección de la vida privada de los trabajadores
4. IMPACTO DE LA EVOLUCIÓN DEL TEDH EN LA JURISPRUDENCIA NACIONAL: DE LA “INVOLUCIÓN” A LA “INCERTIDUMBRE”
 - 4.1. La función jurisprudencial de suplencia legislativa en la fijación de límites al poder de control empresarial: del estancamiento a la involución
 - 4.2. Neutralización teórica nacional del plus de protección práctico europeo: el persistente contrastes entre la doctrina judicial y la jurisprudencial
5. IMPACTO DEL TEDH EN EL LEGISLADOR PROYECTADO: LA CARTA DE “CIUDADANÍA LABORAL DIGITAL RESPONSABLE”
6. LECTURAS SOCIALES “INDIRECTAS” DE LA JURISPRUDENCIA CIVIL DEL TEDH SOBRE PRIVACIDAD
7. EPITOME: EN BUSCA -PERMANENTE- DEL JUSTO EQUILIBRIO

1. INTRODUCCIÓN: CEDH, UNA LEY “RUDIMENTARIA”, TEDH, UNA JURISPRUDENCIA ABANDERADA

Que nuestro tiempo atestigua una época de notables cambios político-normativos en el ámbito de la protección de la privacidad de las personas, fuera y dentro de su trabajo, es un tópico jurídico o lugar común hoy, fuertemente marcado por la creciente y desbordante “huella digital” de la ciudadanía de nuestros días, al menos en los países desarrollados. En el ámbito de la Unión Europea, bastaría para confirmarlo el impacto innovador, en parte real y en parte (más bien) pretendido, de la reciente entrada en vigor del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril, 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 (Reglamento general de protección de datos -RGPD-). Su artículo 88 reclama la atención sobre la necesidad, no ya sólo la conveniencia, de que esa renovación legal general implique un imponente desarrollo específico, legislativo y convencional, en el ámbito de las relaciones de trabajo para cada Estado miembro. Naturalmente, si reclama este

movimiento regulador específico socio-laboral es porque, a día de hoy, no puede verificarse en la práctica totalidad de los sistemas y experiencias europeos¹.

Sobre esos desarrollos de modernización legislativa, acorde con las mutaciones de la realidad de las relaciones comunicativas personales y sociales, e incluso antes, a través incluso de la solidificación de diversos y específicos derechos fundamentales civiles (de libertad), como el derecho al respeto de la vida privada y familiar (art. 7 de la Carta de Derechos Fundamentales de la Unión Europea -CDFUE-) y el derecho a la protección de datos personales (art. 8 CDFUE), el TJUE, máximo órgano de garantías judiciales de la UE, ha podido desplegar una importante actividad protectora. Puesto que no es el objeto específico de nuestro artículo, bastará con reseñar aquí sólo algunas, para ilustrar el fuerte protagonismo jurisprudencial en la protección de la privacidad de las personas en el actual entorno de transformación tecnológica (especialmente digital). Por ejemplo, la que sin duda es la sentencia del TJUE más conocida de los últimos años, la sentencia *Google Spain (2014)*, relativa al “derecho al olvido en Internet”, cuya novedad fue relativizada por el TJUE, frente al Abogado General, al entender que no precisaba un desarrollo legal para comprenderlo en las garantías del art. 8 CDFUE.

Algunas de sus afirmaciones son muy relevantes para comprender donde radican los nuevos riesgos para la privacidad de las personas en la era digital. Esos peligros no estarían ya sólo, ni tanto, en el “conocimiento” de datos que afectan a lo más persona de nuestras vidas, pues nosotros mismos los “exhibimos” a menudo, sino más bien en la capacidad que tienen los actuales dispositivos digitales (motores de búsqueda) para la “organización y...agregación de la información publicada en Internet”. A partir de esa reconstrucción cumulativa crearía “una visión estructurada de la información relativa a esta persona que puede hallarse en Internet que les permita establecer un perfil más o menos detallado del interesado» (apartados 37 y 38). Por eso, incluso «...un tratamiento inicialmente lícito de datos exactos puede devenir, con el tiempo, incompatible con dicha Directiva cuando estos datos ya no sean necesarios en relación con los fines para los que se recogieron o trataron». Una vez más, pues, emerge la trascendencia del “fin” (*V. Ihering*) para el juicio de valoración de la licitud jurídica de las conductas.

Así lo habría asumido también recientemente, respecto de ese mismo derecho (hoy art. 17 RGPD), la STCO 58/2018, 4 de junio, que declara vulnerados el derecho al honor e intimidad (art. 18.1 CE) y a la protección de sus datos personales (art. 18.4 CE), por el uso de nombres propios como criterio de búsqueda y localización de noticias en una hemeroteca digital, revocando parcialmente el pronunciamiento contrario de la Sala 3ª del TS. Ahora bien, sí realiza un análisis muy minucioso y ponderado respecto del juicio de proporcionalidad, matizando y

¹ Por todos, vid. Miñarro Yanini, M. “La «Carta de derechos digitales» para los trabajadores del Grupo Socialista en el Congreso: un análisis crítico ante su renovado interés”, RTSS-CEF, n. 424, julio 2018.

precisando el alcance de su decisión, porque "...a la hora de valorar el sacrificio requerido a la libertad de información..., para asegurar el disfrute adecuado del derecho a la intimidad...en conexión con el derecho a la autodeterminación informativa... es necesario recordar la importancia de las hemerotecas digitales en el contexto de las actuales sociedades de la información”.

La evolución cultural y el cambio de la realidad tienen una gran incidencia en ese juicio, que ha de ser muy ponderado por estar en juego otros derechos y libertades fundamentales. Actividades tan cotidianas otrora como la “predicación puerta a puerta”, que hacen determinadas comunidades religiosas y que se ampararían en otras libertades fundamentales (de conciencia y religión, por ej., ex art. 10 CDFUE), también quedan sometidas a las normas de protección de datos personales (STJUE de 10 de julio de 2018, asunto C-25/17, que cita jurisprudencia del TEDH sobre la libertad religiosa), evidenciando su “voracidad” o predominio. Entroncarían de esta forma la precedente doctrina (STJCE 6 de noviembre de 2003, *Lindqvist*, C-101/01) con la nueva

Justamente, esta jurisprudencia está trufada, desde sus orígenes, de la necesidad de contemperar la protección de la vida privada de las personas en general, y de sus datos en particular, sobre todo en los nuevos escenarios de la transformación digital, con la propia vida efectiva de los demás derechos y libertades fundamentales en juego, personales y de índole económica (libertad de circulación de datos), preconizando una solución típica de “*justo equilibrio entre los derechos e intereses en juego*, incluidos los derechos fundamentales tutelados por el ordenamiento jurídico comunitario» (apartado 90). En el caso concreto, el TJCE entonces, como el TCO ahora, centrará la decisión en:

«...ponderar, por una parte, la libertad de expresión de la Sra. Lindqvist en el marco de su trabajo como catequista, así como la libertad de ejercer actividades que contribuyen a la vida religiosa y, por otra parte, la tutela de la intimidad de las personas cuyos datos incluyó la *Sra. Lindqvist* en su sitio Internet» (STJCE de 6 de noviembre de 2003, *Lindqvist*, C-101/01, apartado 86).

Pero el objeto de este estudio no es ni el Derecho de la UE en materia de tutela de la privacidad en general, y de los datos personales en particular, ni el papel del TJUE en el progreso de esa protección, a luz de las nuevas realidades y normas. Aquí nos centraremos en el análisis de la influencia que, para la protección de una esfera de vida privada efectiva de la persona en el seno de las relaciones de trabajo, está teniendo el Tribunal Europeo de Derechos Humanos (TEDH), como órgano máximo de garantías jurisdiccionales del Derecho del Consejo de Europa, muy en particular de esa “carta europea de derechos humanos civiles” tan relevante como es el “viejo” (1950) Convenio Europeo para la Protección de los Derechos Humanos (CEDH). Sin embargo, ni CEDH especifica la protección para los datos personales (su artículo 8 se limita a reconocer y garantizar el derecho genérico y en su versión más clásica), ni la evolución posterior del Derecho

del Consejo de Europa en materia ha sido tan intensa jurídicamente como la de la UE, sin desmerecer una norma tan influyente -también en el Derecho de la UE- como el Convenio 108 de protección de datos (1981) -se ratificó por España en 1985- (20 años después se firmó su Protocolo Adicional relativo a las autoridades de control y a los flujos transfronterizos de datos, 2001). Ahora bien, a diferencia de la UE, el Consejo de Europa prefirió una senda de progreso mediante “recomendaciones sectoriales”, por tanto, sin fuerza jurídica vinculante, y para aspectos específicos, cierto, incluyendo el entorno laboral (*Recomendación relativa al tratamiento de datos personales en el entorno laboral de 2015*, que sustituye a la precedente de 1989).

Superando plenamente estas carencias, deficiencias e imprecisiones normativas, tanto de su fuente “constitucional” originaria como de sus posteriores desarrollos, no hay ninguna duda sobre la absoluta “autoridad de liderazgo europeo” del TEDH en materia de protección del derecho a la vida privada, incluyendo específicamente una importante zona de reserva o garantía de la misma en la esfera laboral ex art. 8 CEDH. Tanto el TJUE como los Tribunales Constitucionales nacionales (para el caso español la sentencia que se acaba de citar es un claro ejemplo) reconocen esa preeminencia, con constantes remisiones a la norma convencional europea y a la jurisprudencia del TEDH. La garantía del derecho genérico al respeto de la privacidad de la persona -así como a la correspondencia (objeto de estudio específico en este monográfico)- habría bastado no ya sólo para convertir la jurisprudencia del TEDH en abanderada de la evolución en un sentido expansivo de aquél derecho, sino para integrar plenamente en su contenido una significativa tutela, teórica y práctica, del derecho a la protección de datos personales. También en virtud de la influencia del referido Convenio n. 108 del Consejo de Europa, el TJEU habría hecho de la protección de los datos personales un ariete fundamental para progresar en la efectividad práctica del ejercicio del derecho humano al respeto de la vida privada en todas las facetas de la vida de una sociedad democrática (artículo 8 CEDH), incluida la laboral, dotándolo en este ámbito de obligaciones positivas (deberes de hacer), tanto a cargo de los Estados como de los propios particulares, no sólo de obligaciones negativas (deberes de respeto)

En definitiva, no ha necesitado el TEDH de profundos desarrollos legislativos en el seno del Consejo de Europa para llevar más lejos que ningún otro nivel jurisdiccional europeo la protección de la vida privada, sino que le ha bastado la integración de esas evoluciones (internacionales y nacionales) en su más clásica jurisprudencia sobre conceptos y principios generales: expectativas razonables de intimidad; deberes de transparencia en el ejercicio de los poderes de investigación -también digital-; juicio de proporcionalidad o principio de justo equilibrio².

² Vid. STEDH, de 16 de julio de 2013, *Wegrzynowski y Smolczewski c. Polonia* (recurso 33846/07). En la misma línea, la STJCE (Gran Sala), 16 de diciembre de 2008, (C-73/07), donde protege especialmente la actividad periodística, garantía de la sociedad democrática.

Como es lógico, lo que esta técnica jurídica gana en apertura a la innovación en virtud de los cambios de la realidad y de las pautas axiológico-culturales lo perdería en certidumbre y previsibilidad sobre las decisiones de los crecientes casos planteados. Así lo prueban ciertos “vaivenes” (ek- caso *Barbulescu I v. II*) y la proliferación de votos particulares (ej. Caso *López Ribalta*)

Precisamente, y situados en un *sistema multinivel de protección europea del derecho a la vida privada de los trabajadores*, en cuanto personas y ciudadanos, resulta de todo punto llamativo desvelar una profunda contradicción en el mismo. Mientras que existe una significa convergencia en el nivel de protección de este derecho en el plano normativo y entre jurisprudencias de la máxima autoridad europeas, utilizándose de forma recíproca para perfeccionar, al hilo del cambio real y normativo, el efecto útil o la efectividad de la tutela del derecho, hallamos un fuerte contraste entre la jurisprudencia del TEDH y los niveles jurisdiccionales máximos nacionales a la hora de delimitar, de una forma concreta y práctica, no general y abstracta, el sentido y los límites de aquel derecho. En otros términos, si cabe constatar un fértil diálogo entre las jurisprudencias de ambos niveles máximos de jurisdicción europea relativa a la protección del derecho a la vida privada, este estado dialógico y armónico del arte jurisprudencial europeo muta en conflicto agudo con los niveles nacionales de máxima autoridad -y en plena sintonía, en cambio, con los votos particulares de esa posición nacional mayoritaria³.

Paradójicamente, mientras que el TC y, sobre todo, el TS (ej. STS, 4ª, 119/20188 de febrero) tratan de relativizar ese contraste, sobre la base de una comparación sólo formalista o puramente instrumental abstracta, los niveles inferiores del orden social de la jurisdicción, juzgados y salas de suplicación, tienden a evidenciar que sí existe ese contraste y optan por dar preferencia, en virtud del art. 96 CE, a la posición del TEDH. No obstante, para añadir mayor complejidad y también incertidumbre al panorama, ya de por sí confuso e inestable, procuran en sus decisiones que la interpretación no resulte extremadamente disruptiva entre unos niveles (europeo) y otros (nacional supremo y nacional constitucional), buscando un, difícil, equilibrio, que suele saldarse, a diferencia de lo que es más frecuente en el nivel de la jurisdicción suprema, con el reconocimiento de protección a la vida privada, incluso con una componente “social”, del trabajador y, por lo tanto, en detrimento del poder de control empresarial -aunque resulte justificado, pero no proporcionado-. En consecuencia, resultar de gran interés hoy, en espera de futuros y proyectados desarrollos legislativos, realizar un análisis actual de estas situaciones de diálogo y conflicto entre la jurisprudencia del TEDH en materia de protección de la vida privada del trabajador en sus relaciones con la empresa y los más diversos niveles de la justicia nacional al respecto, tanto ordinaria como constitucional.

³ Vid. Casas Baamonde, M.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?...*”. Editorial Derecho de las Relaciones Laborales, n. 2/2018, pp. 103-121.

2. EL “MÉTODO (JUDICIAL) ENSAYO Y ERROR?”: UN ESCENARIO COMPLEJO E INCIERTO EN ESPERA DE NORMA ESPECÍFICA.

El contraste entre la acelerada transformación de la realidad y la lenta adaptación legislativa es otro tópico jurídico, especialmente cierto en relación a la regulación de la protección de la vida privada de las personas en una sociedad dada a la “información” y a la “transparencia” (*Byung-Chul Han*⁴), así como al “exhibicionismo” (U. Ecco), en la que más que tener cuenta “aparecer”. Aunque el referido RGD comunitario pretende recuperar una cierta armonización, por razones ambivalentes, esto es, optimizando las razones de protección de la privacidad (alma humana) y las de promoción del flujos de datos en un mercado interior, a fin de no perjudicar uno de los nuevos negocios de mayor rentabilidad del presente y del futuro inmediato (alma económica), sus limitaciones, tanto generales como sectoriales, siguen siendo manifiestas, más aún en el ámbito de las relaciones de trabajo, donde, como se dijo, la regulación específica y de equilibrio nacionales-legislativa y convencional- ha sido anunciada, incluso promovida, pero sigue en espera. El problema se agrava porque a más crece la rentabilidad de esta línea de negocio (la información personal procesada digitalmente -Big data- todavía se produce a coste 0 de la “materia prima” con un exponencial margen de beneficio), más riesgos de usos desviados, intensificando los flujos sin autorización real (consentimiento libremente informado ex art. 9 RGD).

Si tanto el “exhibicionismo voluntario de datos personales” como el tratamiento informatizado de los mismos genera un “saber” sobre las personas que otorga un mayor “poder” de adoptar decisiones (ej. “*micro-targeting mercado-técnico*” o uso de los datos de un consumidor potencial para influir en sus decisiones), tal reforzamiento digital conllevará la mayor vulnerabilidad para las personas sometidas a él, particularmente de los trabajadores, por ser “sujetos de disciplina”. La vigilancia digital permite adelantarse a los actos de las personas “señaladas”, permite “dominarlas”, no ya sólo controlarlas. De ahí que junto al discurso sobre sus “oportunidades de mejora”, tienda a imponerse, el de los “usos de riesgo” para la privacidad de las personas (también para su salud), esto es, “usos tóxicos” del creciente “rastreo digital” que creamos, por nuestra decisión y/o a través de dispositivos digitales que otros utilizan para recabar información plena.

La actualidad está salpicada de escándalos que se asocian con la violación de la privacidad en virtud de los nuevos “dispositivos de saber-poder tecnológico” (propios de una era panóptica digital). El problema no sería tanto, o no sería sólo, el flujo de información que permiten, sino más bien sus “usos cumulativos” y

⁴ Vid. Byung-CHul, Han. *La sociedad de la transparencia*. Barcelona, Herder Editorial, 2013. Una breve crítica de su obra en Adolfo Vásquez Rocca. https://rinabrundu.com/2015/12/15/byung-chul-han-la-sociedad-de-la-transparencia-psicopolitica-neoliberal-exitismo-patologico-y-cansancio-en-el-enjambre/#_ftn8

“retrospectivos”, pues además de recrear un perfil personal total, como se decía, permite guardarlo mucho tiempo lo que, en sí mismo, es un grave riesgo para la privacidad, porque se acumulan y permanecen invisibles hasta que emergen con una virulencia social difícil de frenar. En consecuencia, el nuevo contexto de la empresa digital y sus desarrollos vertiginosos están replanteando el alcance y límites recíprocos entre los derechos fundamentales de la persona⁵, no sólo el respeto de la privacidad, aquí objeto de análisis, y las mejoras de eficiencia (también de disciplina) de los poderes, públicos y privados, por supuesto también empresariales (de gestión y de control) que el saber digital crea. Al respecto, conviene tener bien presente que no solo se trata de adelantos tecnológicos sino de situaciones de poder que plantean nuevas relaciones sociales y contractuales, por lo que su afrontamiento “gota a gota”, “caso a caso”, y del método “ensayo-error”, dificulta de forma notable su gobierno, de ahí la recurrente llamada a políticas de uso socialmente razonable de estos dispositivos en las empresas, a poder ser negociados.

Al igual que los Gobiernos (unos más abiertamente que otros), están creando un tipo de sistema de control total de sus ciudadanos (se registra, califica y valora cada una de las acciones de sus ciudadanos -súbditos-), a través de “listas de crédito-reputación social” (el ejemplo más claro es el sistema “bonus-malus” social del Gobierno chino⁶), las empresas tienden a un tipo de “saber-poder” análogo, para mejorar tanto su control (vigilar mejor para castigar más eficazmente) como sus rendimientos (mejorar tanto sus capacidades -productividad- como su disponibilidad -compromiso-). Si el “Big Brother” (Gran Hermano) de Orwell y el Panóptico de Bentham describían un control físico de la población de este tipo (sujeción a una serie de normas y vigilancia de todo lo visible), se quedaba extramuros el “pensamiento”, el “panóptico digital” es una forma de control más eficiente porque apenas tiene ángulos muertos, alcanzar la psique, de modo que “*trabajando con las emociones (compromiso psicológico) influye en las acciones*”⁷

Por eso, en la era digital, la garantía de efectividad de la vida privada de las personas en general, y de los trabajadores en particular, no sería sólo un derecho fundamental de la personalidad (vertiente individual), sino que constituiría, al tiempo, una misión pública necesaria para garantizar una sociedad realmente

⁵ Vid. Tascón López, R. “*Tecnovigilancia empresarial y derechos de los trabajadores*”. RTSS-CEF, n. 415, octubre 2017, pp. 53 y ss.

⁶ Vid. Veliz, Carissa, https://elpais.com/tecnologia/2018/04/06/actualidad/1523030681_007734.html.

⁷ Vid. Byung-Chul, Han. *Psicopolítica. Neoliberalismo y nuevas técnicas de poder*, Herder Editorial, 2014, p. 86. Sigue así una línea propia de la “microfísica del poder” propia de M. Foucault, si bien trata de dar por superada su “sociedad disciplinaria” por otra “sociedad del rendimiento”, donde el control sería mayor por la aceptación subjetiva de la dominación. Para la centralidad del debate saber-poder vid. Foucault, M. *Vigilar y castigar. Nacimiento de la prisión*, Editorial Siglo XXI. Madrid, 2008

libre y democrática (vertiente general o colectiva). Una dimensión general que, como ningún otro Tribunal, ha comprendido, y practicado, el TEDH, para el que, en coherencia con la previsión del art. 8.2 CEDH⁸, el respeto a la privacidad *no sólo tiene una dimensión social*, que luego analizaremos en detalle en su garantía laboral, *sino que constituiría un imperativo general (común) de democracia y de libertad*. Como veremos, esta construcción teórica del derecho fundamental no es baladí para el juego práctico de sus límites en el ámbito laboral, desde el momento en que permite reforzar platillo de la balanza propio del trabajador inclinando el fiel a su favor por estar en juego “bienes comunales” o “colectivos”, no sólo particulares, salvo que haya un interés muy preciso del empleador y el sacrificio que exija del derecho del trabajador sea el menor posible: “*El mito de que la privacidad es un lujo reservado a pudorosos es falso. Quien salvaguarda su privacidad no está anteponiendo su interés personal de manera egoísta, sino que está protegiendo el bien común: la seguridad de todos y la democracia*”⁹

Esta protección de valores democráticos, especialmente puestos en riesgo por el poder tecnológico, lleva al TEDH a colocar a la persona en el centro de imputación de normas de garantía, no el poder público -sujeto principal de obligaciones (negativas y positivas)-, ni a la empresa, por ser el núcleo duro de una “Constitución (material o axiológica) civil Europea”. Sin necesidad de identificar en el art. 8 CEDH un genuino derecho de protección de datos, hace del derecho genérico a la vida privada no sólo un bastión blindado al conocimiento ajeno (vertiente negativa) sino también una fuente de poder de gobernar los usos de las informaciones que le conciernan (vertiente positiva). De ahí que lo transforme en un valor central de la “libertad ciudadana informada” en la sociedad de la comunicación, exigiendo o *consentimiento o información previa útil*.

A falta de una “carta de derechos civiles de ciudadanía digital”, el TEDH hace del art. 8 CEDH no sólo una fuente de límites al “poder-saber tecnológico” -de sujetos públicos y de sujetos privados, en particular empleadores-, sino una fuente integradora de obligaciones a cargo de los mismos, en aras de un “saber-contrapoder informativo” también para las personas, a nuestros efectos para los trabajadores. Con carácter general, la STC 196/2004, de 15 de noviembre, sintetiza la doctrina del TEDH en torno a la extensión y límites de esta faceta del derecho a la vida privada de la persona como un poder autónomo de decisión sobre los datos que le conciernen, no sólo del nivel de conocimiento de esas esferas de vida propia, sino de los flujos de la información disponible sobre ella

⁸ Recuérdese que se dijo que el TEDH (14 de febrero de 2008) y el TJUE (5 de octubre de 2010) asumen un contenido equivalente entre el art. 8 CEDH y el art. 7 CDFUE.

⁹ Un sugerente análisis desde esta visión más institucional y colectiva en la citada Carissa VELIZ. “*Tus datos son tóxicos*”. https://elpais.com/tecnologia/2018/04/06/actualidad/1523030681_007734.html. Pero, sin ninguna duda, quien mejor ha fundamentado jurídico-filosóficamente esta dimensión institucional y política del derecho a la vida privada, en su moderna dimensión de protección de datos, es Rodotà, S. *Democracia y protección de datos*. Cuadernos de derecho público, Nº 19-20, 2003

y de los usos que, por lo tanto, puedan hacerse de ella (derecho de control sobre datos referidos a la persona que, habiendo ya salido de la esfera de la intimidad, se convierten en piezas de un archivo -electrónico o no-). Por lo tanto, se pone en evidencia la estrecha conexión entre la protección de datos y el respeto a la vida privada, cubriendo la laguna del CEDH en esta materia, confirmando el rigor de la serie de límites al poder potencialmente invasivo de la vida privada¹⁰:

a) los límites deben estar establecidos por ley

b) que esta ley sea accesible a la persona concernida y resulten previsibles sus consecuencias (transparencia). No podrá regularlos de forma vaga o imprecisa).

c) resulten indispensables en una sociedad democrática para el logro de fines de esta naturaleza, respetando las condiciones del juicio de proporcionalidad útil

De ahí que sea notablemente apreciable la evolución desde un tiempo analógico o pre-digital al tiempo informático y, hoy, al digital propiamente, por lo que la inquietud por proteger la vida privada de las personas frente a los riesgos creados por cada nuevo dispositivo tecnológico tiene una notable presencia en la jurisprudencia del TEDH, que ha ido adaptándose progresivamente a esos requerimientos. Ciertamente, con dificultades.

En efecto, los “dispositivos tecnológicos” y los límites de sus usos no siempre son, más cuando falta una legislación específica -incluso cuando no está presente la ley-, adecuadamente entendidos por los Tribunales. De ahí, que resulte una genuina máxima de experiencia, registrable, en una mayor o menor medida, en todas las experiencias jurídicas occidentales (de especial interés comparativo el caso norteamericano -el TS de EEUU asienta también su jurisprudencia sobre el concepto de “expectativa legítima de privacidad del ciudadano”), el progreso no lineal, sino de decantación gradual y sentido equívoco, con notables rectificaciones y la perpetuación de zonas de sombra¹¹. En suma, el protagonismo jurisprudencial en esta materia, que siempre se resuelve en un juicio ponderativo, medie o no legislación adaptada, más activista o menos según sí exista o no aquella regulación (legal o convencional, para el caso laboral), resulta inexorable, pero tiene sus costes, en términos de complejidad e incertidumbre (imprevisibilidad).

¹⁰ En esta visión expansiva del derecho (garantía de efectividad) y restrictiva del límite (mínimo sacrificio) coincide con la jurisprudencia comunitaria: STJUE 11 de diciembre de 2014, sentencia Ryneš, C-212/13, Apartado 28. En esta misma lógica convergente entre el TJUE y el TEDH, desde el primado de éste, el TJUE mantiene un concepto de vida privada en sentido amplio: «es irrelevante el hecho de que los datos publicados se refieran a actividades profesionales» (STJUE, Gran Sala, 9 de noviembre de 2010, C-92/09 y C-93/09, Apartado 59). Una necesidad de ponderación ajustada y concreta, no abstracta, primando el derecho individual sobre intereses de alcance general, que también está en la STJUE, Gran Sala, de 8 de abril de 2014, Digital Rights Ireland, C-293/12 y C-594/12: «...antes de divulgar información sobre una persona física, las instituciones están obligadas a poner en la balanza, por una parte, el interés de la Unión en garantizar la transparencia de sus acciones y, por otra, la lesión de los derechos reconocidos en los arts. 7 y 8 de la Carta. Ahora bien, no cabe atribuir una primacía automática al objetivo de transparencia frente al derecho a la protección de los datos de carácter personal [...] ni siquiera aunque estén en juego intereses económicos importantes» (apartado 85).

¹¹ Vid. Ordoñez Solís, D. *La protección de los derechos fundamentales en Internet en la jurisprudencia europea*, Editorial Reus, Madrid, 2014.

Los Tribunales suelen ser conscientes de esta dificultad, de ahí que anhele una legislación que les alivie la decisión. Paradigmática la sentencia *Ontario v. Quon* (560 US, 17 de junio de 2010) del Tribunal Supremo estadounidense (requerido para resolver si se vulneró o no la privacidad de unos mensajes de texto descubiertos de modo fortuito por el Departamento municipal de policía cuando investigaba las razones de una elevada factura del servicio telefónico de sus agentes). La mayoría, expresada por el juez Kennedy, reflexionaba sobre las dificultades del reto:

“El Tribunal debe proceder con cuidado al considerar la totalidad del concepto de expectativas de privacidad en las comunicaciones realizadas a través de equipos electrónicos que pertenezcan al Gobierno en su calidad de empleador. El poder judicial se arriesga a cometer errores [...] al elaborar una doctrina demasiado detallada de las implicaciones en la Cuarta Enmienda de la tecnología emergente antes de que su función en la sociedad se haya revelado con claridad”

No obstante, el voto concurrente del juez *A. Scalia* advierte:

«...aplicar la Cuarta Enmienda a las nuevas tecnologías puede ser en ocasiones difícil, aunque cuando es necesario decidir un caso no nos queda otra elección [...] Que los tiempos están cambiando es una débil excusa para evadirnos de nuestro deber».

Prácticamente una década después, y por razones parcialmente coincidentes y otras específicas, como veremos, buena parte de los niveles inferiores de la jurisdicción social española tienen una misma percepción de complejidad e incertidumbre del estado del arte interpretativo en esta materia. Sin perjuicio del análisis más detenido que se hará en el lugar oportuno de este estudio, merece la pena traer a colación la percepción que tiene la sala de suplicación castellano-manchega, de la situación jurisprudencial actual sobre los límites de la facultad empresarial de control de la conducta de los trabajadores a través de sistemas tecnológicos (en el caso video vigilancia). A su juicio, “no existe una respuesta consolidada, probablemente debido a la escasa regulación legal en esta materia, lo que ha dado lugar a una jurisprudencia y doctrina constitucional ciertamente vacilante, si no discordante a última hora”. De ahí que señale un panorama especialmente “incierto” y llamado a “revisión” para armonizarse con la nueva doctrina del TEDH (STSJ C-LM, 25/2018, 12 de enero, Rec. 1416/2017).

Veamos brevemente cómo se ha llegado a esta incierta situación. Para ello, se analizará primero, de forma sintética, la evolución de la doctrina del TEDH, para, después, hacer lo propio con la doctrina del TC y la jurisprudencia nacional. Finalizaremos con un análisis de contraste entre los diversos niveles jurisdiccionales que intervienen en este sistema complejo de protección del derecho a la privacidad de los trabajadores frente a los poderes empresariales de control tecnológico (hoy cada vez más digital, pero no sólo), a fin de intentar ensayar una vía de salida más dialógica para tan conflictiva y disfuncional situación en una materia de tanta trascendencia social.

3. EVOLUCIÓN JURISPRUDENCIAL DEL TEDH: APERTURA HACIA LA DIMENSIÓN SOCIAL DE LA PRIVACIDAD EN EL TRABAJO

3.1. Planteamiento general: dinamismo y carácter expansivo de la protección de la privacidad del trabajador por TEDH

Históricamente, el TEDH ha venido defendiendo que la noción de “vida privada” es un “concepto amplio que no se presta a una definición exhaustiva”, a fin de garantizar un espacio de reserva y autonomía personal frente a cualquier inferencia no consentida de terceros, públicos o privados. Consecuentemente, no puede reducirse ese concepto a la clásica idea de “intimidad” o “esfera íntima” (STEDH 16 de diciembre de 1992, asunto *Niemietz contra Alemania*), sino que tiene una moderna dimensión social:

“...considera que sería demasiado restrictivo limitar la noción de “vida privada” a un “círculo íntimo” en el que cada uno pueda vivir su vida personal como quiera y excluir completamente al mundo exterior de este círculo. Así, el artículo 8...incluye el derecho a realizar una “vida privada social”, es decir, la posibilidad de que el individuo desarrolle su identidad social. A este respecto, el mencionado derecho consagra la posibilidad de comunicarse con otros para establecer y desarrollar relaciones con sus semejantes...” (STEDH, Gran Sala, de 5 septiembre 2017, *Barbulescu II*, apartado 70)

Pues bien, una vez admitida, de forma relativamente temprana (1997), la protección de la vida privada del trabajador en el marco del art. 8 CEDH, supliendo la falta de tratamiento específico al respecto en gran parte de legislaciones nacionales¹², el TEDH también le hace partícipe de esa tradicional y constante vis expansiva. No cabe duda, pues, de esta evolución garantista del TEDH, de modo que ha venido ampliando progresivamente, no sin constantes discrepancias en su seno, el ámbito de protección jurídica de las personas trabajadoras. A tal fin, el TEDH acota no sólo un espacio de obligaciones negativas, de respeto o reserva (típica garantía “liberal”) sino también de obligaciones positivas, de hacer (“garantía social”).

Por supuesto, el TEDH no desconoce en modo alguno la especificidad de las relaciones de trabajo. Al contrario, asume que tiene características específicas que se deben tenerse en cuenta a la hora de hacer el juicio ponderativo, porque la relación entre una empresa y empleado sería una relación contractual integrada derechos y deberes “especiales” y caracterizada por “una relación de subordinación”. De ahí que tenga “su propio sistema jurídico, que es claramente distinto del sistema general de relaciones entre individuos” (STEDH 12 de enero

¹² Como destaca la sentencia *Barbulescu II*: “únicamente Austria, Finlandia, Luxemburgo, Portugal, Reino Unido y Eslovaquia tratan la cuestión del ejercicio de la vida privada en el lugar de trabajo de una manera explícita, ya sea como parte de la legislación laboral, ya sea mediante leyes especiales” (ap. 52)

de 2017, *Saumier c. Francia*, reclamación núm. 74734/14, ap. 60). El TEDH, en línea con el RGPD comunitario, acepta que, desde un punto de vista normativo, la legislación laboral cuente con mayor margen para la “negociación contractual” al ahora de fijar el contenido de sus relaciones, asumiendo la legitimidad de ciertos controles empresariales que, fuera de la relación laboral, requiere autorización judicial. Habría que recordar su interesante doctrina sobre la legitimidad de los controles de detección de consumos de drogas en las empresas, como una central nuclear (*STEDH 9 de marzo de 2004, Wretlund c. Suecia, reclamación 46210/99*)

Desde esta perspectiva de mayor flexibilidad del tratamiento de la privacidad en el ámbito de las relaciones de trabajo, y constatando una política legislativa del Derecho del Trabajo mayoritariamente abstencionista en torno a proveer de reglas específicas, así como la inexistencia de un marcado consenso en torno a las soluciones, el TEDH otorga “un amplio margen de discrecionalidad para valorar la necesidad de adoptar un marco jurídico que establezca las condiciones en las que una empresa puede adoptar una política que regule las comunicaciones no profesionales, electrónicas u otro, de sus empleados en su lugar de trabajo” (sentencia *Barbulescu II*, apartado 118). Pero, claro está, libertad reguladora y flexibilidad decisoria no puede significar ni arbitrariedad ni abuso, por lo que, cualquiera que sea la concreción legislativa de las relaciones entre el derecho a la vida privada del trabajador y el poder de control empresarial, siempre se ha de garantizar que aquel derecho no resulte indebidamente sacrificado. Por lo tanto, siendo el TEDH igualmente consciente, como el TS norteamericano en el caso referido ut supra, “de que la situación está cambiando rápidamente en este ámbito” (sentencia *Barbulescu II*, apartado 120), concluye que “*la garantía proporcionalidad es elemento esencial*” para determinar la legitimidad del ejercicio del poder empresarial y el “justo equilibrio entre los intereses divergentes en juego”.

En el platillo del empleador, el TEDH viene reconociendo que la empresa tiene “un interés legítimo en garantizar el buen funcionamiento de la empresa”. Y para ello, ningún inconveniente debe haber para que el empleador aproveche las mejoras propias de los avances tecnológicos para crear dispositivos que “garanticen que sus empleados desempeñen sus funciones profesionales de manera adecuada y con la celeridad requerida”. En el platillo del trabajador, el TEDH insistirá en que el carácter laboral de la relación no puede hacer perder la esfera de protección razonable que aseguraría a toda persona el art. 8 CEDH. De ahí que, por una parte, haya acuñado el concepto de derecho al respeto de la “vida social privada” de la persona -por lo tanto también del trabajador-. Y, de otra, haya considerado insuficiente para validar el actuar empresarial de control con su “deber de transparencia”, esto es, de información específica de la actividad a desarrollar en el control y sus finalidades concretas a fin de delimitar el espacio de la “expectativa legítima de privacidad”. Aunque, como veremos con algún detalle ut supra, el TEDH recuerda que la expectativa razonable de protección de

la privacidad es “*un criterio importante*” (*una condición necesaria*), aunque “*no necesariamente decisivo*” (*una condición suficiente*) (STEDH 5 de octubre de 2010, Köpke c. Alemania).

En efecto, para el TEDH “las instrucciones de una empresa no pueden anular el ejercicio de la privacidad social en el puesto de trabajo” (sentencia Barbulescu II, ap. 80). Consecuentemente, ahora introduciría, de un lado, una prohibición de reducción absoluta de esa dimensión social de la vida privada en el seno de la relación de trabajo (ilegitimidad de la precedente opción empresarial de excluir todo uso no profesional de dispositivos propiedad de la empresa). De otro, un juicio de proporcionalidad mucho más concreto y útil para la vida práctica del derecho en la empresa, fundamental para hacer creíble el justo equilibrio, sin perjuicio de reforzar igualmente los típicos juicios previos de justificación (existencia de un fin legalmente previsto) y de transparencia informativa, clave para hacer efectivo el principio de confianza (buena fe) relacional¹³.

3.2. Una historia de garantías en 7 hitos: breve recorrido por las sentencias del TEDH en materia de protección de la vida privada de los trabajadores

Aunque ciertamente no son las únicas relevantes, sí que podría resumirse bien la historia de la jurisprudencia del TEDH en relación a la protección de la vida privada del trabajador, y su evolución garantista, no sin fuertes tensiones en su interior, en 7 hitos, en 7 “precedentes” o “casos jurisprudenciales” que permiten conocer de forma precisa cómo ha ido fijando aquella doctrina protectora en prácticamente en dos décadas. Así:

1ª) Caso Halford c. Reino Unido (25 de junio de 1997): *el deber de información previa sobre la política de uso de los dispositivos electrónicos como presupuesto de la expectativa razonable de tutela de la privacidad*.

Es el primer precedente referencial en la construcción originaria del juego de la privacidad del trabajador en el seno de la relación de prestación de servicios, eje sobre el que luego vertebrará toda la jurisprudencia nacional en la materia (cuatrienio 2007-2011). En ella se recoge toda la jurisprudencia general previa del TEDH, proyectándola al ámbito profesional, con lo que, al igual que el TS norteamericano, pondrá el acento en la protección de la esfera de la persona, no del lugar en el que se desenvuelve. La persona debe hallar protección de su identidad social, forjada a través del desarrollo de las distintas relaciones con otros, destacando la laboral, pues en ellas se juegan muchas oportunidades para fortalecer sus lazos con el mundo exterior (*caso Niemietz*, ap. 29).

¹³ El TEDH ha efectuado una síntesis de las resoluciones judiciales emitidas respecto de la cuestión relativa a la vida privada de los trabajadores en la prestación de servicios. Vid. ECHR. “*Surveillance atworkplace*”. https://www.echr.coe.int/Documents/FS_Workplace_surveillance_ENG.pdf

En este caso, y dada la fecha, el tipo de dispositivo tecnológico ante el que se defendía la vida privada era el teléfono. Como se recordará, en este caso, el TEDH dictaminó que hubo violación del art. 8 CEDH porque la trabajadora (policía) tenía una expectativa razonable de privacidad al habersele asegurado que el teléfono que utilizaba para comunicarse con su abogado era privado, esto es, tenía autorización de la empresa para usar el teléfono de su propiedad para usos particulares.

2ª) Caso Copland c. Reino Unido (3 de abril de 2007, queja 62617/00). Reafirma la doctrina Halford.

Una década después, constatados ya los efectos de la transformación digital que por entonces empezaba a cernirse sobre el mundo del trabajo igualmente, el TEDH tendrá la oportunidad de perfilar y consolidar la “doctrina Halford” en torno a cómo ha de entenderse la citada expectativa razonable de privacidad, ya respeto del conjunto de dispositivos digitales. En el caso, la profesora de un colegio público galés fue sometida a vigilancia total (llamadas telefónicas, correos electrónicos y conexiones a Internet). Para justificarla, la empresa invocó la necesidad de controlar el gasto público por lo que tenían que analizar las facturas de teléfono (donde constaban los números, fecha, hora y duración de las llamadas), las visitas a Internet y direcciones mail. El TEDH, tras cuidar de no deslegitimar en abstracto el ejercicio del poder de control empresarial, precisó sus condiciones de uso legítimo:

- Legitimidad del fin concreto perseguido, no meramente genérico (ejemplo: la defensa y prevención frente a infracciones de sus obligaciones por el trabajador)

- Información previa de la posibilidad de control

- Proporcionalidad de la medida de vigilancia, a fin de que sea razonable

No mediando la debida información, el poder devendría ilegítimo. Precisamente, por no tener esa expectativa razonable de privacidad, el TS norteamericano, pocos años después (citada sentencia Ontario v. Quon de 17 de junio de 2010) consideró que *no se había violado el derecho fundamental a la privacidad del agente de la policía de la ciudad californiana* que había sido sancionado disciplinariamente por el hecho de que, cuando las autoridades municipales revisaron las causas de una elevada factura telefónica, comprobaron que este policía utilizaba el teléfono del trabajo para remitir a otros compañeros mensajes de texto con contenidos eróticos. Esto es, hacía un uso desviado del dispositivo telefónico, proporcionado sólo para asuntos profesionales.

3ª) Caso Köpke c. Alemania (5 de octubre de 2010): *la vigilancia encubierta también es legítima, si resulta proporcionada por las circunstancias del caso.*

Como ya se anticipó, siendo la expectativa razonable de protección de la vida privada del trabajador una condición importante de legitimidad del control empresarial, delimitada en función de la información previa disponible por el tra-

bajador y a cargo del empleador, no es determinante, de modo que puede no ser ni una condición insuficiente para la legitimidad final, pero también puede dejar de ser una condición necesaria para tal valoración de licitud. En efecto, en el *caso Köpke*, una cajera -comienza la saga de este colectivo de profesionales- fue sometida a video-vigilancia por la sospecha de estar realizando hurtos en la empresa, sin que se le informara de la medida. Sorprendida en tales infracciones, fue despedida, sobre la base de las grabaciones. Los diversos niveles de la jurisdicción alemana que intervinieron declararon la procedencia del despido, desestimándose el recurso de amparo constitucional.

Para el TEDH, sobre la base de que Alemania no había regulado legalmente el uso de cámaras de video-vigilancia por los empleadores, pero sí existía jurisprudencia que asumía su legitimidad sobre la base del método de la ponderación entre el derecho a la intimidad de los trabajadores y la protección de los intereses de los empleadores, sin entrar en mayor valoraciones en torno a la conformidad o no de esta jurisprudencia con el CEDH, legitimará el actuar empresarial, por lo que no hubo condena a Alemania. El TEDH consideró que Alemania no estaba obligada por el art. 8 CEDH a regular de forma expresa en la ley el derecho a la intimidad de los trabajadores (Schutzgebot) en relación al uso de “video-vigilancia encubierta” por parte de los empleadores. Y que el uso que había hecho la empresa era proporcionado a las circunstancias del caso (se habían detectado pérdidas -fin legítimo-; la conducta era sospechosa y fueron solo ellos objeto de vigilancia; la medida fue limitada en el tiempo y “solo había cubierto el área que rodea la caja y era accesible para el público”)

En suma, para el TEDH:

“...la injerencia en la vida privada del solicitante *se limitó a lo necesario para alcanzar los objetivos perseguidos*.... Los tribunales nacionales habían considerado además que el interés del empleador en la protección de sus derechos de propiedad *solo podía salvaguardarse eficazmente mediante la recopilación de pruebas* a fin de demostrar la conducta delictiva del solicitante en los procedimientos judiciales...”.

Apreciamos aquí ya la centralidad de la normativa nacional de protección de los datos personales, así como la incertidumbre que genera el juicio de proporcionalidad del control, por cuanto se abre a decisiones dispares. Precisamente así sucederá años más tardes en el *caso López Ribalta*, donde llegará a la conclusión contraria, realizando una ponderación opuesta.

4^a) Caso Barbulescu (I -12 de enero de 23016- y II -5 de septiembre de 2017-). *El deber de información previa debe ser muy preciso y el juicio de proporcionalidad concreto, no abstracto*

Por ser el asunto hoy más conocido, además de servir de referencia determinante para otro estudio incorporado en este monográfico (derecho a la correspondencia ex art. 8 CEDH), aquí nos vamos a limitar a extraer, de forma muy

sucinta, las conclusiones más relevantes del “*test Barbulescu de protección de la privacidad*” del trabajador frente a los contemporáneos poderes de control digital. Al respecto, conviene poner de relieve que en la sentencia inicial, de Sala, favorable al interés empresarial, no se apartaba de sus precedentes, sino tan sólo los modulaba respecto del caso concreto, en la medida en que entendía que en él sí hubo una información previa suficiente, aun genérica, al igual que un juicio de proporcionalidad, aunque laxo. Sin embargo, la revocación por la Gran Sala, también sobre sus precedentes, pondrá de relieve que ni la información previa fue precisa, como se debía, ni el juicio de proporcionalidad resultó lo suficientemente equilibrado para los intereses del trabajador¹⁴.

Como es, de todos, bien sabido, esta doctrina, pese a no tener como referencia la experiencia española, resulta de especial incidencia en nuestro país. La razón reside en que la polémica STC 39/2016, que significará, como recordaremos brevemente ut supra, una rectificación importante de la precedente doctrina en esta materia, tomó como una referencia principal la *sentencia Barbulescu I*. A su vez, la jurisprudencia nacional hizo suya esta doctrina constitucional, que liberaba a las empresas de una importante carga de información previa precisa y finalista. En coherencia, la revocación por la Gran Sala del TEDH de aquella parecería abocar a una paralela revisión, o modulación, cuando menos, tanto de la doctrina constitucional como de la emuladora jurisprudencia social, en aras de una mayor armonización con la doctrina del TEDH. Como también veremos, no parece entenderlo del mismo modo el TS.

5ª) Caso *Antovic and Mirkovic v. Montenegro* (28 de noviembre de 2017). *La autorización del trabajador es la regla, para las grabaciones de su actividad, y su imposición empresarial la excepción*

Apenas dos meses después, el TEDH sorprendió con una decisión que llevaba más allá de lo previsible hasta el momento la garantía de privacidad social. La STEDH de 28 de noviembre de 2017, Reclamación 70838/13 (definitiva el 28 de febrero de 2018), reconoce, por ajustada mayoría (4 votos contra 3), que existió violación del art. 8 CEDH en el caso de 2 profesores de la Facultad de Matemáticas de la Universidad de Montenegro por haberse grabado (video-vigilancia), durante un tiempo, sus clases en el auditorio de la citada Facultad, en la que impartían docencia y sin su consentimiento.

Aunque se trataba de zonas de trabajo en las que siempre concurría, por definición, un grupo de personas (profesor y estudiantes), lo que dejaba ver al público lo que se registraba en el mismo lugar y mismo tiempo, y las finalidades de tal grabación eran legítimas (“garantizar la seguridad de los bienes y las personas...y la vigilancia de la enseñanza”), la mayoría entenderá concurrente la vulneración del derecho de los profesores a su “*vida social privada*” por ausencia de auto-

¹⁴ Cfr. Preciado Domènech, C.H. “Comentario de urgencia a la STEDH de 5 de septiembre de 2017. *Caso Barbulescu c. Rumanía (Gran Sala). Recuperando la dignidad en el trabajo*”, Jueces para la Democracia, septiembre 2017

rización. Se trataría de una actividad, la docencia, que no sería exclusivamente público-académica, sino que crearía relaciones singulares con el alumnado, como sucedería en virtud de preguntas y debates de un lado -profesor- y otro -alumnado-, en virtud de las cuales se construye una suerte de “identidad social de grupo” respecto de la que existe una expectativa razonable de reserva para ese grupo.

Precisamente, *este argumento relativo a la singularidad de la relación académica* será la enfatizada por 2 de los 4 Magistrados que firmaron la decisión mayoritaria, para los cuales este argumento debió desarrollarse más, y no el relativo a la protección de la vida privada en los lugares de trabajo como tales. A su juicio, la docente sería una relación presidida por la “libertad académica” y, por lo tanto, le resultaría inherente un espacio de reserva frente al control o no monitorización por las autoridades académico-administrativas. De ahí su expectativa razonable de que no van ser controlados. Una visión radicalmente contraria a la que defenderá el voto particular de los 3 Magistrados discrepantes, conforme al cual: “...los solicitantes son profesores universitarios que dictaban conferencias en un anfiteatro universitario y, por lo tanto, participaban plenamente en una actividad profesional en un entorno casi público...”.

En suma, para la mayoría, la video-vigilancia encubierta de un empleado en su lugar de trabajo debe considerarse como una intrusión considerable en la vida privada del empleado, pues implica la documentación grabada y reproducible de la conducta de una persona en su lugar de trabajo, que el empleado, que está obligado por el contrato de trabajo para realizar el trabajo en ese lugar, no puede eludir (caso Köpke). No hay ninguna razón para que el TEDH se desvíe de esa conclusión, pues

“...incluso cuando las normas del empleador con respecto a la vida social privada de los empleados en el lugar de trabajo son restrictivas, no pueden reducirse a cero. *El respeto por la vida privada continúa existiendo, incluso si puede restringirse en la medida de lo necesario* (Bărbulescu, § 80)”.

Para el TEDH, los tribunales nacionales no examinaron la cuestión de si los actos se ajustaban a la ley, dado que no excluyeron que la video-vigilancia fuera una injerencia en la vida privada. Sin embargo, la Agencia de Protección de Datos sostuvo explícitamente que violaba la Ley de Protección de Datos Personales. Una vez más, la normativa de protección de datos resulta determinante para la suerte final del derecho a la protección de la privacidad, avalando el TEDH la posición de las autoridades propias de control de efectividad de esa normativa específica sobre la doctrina jurisprudencial.

6ª) Caso López Ribalta y otras c. España (9 de enero de 2018). *El deber de información previa se concreta en la normativa de protección de datos y ha de útil.*

A menor garantía de la legislación de protección de datos, menor expectativa de protección de la privacidad del trabajador, sentenció el caso Köpke. A mayor

protección de datos personales mayor expectativa de privacidad del trabajador, replicará el caso *López Ribalta* (STEDH de 9 de enero de 2018), por lo que la calidad de protección de la vida privada se convertiría en una función directamente proporcional a la calidad de la normativa de protección de datos personales. El TEDH sentenciaría, por 6 votos contra 1, que se vulnera el art. 8 CEDH por la *vigilancia encubierta* de un grupo de cajeras de un supermercado español. Curiosamente, para alcanzar aquel fallo condenatorio contra el Estado español, tomará nota de la doctrina constitucional, como si está fuese lineal y no suscitase significativas contradicciones (SSTC 186/2000, 29/2013, y 39/2016). En todo caso, la clave del razonamiento del TEDH, para llegar al fallo condenatorio del Estado español y, en consecuencia, desautorizar el juicio jurisdiccional nacional, que no consideró vulnerado el derecho, será la exigencia legal de información previa precisa.

Clarificador resulta el siguiente razonamiento:

“68...a diferencia de Köpke, la video-vigilancia encubierta no siguió una sospecha fundamentada previa contra los solicitantes y, en consecuencia, no estaba dirigida específicamente a ellos, sino a todo el personal..., durante semanas, sin límite de tiempo y durante todas las horas de trabajo. En Köpke, la medida de vigilancia fue limitada en el tiempo, se llevó a cabo durante dos semanas y solo dos empleados fueron blanco de la medida. Sin embargo, en el presente caso, la decisión de adoptar medidas de vigilancia se basó en una sospecha general contra todo el personal...”

La sentencia ha merecido duras críticas, por *incoherente, falta de ejemplaridad y poco prudente*, que orillarían, a diferencia del precedente alemán -el voto particular del juez Dedov aprecia ruptura-, el margen de apreciación ponderativa de los Tribunales nacionales, sacrificando el derecho de propiedad del empleador por el derecho a la privacidad del trabajador. Pero también ha contado con loas¹⁵. Aquí interesa destacar que se refuerza la doble evolución impulsada por la *sentencia Barbulescu*. Por un lado, el reforzamiento del deber de información previa en condiciones útiles para la defensa del derecho del trabajador (“saber” fehacientemente de la vigilancia empresarial le atribuye “poder” tomar decisiones adecuadas a sus intereses). De otro, la necesidad de que el juicio de proporcionalidad se haga de forma exhaustiva, concreta, no nominal.

Si bien, desde el sector de la abogacía de empresa, se le reprocha que no tenga en cuenta la necesidad de eficacia práctica del poder empresarial, el TEDH argumenta que sí se salvaguarda, si se ejerce por medios más razonables “en particular informando previamente..., *incluso de forma general*, sobre la instalación de un sistema de video-vigilancia y proporcionándoles la información prescrita

¹⁵ Vid. Rojo Torrecilla, E. “*Nuevamente sobre el derecho del trabajador a la privacidad en la empresa y su control por cámaras de vigilancia. Estudio del caso López Ribalta y otras contra España (a propósito de la sentencia del Tribunal Europeo de Derechos Humanos de 9 de enero de 2018), I y II*”. En sendas entradas de su actualizado y sugerente Blog (16 y 17 de enero de 2018)

en la Ley de Protección de Datos Personales”. En suma, poder “vigilar”, sí, “poder castigar”, también, pero primero debe informarse de forma adecuada (deber de transparencia comunicativa), aunque, y aquí queda una significativa duda de esta doctrina ¿si basta con la información general, no cabría pensar que las trabajadoras ya debían conocer la existencia de esas cámaras? En cualquier, caso la STEDH de 9 de enero de 2018 *vendría a corregir en realidad la doctrina involuntiva de la STC 39/2016, de 3 de marzo de 2016*.

En efecto, para el TC, siempre que hay causa objetiva que justifique la medida (sospecha fundada de hurtos) y una publicidad genérica, el control empresarial tendrá legitimidad constitucional, sin que el incumplimiento de la norma sobre protección de datos equivalga a infracción del derecho fundamental a la intimidad, manteniéndose en el plano de las infracciones legales. El TEDH valora, sin embargo, que tal infracción legislativa sí equivale a violación del derecho humano a la privacidad.

La sentencia del TEDH no descuida su búsqueda del “justo equilibrio”, dando al interés empresarial una importante concesión¹⁶: *se excluye la violación del derecho a un juicio justo*, por lo que las sentencias que declararon procedentes los despidos eran correctas desde el prisma del art. 6 CEDH. Por lo tanto, *el despido no se verá afectado*, aunque la prueba invalidada sí dará lugar a resarcimiento del daño moral. No deja de ser relevante -más de lo advertido hasta ahora- para la práctica (empresarial y judicial) esta doctrina, porque el uso indirecto de estas grabaciones nulas para crear otras válidas se acepta por el TEDH. En buena medida se asume aquí tanto el interés del empleador a medidas eficaces de control como el interés público a una administración de justicia más adecuada a la hora de ponderar los derechos e intereses particulares en juego. Por tanto, el TEDH

¹⁶ Aunque el fin no justifica los medios el TEDH no descuida, sin acoger en toda su plenitud, el argumento de la garantía de eficacia del poder de investigación (empresarial). Esta fuerte tensión entre el interés de la eficacia investigadora y el de la privacidad es un clásico en todas las experiencias judiciales, como en la norteamericana. Así, por ejemplo, la sentencia *United States v. Jones* (2012) *declaró ilegal el uso del GPS para combatir la criminalidad sin la correspondiente autorización judicial*. Y en el asunto *Kyllo* (2001), también declaró nula la prueba de *escáner de termografía infrarroja* en virtud de la cual, la policía, desde la calle, demostraba que una parte de la vivienda emitía más calor en comparación con el resto de los apartamentos aledaños, evidenciando una plantación de marihuana que usaba potentes lámparas. Esta primacía del derecho sobre la eficacia de la facultad de policía también quedó reflejada en la sentencia *Riley c. California* (2014). En ella se planteó si la policía podía registrar la información contenida en un teléfono móvil (smartphone) que había sido intervenido a un particular, detenido por una infracción de tráfico, sin necesidad de autorización judicial. En una sentencia prácticamente unánime el presidente Roberts expresó esta idea: «El hecho de que la tecnología permita ahora que un particular lleve información consigo no significa que la información sea menos digna de la protección por la que lucharon los Fundadores. (...)». Una vez más, la decisión no es unánime. Un Magistrado -el juez *Alito*- formuló un voto particular para puntualizar dos aspectos relevantes. Por una parte, consideró que no se podía aplicar la regla utilizada en la era pre-digital para registrar un teléfono móvil, sino que requería una nueva interpretación de la aplicación de la ley y los intereses de la privacidad (argumento de evolución social). Por otra parte, estimó que correspondía al legislador, elegido por los ciudadanos y en mejor posición que los jueces, evaluar y responder a los cambios que ya se han producido y, más aún, a los futuros (argumento político-normativo). Para la síntesis de estas sentencias vid. Ordoñez Solís, D. La protección de los derechos fundamentales en Internet en la jurisprudencia europea, Editorial Reus, Madrid, 2014.

parece querer mediar en la cuestión de la eficacia de esta nulidad de las pruebas tecnológicas en el despido cuando éste puede acreditarse por otras vías. Se volverá después sobre este importante aspecto, que ha pasado desapercibido para buena parte de la doctrina científica y, sobre todo, de la doctrina judicial.

7ª) Caso *Libert c. Francia* (22 de febrero de 2018). *¿El retorno a la posición originaria de defensa de una expectativa de privacidad conforme a la información dada sobre la normativa interna y un juicio estricto de proporcionalidad?*

Poco más de un mes después, el TEDH nos sorprende con otra sentencia de gran calado; pero ahora con un fallo de sentido contrario a los últimos precedentes. Esta vez, la mayoría -6 contra 1- de la Sala 5ª se inclina, para un asunto de una conocida y potente empresa pública francesa, a favor de la potestad de vigilancia tecnológica en detrimento del derecho a la privacidad. Es el esperado -y un tanto decepcionante- caso *Libert c. Francia* (STEDH de 22 de febrero de 2018, Reclamación 588/13, devenido definitivo, en virtud del artículo 44.2 del CEDH, el 2 de julio de 2018). El caso se refiere al despido de un empleado de la SNCF tras la incautación de su ordenador profesional que reveló el almacenamiento de archivos pornográficos y falsos certificados realizados en beneficio de terceros. El TEDH considera que la consulta empresarial de los archivos por el empleador sí fue conforme con un objetivo legítimo de garantizar que se usen los equipos propiedad de la empresa para su fin productivo.

Como en el caso *Köpke*, el TEDH considerará determinante el margen de decisión legislativa nacional. Parte del reconocimiento en el Derecho francés (art. L. 1121-1 y L.1321-3 del Code du Travail) de un principio de protección de la intimidad, según el cual, los empleadores pueden abrir ficheros profesionales, no los identificados como “privados”. En la normativa interna de la empresa se indicaba que las informaciones de carácter privado contenidas en ficheros “debían ser claramente identificadas como tales”, algo que no había ocurrido en el caso enjuiciado, pues los archivos indicaban sólo “personales”, lo que podía ser ambiguo, ya que personal podría referir a expedientes profesionales llevados de forma personal, no ya asuntos privados, pues su uso para tales estaba prohibido, salvo casos excepcionales. La Cour d’Appel estimó que el trabajador había vulnerado la normativa deontológica de la SNCF al hacer un uso “privado” de los medios informáticos puestos a disposición de los trabajadores, pues en esta caso no había sido puntual, que toleraba la empresa, sino continuado. Tesis acogida por la *Cour de Cassation*, que insistió en la razonabilidad de la conducta empresarial. Además, puso de manifiesto el uso claramente abusivo del dispositivo, pues almacenó “1.662 archivos pornográficos que representaban un volumen de 787 megabytes durante un período de cuatro años, y que también había utilizado su ordenador de trabajo para preparar declaraciones falsas”.

El TEDH asumió aquí, a diferencia parcial del caso (español) López Ribalta, el margen de decisión, tanto legislativa como de juicio jurisdiccional, nacional:

“La utilización de los recursos del sistema de información de la SNCF sólo es posible en el marco de la actividad profesional del personal, definida por su función y dentro de los límites de las delegaciones que se les han concedido. No obstante, *el uso personal ocasional y razonable de la mensajería y de Internet se tolera en la vida práctica o familiar, siempre que no afecte a la calidad del servicio asociado*. La información de carácter privado debe identificarse claramente como.... Lo mismo se aplica a los medios de comunicación que reciben esta información (directorio” PRIVADO”). Este uso está sujeto a una autorización estrictamente personal que de ninguna manera puede ser transferida, ni siquiera temporalmente, a un tercero sin ninguna responsabilidad por parte del propietario. Podrá ser revocada en cualquier momento y cesará si la actividad profesional que la haya justificado queda suspendida temporal o definitivamente. (...)” (Apartado 19).

En suma, en este caso, la injerencia tecnológica empresarial en la vida privada del trabajador¹⁷, pese a carecer de una información específica previa (los ficheros fueron abiertos sin la presencia del trabajador y sin ser informado de ello), hallará *causa proporcionada* (el empleador pueda verificar en tales circunstancias que sus empleados realizan sus tareas profesionales de manera adecuada y con la celeridad requerida). De este modo, la decisión de sala del TEDH *parece frenarse en su avance interpretativo, retrocediendo incluso respecto de la sentencia Barbulescu II (la ausencia de recurso nos privará, por ahora, del más que oportuno pronunciamiento de la Gran Sala)*. De un lado, se conforma con la *existencia de una normativa interna clara y conocida* (que exige la identificación del correo excluido del control empresarial como “privado”, no siendo suficiente la referencia “personal”, pese a ser esta la denominación utilizada por la jurisprudencia para fijar la diferencia entre correos incluidos y excluidos del control). De otro, bastará la constatación de un uso intensivo no profesional del ordenador para tener como proporcionado el margen de control del mismo de las autoridades nacionales (apartado 52). En definitiva, y tras esta corta pero intensa producción jurisprudencial del TEDH desde “Barbulescu I”, el panorama europeo más se ensombrece que se aclara.

4. IMPACTO DE LA EVOLUCIÓN DEL TEDH EN LA JURISPRUDENCIA NACIONAL: DE LA “INVOLUCIÓN” A LA “INCERTIDUMBRE”

4.1. La función jurisprudencial de suplencia legislativa en la fijación de límites al poder de control empresarial: del estancamiento a la involución

Asumido jurisprudencialmente, desde hace más de una década (2007), un poder general del empleador de controlar tecnológicamente la actividad del trabaja-

¹⁷ En este caso se trata de una persona jurídica de derecho público, aun sometida a Derecho privado, pero la clave interpretativa es análoga. A diferencia del asunto Barbulescu, cuyas injerencias al respeto de la vida privada fueron en el sector privado, la queja será analizada como obligación negativa, no como obligación positiva del Estado.

dor, en virtud del art. 20.3 ET y en detrimento del art. 18 ET (límites del poder de policía empresarial), ni el legislador ni la jurisprudencia laborales mostraron la debida atención a la evolución producida por la normativa de protección de datos en el conflicto entre la privacidad del trabajador y la libertad de empresa. Esta profunda disociación legislativa en el plano laboral entre el derecho a la autodeterminación informativa en una esfera, la laboral, dominada crecientemente por la digitalización, y el derecho a la privacidad del trabajador, ha venido plagando nuestro sistema de insuficiencias reguladoras (vicio de lagunas) y de contradicciones (vicio jurídico de antinomias). Aunque era de esperar que, con el progresar del tiempo, el TC y el TS pudieran corregir estas deficiencias, lo cierto es que ha contaminado también el actuar jurisprudencial. Consecuentemente, si a finales del siglo pasado los principales estudios en esta materia concluían un altísimo grado de inseguridad jurídica¹⁸, el acopio de un inmenso cuerpo de doctrina jurisprudencial (ordinaria y constitucional), lejos de reducirlo lo ha ampliado, agravándose por el fuerte contraste entre la revisada evolución del TEDH y la involución del TC español

La incertidumbre real es mayor porque, como se anticipó, en teoría, desde una perspectiva abstracta, TC y TS han venido asumiendo como criterio resolutivo básico del conflicto el vetusto -y más correcto- principio de proporcionalidad (justo equilibrio), por encima del -no menos antiguo, pero más impropio aquí, por tratarse de conflicto entre derechos fundamentales- de buena fe (deber de transparencia y prohibición de usos abusivos). Este canon de legitimidad, asumido por el TEDH, servía tanto para dar validez al control empresarial (STC 186/2000) como para anularlo (STC 98/2000).

Desde esta perspectiva general de comparación entre ambas doctrinas -europea y nacional-, que el TC español validase tempranamente medidas de video-vigilancia (por cámara) encubierta (con omisión del deber de información colectiva ex art. 64.1.3 ET), si concurría una “razonable sospecha de hurtos” (u otro tipo de infracciones laborales) y un modo de ejercicio proporcionado (para la zona de caja y tiempo limitado), no parece contrariar la reciente doctrina del TEDH, que también lo acepta en ciertas circunstancias (casos *Köpke* y *Libert*). Por lo tanto, para el TC, si no es dudoso el deber general de adaptabilidad de los derechos fundamentales de los trabajadores a los requerimientos de la organización empresarial, que legitima la regulación interna del uso de los medios informáticos de titularidad empresarial, así como la facultad empresarial de vigilancia (tecnológica -auditorías informáticas, GPS, control biométrico, etc.) del cumplimiento con-

¹⁸ Vid. Sala Franco, T. “*El derecho a la intimidad y a la propia imagen y las nuevas tecnologías de control laboral*”. En AAVV. (E. Borrajo -Dir.-). Trabajo y libertades Públicas. La Ley, Madrid, 1999, p. 205. No se cumplió, pues, la “profecía” de ciertos autores, que auguraban la solución al problema de la inseguridad jurídica a partir de una sólida y solvente doctrina jurisprudencial general. Cfr. López Aniorte, M.C. “*Límites constitucionales al ejercicio del poder directivo empresarial mediante el uso de las TIC y otros medios de vigilancia y seguridad privada en el ordenamiento laboral español*”. *Política y Seguridad Pública*, vol. 1, n. 4, 2014, pp. 31 y ss.

tractual, tampoco lo sería la necesidad de ejercicio proporcionado¹⁹, para asegurar “pleno respeto a los derechos fundamentales”(STC 241/2012, FJ 5). Entre ellos, el derecho a la intimidad, en cuanto derivación de la dignidad (art. 10.1 CE), que *implica reservar un ámbito propio frente a la acción y el conocimiento de los demás, necesario, según las pautas de cultura, para mantener una “calidad mínima de la vida humana”*, también en las relaciones de trabajo [STC 170/2013, FJ 5].

Una convergencia, más aparente o nominal que real, que también parecía darse cuando tanto el TS -de forma pionera²⁰- como -posteriormente- el propio TC asumieron el concepto típico del TEDH para delimitar el margen de protección esperable por el trabajador de su privacidad: la tutela en cada caso (el juicio casuístico es común al referido canon de proporcionalidad) de una *expectativa razonable de privacidad* (STC 12/2012, de 30 de enero, FJ 5). De ahí, que tengan entrada específica los precedentes del TEDH *Halford* y *Copland*. Para el TC, *el dato de la previsión o no de un exclusivo uso profesional será determinante de la expectativa*. De este modo, el TC - y el TS- aceptan que si hubo información previa sobre la normativa interna de control de medios informáticos no cabría razonablemente confiar en el carácter privado de sus usos.

Ahora bien, si resulta evidente que las “músicas” suenan de forma análoga, sus “letras pequeñas” no resultan tan convergentes, evidenciándose un proceso inequívoco de decantación restrictiva de ambos cánones de control de legitimidad del poder, de tal modo que el resultado práctico será a menudo el de la protección de aquél frente a toda esfera útil del derecho a la privacidad. Para acreditar esta afirmación bastará con traer a colación, de un lado, que el TS asumía la pérdida del “uso social” de los medios propios del empleador si éste había dejado bien clara su prohibición absoluta, agotando su uso en finalidades profesionales, y, de otro, que el TC también legitimaba que se carecía de tal expectativa de uso social de la privacidad si una norma colectiva tipificaba como infracción usos extra-laborales, aun no existiendo información previa empresarial (STC 170/2013). A diferencia de lo que decantaría el TEDH, TC y TS *niegan un espacio objetivo y autónomo (social) de privacidad por el trabajador en el uso de dispositivos propiedad de la empresa* al margen de su norma y/o tolerancia, de modo que (solo) quien crea la expectativa, el empleador (o norma colectiva), puede destruirla²¹.

¹⁹ Para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres siguientes requisitos o condiciones: si tal medida es susceptible de conseguir el objetivo propuesto [juicio de idoneidad]; si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia [juicio de necesidad]; y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto [juicio de proporcionalidad en sentido estricto]¹⁹ (STC 96/2012).

²⁰ Las célebres SSTs, 4ª, 26 de septiembre de 2007, RCU 966/2006, y 8 de marzo de 2011, RCU 1826/2010)

²¹ Para diversas posiciones -unos críticos, otros adherentes o comprensivos- de esta “evolución-involución”, vid. Preciado Domenech, C.H. *El derecho a la protección de datos en el contrato de trabajo*. Pamplona, 2017, pp. 76 y ss.; Aparicio Tovar, J. “Los derechos fundamentales

Este proceso de decantación práctica restrictiva de la doctrina teórica sobre los diversos cánones de legitimidad (constitucional y ordinaria) del poder de injerencia del empleador sobre la privacidad del trabajador en la prestación de servicios, frente a un proceso de decantación práctica expansiva del TEDH, se confirmará, agravándose, en la última fase, por el momento, de este proceso de maduración interpretativa y respecto del tercer canon de legitimidad jurídica de aquél poder empresarial: *el deber de información /derecho de saber previos* sobre el sentido y alcance del control empresarial. En efecto, si dando continuidad a la doctrina general sobre la expectativa razonable de privacidad del trabajador a tenor del margen de confianza creado por el actuar empresarial (jurídico y fáctico), la STC 29/2013, de 11 de febrero, reforzaría la posición laboral exigiendo que mediase un deber informativo previo específico laboral (no basta informar del fin general de seguridad pública, hay que comunicar la finalidad laboral perseguida), dando entrada a la función garantista de la normativa de protección de datos, la STC 39/2016, de 3 de marzo (caso Bershka -BSK- España) truncará ese proceso, involucionándolo.

Aunque se ha discutido mucho, y se sigue haciendo, tanto en sede científica como judicial, en torno a la relación de este último precedente constitucional respecto de anteriores, y sobre todo en relación a la doctrina del TEDH, considerándolos unos de signo rupturista, mientras que otros no ven tal fisura, no es baladí indicar que la STC 39/2016 tomó como precedente europeo para confirmar su interpretación liberalizadora y de garantía de la eficacia para el poder empresarial la "*sentencia Barbulescu P*". Pero, como todos sabemos, esta posición hermenéutica inicial ha sido revisada por la Gran Sala del TEDH y, en consecuencia, parece claro que, como afirma el muy fundado voto particular que acompaña a la STC 39/2016, el asumir la posición de la mayoría vendría a vaciar de sentido práctico, si no el modelo de relaciones laborales, más abierto, sí el contenido esencial del derecho a la privacidad del trabajador conforme al plus protector que le ofrece la jurisprudencia del TEDH. Frente al favor constitucional por la teoría de las potestades implícitas de control empresarial, a partir tanto de normas genéricas de carácter legal (art. 6 de la Ley de protección de datos personales, art. 20 ET) como colectivas, incluso de carácter interno (códigos de conducta o políticas empresariales de uso social razonable de medios tecnológicos), el TEDH se muestra más severo y preciso a la hora de legitimar el uso práctico, real, del poder de control empresarial, exigiendo un plus de información: a la genérica -existencia de una norma de control- sumaría la específica -el uso de vigilancia laboral concreto-.

y el juicio de proporcionalidad degradados a mera retórica (a propósito de la STC 170/2013, de 7 de octubre)". Revista de Derecho Social, n. 64, 2013, pp. 143 y ss.; Gallardo Mora, R. "*El derecho fundamental a la protección de datos personales y la video-vigilancia empresarial*". Revista de Derecho Social, n. 62, 2013, pp. 163 y ss. Más recientemente Tascón Rodríguez, R. "*Tecnovigilancia empresarial y derechos de los trabajadores*", RTSS-CEF, n. 415, octubre 2017, pp. 70 y ss.

4.2. Neutralización teórica nacional del plus de protección práctico europeo: el persistente contrastes entre la doctrina judicial y la jurisprudencial

4.2.1. ¿El resurgir de la doctrina de suplicación de la “doble información previa”, genérica y específica laboral?

La desazón e incertidumbre que dominan este ámbito desde antaño continúan dejándose sentir en la incapacidad de lograr un básico acuerdo en torno al impacto real de la evolución del TEDH en la jurisprudencia nacional sobre el conflicto entre vida privada del trabajador y control empresarial. No ayuda tampoco el TEDH, cuando, como la sentencia *López Ribalta*, remite de forma lineal, como si no hubiese fracturas entre ellas, a las diversas sentencias constitucionales en la materia. Pero el contraste es manifiesto, otra cosa será dilucidar hasta dónde, de forma precisa y, por lo tanto, de qué modo debería producirse la rectificación o, cuando menos, modulación por parte del TC y del TS. La mejor prueba de ese persistente conflicto es la diversa visión de él que mantiene la *doctrina judicial mayoritaria* (instancia y suplicación), y la *jurisprudencia*.

Como evidenciaremos de inmediato, sucintamente, la última doctrina judicial de suplicación (también la mayoritaria de instancia social), tiende a dejar constancia de la fractura entre la evolución jurisprudencia del TEDH y la involución de la doctrina del TC y, a su estela, del TS. En cambio, la sala social del TS parece seguir enrocada en su posición precedente, neutralizando cualquier mejora protectora derivada de aquélla. Por lo tanto, a su juicio -en parte errada- la situación práctica sería análoga a la anterior a los precedentes “*Barbulescu*” y *López Ribalta*.

La posición crítica de la doctrina de suplicación social es manifiesta. Entre los muchos ejemplos que podrían citarse, destacaremos aquí la *STSJ Madrid, 233/2018, 23 de abril* (despido de un trabajador de la empresa Ferrovial Servicios). En ella, tras dejar constancia de la equivocidad de la respuesta judicial respecto de los límites a los poderes de control tecnológico empresarial, para lo que repasa los precedentes básicos, tanto del TC como del TS, incluso los asuntos “*Barbulescu*” y “*López Ribalta*”, se declarará la ilicitud de la prueba, calificando la improcedencia del despido (no nulidad), porque, en el caso concreto, la medida de seguimiento del personal adscrito al servicio de bar mediante detectives privados dotados de cámara oculta, además de ser aleatorio y sin sospecha previa de conducta irregular del trabajador -sí de otros compañeros-, tuvo lugar sin información previa de la posibilidad de tales usos. Para la sala de suplicación, no sería constitucionalmente lícito sustituir ese deber de información previa y específica laboral por un puro conocimiento genérico y presunto a partir del eventual conocimiento de este tipo de seguimientos en otros trabajadores de la empresa. La sala

de suplicación opta por la posición garantista²², citando la STS 13 de mayo de 2014, Rec. 1685/2013.

Análoga posición interpretativa, con idéntico resultado, mantendrá la sala social del TSJ castellano-manchego, que ha dictado diversas sentencias tras los citados asuntos del TEDH y en los que deja clara constancia del contraste existente, en su opinión, con la doctrina constitucional y la jurisprudencia del TS nacionales. La *STSJ Castilla-La Mancha 407/2018, 21 de marzo* invalida la prueba de control tecnológico (grabaciones video-gráficas), aceptada en instancia social, por ausencia de información específica en torno a la finalidad laboral del control (las cámaras eran visibles y sólo existía distintivo general). Esta conclusión la alcanza tras un exhaustivo repaso de los precedentes

Aunque, tras este repaso por el Derecho de precedentes jurisprudenciales, la sala es consciente de que existe divergencia entre la STC 39/2016 (que dispensa tanto del consentimiento ex art. 6 LOPD como del deber de información específica previa, bastando con el distintivo genérico de video cámaras conforme a la normativa sobre protección de datos), y algunos de sus precedentes, así como entre la STS de 2 febrero 2017 (Recurso 554/2016), lo que podría llevar a dar validez de la prueba video-gráfica, considera oportuno "...señalar que este criterio jurisprudencial...podría cambiar a la vista de la doctrina sentada por el TEDH...., en la que el tribunal hace constar que la video-vigilancia llevada...por el empleador... no cumplió... con la obligación de informar previamente, explícitamente...y sin ambigüedad de lo relativo a la existencia y características particulares de un sistema de recogida de datos personales”.

En el caso, la sala concluye la nulidad del despido, pero no como consecuencia directa de la nulidad de la prueba video-gráfica empresarial, pues asume la doctrina de la improcedencia -si no media otra prueba válida justificativa de la infracción, sino por tratarse de una trabajadora con jornada reducida por razones de guarda legal. En tales casos, dado que no se acredita la causa infractora alegada, procedería la nulidad objetiva del art. 55.5 b ET y del art. 108.2 b LRJS, sin indemnización adicional²³. En cambio, dado que, en el caso concreto, no concurrió tal circunstancia personal, la *STSJ Castilla-La Mancha, 25/2018, 12 de enero* (Rec. 1416/2017), declaró improcedente un despido cuya principal prueba de cargo era la video-grabación del trabajador fumando dentro de su jornada laboral,

²² En línea análoga, la *STSJ Madrid, 391/2018, 30 de abril* declara existente intromisión en la vida privada -y en las comunicaciones- de una trabajadora al no existir ni regulación del uso de los dispositivos tecnológicos ni advertencia previa de la finalidad disciplinaria de los controles. En ella se cita la *STS de 8 de febrero de 2018*, dejando constancia de que, a su vez, tiene en cuenta la jurisprudencia del TEDH

²³ “No ha lugar a la indemnización por lesión de derechos fundamentales que también se reclamaba en el “suplico” de la demanda, al no apreciarse la existencia de un específico móvil empresarial discriminatorio o de lesión de derechos fundamentales, y ello con independencia de la declaración de nulidad del despido que se efectúa por imperativo legal, no estrictamente constitucional -ni comunitario-” (FJ Tercero)

una vez que ésta debe anularse pues ni se informó debidamente (no se comunicó al trabajador la instalación de una cámara dentro de la caseta control de los vigilantes de seguridad donde presta sus servicios, sin que bastaran los distintivos sobre tales cámaras en la propiedad) ni proporcionada respecto de la finalidad (comprobar un presunto y sospechado incumplimiento laboral del operario -fumar en lugar prohibido-, ya que había otros medios menos intrusivos). Una vez más, tras un exhaustivo repaso de la doctrina jurisprudencial y de la jurisprudencia social, con recapitulación de cuáles son los criterios nacionales para el control de validez de las pruebas tecnológicas, se pone de manifiesto *el favor de nuestro sistema jurídico por un estricto deber de información previa y específica a fines laborales*, de modo que la *exención general del deber de consentimiento* quede compensada con un *deber general de información útil*.

Por supuesto, la sala de duplicación social recuerda que la STC 39/2016 supuso la liberación “a las empresas de esta carga informativa explícita y precisa, al tiempo que convierte la sospecha de que un trabajador está cometiendo irregularidades, en una habilitación para instalar las cámaras en el lugar de trabajo, resolviendo así de forma contraria a la STC 29/2013, sin explicación alguna sobre las razones del cambio de doctrina...”. Pero, inmediatamente precisa que tal involuación jurisprudencial deberá, a su vez, rectificarse, pues sobre ella “indudablemente va a influir la reciente Sentencia de 9 de enero de 2018... en la que se reafirma el criterio sostenido en la anterior de 5 de septiembre de 2017 dictada por la Gran Sala (...). Considera el TEHD que los derechos del empresario podrían haberse satisfecho, al menos en cierto grado, por otros medios, concretamente informando previamente a las demandantes, incluso de forma general, de la instalación de un sistema de video vigilancia y proporcionándoles la información prevista en el artículo 5 de la LOPD”. A su juicio -ingenuo, como veremos-, tal doctrina del TEDH “...previsiblemente también influirá en la última jurisprudencia del Tribunal Supremo que ha aplicado la doctrina constitucional de la STC 39/2016...”.

Curiosamente, la sala de duplicación social llega al mismo juicio anulatorio, de la prueba tecnológica no suficientemente transparente, que alcanzaría con la doctrina del TEDH, aplicando la doctrina constitucional cuya crítica, con razón, acaba de realizar. A su juicio -errado-, el art. 5.1 LOPJ le impondría una vinculación más fuerte al TC que al TEDH, cuando el art. 96 CE le exige, dado que aplica legalidad ordinaria sujeta a la primacía del Derecho Internacional (art. 8 CEDH), lo contrario para resolver el asunto. Por eso, no aplicará directamente la doctrina del TEDH (juicio de convencionalidad), sino que se mantendrá en el precedente de la STC 39/2016, aunque no lo considere concordante con aquélla. Ahora bien, si una primera lectura de la misma llevaría a dar validez a la prueba video-gráfica, según el canon de información básica (conforme al distintivo de la normativa de protección de datos personales), un análisis más profundo de la misma, desde el canon clásico de proporcionalidad, evidenciaría la invalidez constitucional de tal

prueba, porque "...el comportamiento empresarial...no cumple el triple juicio de proporcionalidad exigible a toda medida restrictiva de derechos fundamentales. (...)". Y ello, precisa la sentencia de suplicación, porque "aunque no parece existir duda sobre el carácter justificado de la medida,... no puede afirmarse que fuera necesaria, en tanto en cuanto existían otros medios más moderados, menos agresivos del derecho a la intimidad personal del trabajador..."(FJ Sexto).

Un juicio de proporcionalidad, como última trinchera del control judicial, que tampoco pasará el asunto conocido por la SJS Madrid n. 19, 453/2017, 17 de noviembre, caso empresa AMADEUS SOLUCIONES TECNOLÓGICAS S.A), que sí hará, frente a la decisión de la sala social castellano-manchega, una aplicación directa de la doctrina del TEDH. Para el juzgador de instancia social la actuación empresarial no superará los criterios del TEDH, por desproporcionada: "el objetivo de la empresa, que se orientaba a determinar la carga de trabajo de la demandante y su dedicación al mismo, hubiera podido alcanzarse por otras vías menos invasivas, tales como el control de los resultados del trabajo de la demandante (que no se olvide que se desarrollaba en el centro de trabajo) o por medio de la exigencia de una dación de cuenta por parte de la actora de las tareas realizadas durante su jornada, incluso de forma diaria durante un cierto periodo...". En este caso -volveremos después sobre ello-, no obstante, sí que tal nulidad de la prueba video-gráfica llevará a la nulidad del despido, con indemnización adicional por daño moral, con lo que mantiene una posición diferente a la sostenida en este -importante- punto por la doctrina de suplicación castellano-manchega²⁴.

Una aplicación directa de la jurisprudencia del TEDH (concretamente de la sentencia López Ribalta), en detrimento de la doctrina constitucional, y una calificación de nulidad del despido, a raíz de la nulidad de la prueba video-gráfica, que defenderá también la *STSJ PV 470/2018, 27 de febrero*²⁵. En ella, tras un enésimo reconocimiento de la complejidad del estado del arte interpretativo jurisprudencial en la materia, no sólo por la dificultad del conflicto y su proliferación en el foro sino también por el contraste entre la justicia constitucional y la europea, se asume la preferencia de ésta: "la Sala ha de tener también en cuenta - y muy especialmente - la reciente STEDH de 9 de enero de 2018 - López Ribalta-...(...)". Por eso, considera que "la grabación realizada por la empresa vulnera el derecho a la vida privada de la trabajadora demandante, dado que no fue informada de la existencia de tal sistema de video vigilancia ni de los extremos de los que debió haber sido informada según la previsión del artículo 5 LOPD...". Eso sí, a dife-

²⁴ Para un sugerente análisis vid. Benito-Butrón Ochoa, J.C. "*¿Cabe reconocer la indemnización de daños cuando se declara nula una prueba con lesión de derechos fundamentales aunque el despido no sea declarado nulo (solo improcedente)?*", RTSS-CEF, n. 421, abril 2018, pp. 124 y ss.

²⁵ Una cajera, socia-trabajadora de la cooperativa EROSKI, es despedida en virtud de la imputación de una infracción muy grave -manipulación fraudulenta en el cobro de artículos de caja- desvelada a través del análisis pormenorizado de diarios electrónicos y visionado de la cámara instalada encima de la caja. El total apropiado sería de 83 Euros, resultante de 9 tickets fraudulentos en el mes de diciembre

rencia de la sentencia de instancia social madrileña, no incluye una indemnización adicional, porque no se reclamó en la instancia social

Puede observarse, de este modo, cómo la evolución jurisprudencial del TEDH parece estar sirviendo a la doctrina judicial de suplicación para “resucitar” su conocido “test de la doble información previa” para superar, en el ejercicio del poder de control tecnológico del empresario, la expectativa razonable de privacidad social del trabajador: una política de uso de los dispositivos tecnológicos, predeterminada y comunicada, en primer lugar, y una información específica sobre los medios para garantizar que aquélla se cumple (garantía empresarial del uso correcto de los medios tecnológicos propiedad del empleador), después (ej. STSJ Cantabria, 18 de enero de 2007, rec. 187/2007). Frente a la doctrina constitucional de la potestad implícita de control del uso correcto de los dispositivos tecnológicos, inherente a toda prohibición de usos no productivos de aquéllos, los Tribunales Superiores de Justicia, de forma mayoritaria, mantenían que tal potestad ha de explicitarse, sin ambages. Ahora, el TEDH vendría a darles la razón, al menos con carácter general y, en consecuencia, la doctrina de suplicación social se muestra convencida de la necesidad de rectificación del TC y del TS para reconciliarse con el TEDH.

Si bien es cierto que no todas las decisiones judiciales posteriores a los asuntos del TEDH aquí analizados alcanzan un juicio anulatorio de la prueba tecnológica, pues *en algunas de ellas, las menos ciertamente, se asume su validez*, sí que en todas queda de relieve el referido contraste entre la jurisprudencia nacional, restrictiva, y la europea, expansiva. Es el caso, por ejemplo, de la Sentencia *del Juzgado de lo Social n.1 de Oviedo 171/2018, 22 de marzo*. En este caso, en el que se impugna el despido por violar su derecho a la intimidad y a la protección de datos, al haber sido grabado en el trabajo sin su consentimiento, ni informado de que estaba siendo grabado ni que podía ser sancionado en base a esas grabaciones, el juzgador, respecto de la prueba video-gráfica, decide mantenerse fiel “...a la última doctrina fijada por el Tribunal Supremo..., que si bien podría variar en base a la última doctrina fijada por TEDH en el caso Barbulescu y López Ribalta, es la que se mantiene vigente en el momento actual”. En consecuencia, validará la prueba porque la instalación de cámaras de seguridad era una medida justificada por razones de seguridad (control de hechos ilícitos imputables a empleados, clientes y terceros, así como rápida detección de siniestros), idónea para el logro de ese fin (control de cobros y de la caja) y proporcionada al fin perseguido, pues “es la única forma que existía para...acreditar quién se había apropiado del dinero”.

Las deficiencias informativas identificadas en el caso -consta el distintivo de las cámaras, pero no la información precisa sobre su uso para investigar de forma específica eventuales infracciones-, no pueden llevar, conforme a esa jurisprudencia constitucional y ordinaria, a la nulidad de la prueba tecnológica. De modo

que “...frente a los defectos informativos...pudieron reclamar a la empresa más información o denunciarla ante la Agencia Española de Protección de Datos, para que la sancionara...”. No obstante, el despido fue declarado improcedente por la falta de nitidez de la grabación.

Una posición de favor hacia la máxima eficacia del poder de control tecnológico del empresario, siempre que medie la superación del referido test de proporcionalidad, que incluso se evidencia en el ámbito penal, cuando, paradójicamente, la sala penal del TS se había mostrado mucho más restrictiva que el TC y que la sala social del TS, si bien es cierto que en relación al derecho del secreto de comunicaciones. Desde aquella perspectiva más expansiva, de interés resulta la Sentencia de la Audiencia Provincial de Madrid, 283/2018, 3 de abril, que incluso asume la posibilidad de legitimar el control empresarial de los ordenadores sin información específica previa, incluso respecto de las normas generales de uso de los dispositivos propiedad de la empresa. En efecto, si con carácter general se exige esa delimitación e información previa de la política de uso en la empresa de los dispositivos de comunicación digital para justificar el control, en ciertos casos -excepcionales- se puede prescindir de tal deber. Sería la situación de aquellos usos del ordenador que resulten tan determinantes para la prestación de servicios -ej.: programadores informáticos- que haga inherente ese control al conocimiento profesional de tales empleados cualificados, porque resulta razonable atendiendo al tipo de actividad realizada por el trabajador:

“...Aunque no consta que por parte de la empresa y con arreglo a la buena fe se hubieran establecido previamente las reglas de uso de los ordenadores, no puede obviarse...que...no sólo eran propiedad de la empresa y se facilitaban al trabajador para utilizarlos en el ejercicio de su prestación laboral, sino que esa herramienta...era la... fundamental e imprescindible y que el control...sobre los ordenadores alcanzaba una especial relevancia, y que, en consecuencia, los trabajadores acusados, en su condición de programadores informáticos tenían que tener cumplido conocimiento de que su actividad (realizada a través de las computadoras) iba a ser objeto de examen continuo”.

Fuera de estos casos, sí que sería exigible la información previa y precisa, tal y como esta sentencia penal indica, también recordando la intensidad de este deber en el asunto *Barbulescu*. En el caso, la sentencia de apelación penal, aunque rehabilitó las pruebas informáticas anuladas por la instrucción-instancia judicial penal, alcanzaría un mismo juicio de absolución -por tratarse de sentencia absoluta- la de instancia, no revisable en apelación mediante nueva valoración de las pruebas-.

4.2.2. “R que R” del TS nacional: el juicio de proporcionalidad del TEDH en nada diferiría del propio del TC

En contraste con esta crítica de la doctrina judicial mayoritaria, que muestra su fundada expectativa de corrección de la jurisprudencia nacional, la STS 119/2018, de 8 de febrero (caso Inditex) se alinea con el precedente constitucional de la STC 170/2013 -invocada por la empresa en sus recursos de suplicación y de unificación de doctrina- y considera que no hay ni una sola razón para entenderla corregida por el TEDH. Consecuentemente, en un caso típico de control informático sin consentimiento del trabajador, aunque mediaba conocimiento de la prohibición de uso personal de dispositivos móviles propiedad de la empresa y de la posibilidad de ser sancionado en tal caso, con resultado de despido del trabajador²⁶, el TS lo avalará, validando la prueba tecnológica anulada en suplicación social. Para el TS la utilización del ordenador queda dentro del ámbito de poder de vigilancia y por ello su ejercicio se ampara en el art. 20 ET y no tiene las limitaciones de la función de «policía privada» ex art. 18 ET, sino las genéricas del principio de proporcionalidad. Y, a tal fin, nada nuevo añadiría la STEDH de 5 de septiembre de 2017 [Caso «Barbulescu»], ya que, sin perjuicio de calificarlos como «prolijos», para el TS, los criterios del TEDH serían «sustancialmente coincidentes con los de la jurisprudencia constitucional» (SSTC 241/2012 -con voto particular- y 170/2013). Por tanto, en el caso concreto:

“la conducta empresarial...pasa holgadamente el filtro de los requisitos que el Alto Tribunal europeo exige para atribuir legitimidad a la actividad del grado de intromisión del empresario”.

De este modo, una vez sintetizados, genéricamente, cuáles son tales criterios (una razón justificativa empresarial legítima de la monitorización; inexistencia de un medio menos intrusivo para la consecución del objetivo, el destino dado por la empresa al resultado del control y la previsión de garantías para el trabajador), concluirá que no hay nada de nuevo en ellos, ni respecto de la doctrina constitucional ni de la propia:

“...pues sin lugar a dudas los factores que acabamos de relatar y que para el TEDH deben tenerse en cuenta en la *obligada ponderación de intereses*, creemos que se reconducen básicamente a los tres sucesivos juicios de «idoneidad», «necesidad» y «proporcionalidad» requeridos por el TC y a los que nos hemos referido en el FD Quinto [5.b)]. Juicios que a nuestro entender han sido escrupulosamente respetados en el caso de autos, por las razones más arriba expuestas [FJ Sexto. 2]”

²⁶ En la empresa existe una concreta normativa empresarial «de los sistemas de información» y de «política de seguridad de la información» del Grupo Inditex, que limita el uso de los ordenadores de la empresa a los estrictos fines laborales y que prohíbe su utilización para cuestiones personales. Los empleados del Grupo Inditex, cada vez que acceden con su ordenador a los sistemas informáticos de la compañía, y de forma previa a dicho acceso, deben de aceptar las directrices establecidas en la Política de Seguridad de la Información del Grupo Inditex. El examen del ordenador utilizado por el trabajador accionante fue acordado tras el «hallazgo casual» de fotocopias de las transferencias bancarias efectuadas por un proveedor de la empresa en favor del trabajador demandante -prohibido en el Código de Conducta de la demandada e imputado en la carta de despido-.

Incomprensiblemente, el TS reduce la evolución jurisprudencial del TEDH a casi una caricaturización de la misma, volviendo al momento originario: el más puro o estricto juicio de proporcionalidad. Sin poder entrar aquí y ahora en profundidad sobre tan importante cuestión, parece más que evidente que no puede -ni debe- despacharse de este modo tan simple la evolución jurisprudencial del TEDH. Primero, porque resulta manifiesto que sí contiene una novedad determinante respecto de los precedentes, y es que no cabe una prohibición absoluta de usos no laborales de los dispositivos digitales o tecnológicos, porque éstos tienen una inexorable “vertiente social”. Por lo tanto, frente a lo sostenido por el TS español, e incluso por el TEDH en el precedente *Copland*, no es posible atribuir a la eventual normativa o política de empresa sobre usos de este tipo de dispositivos una condición de canon determinante, sí relevante, pero no definitivo. En segundo lugar, siempre ha de darse una información específica previa, adaptada a la normativa de protección de datos, de modo que su ausencia debe ser excepcional. Finalmente, en todo caso, la proporcionalidad no debe ser abstracta, sino concreta, de modo que no suponga el sacrificio absoluto del derecho a la privacidad en aras de la mayor eficacia del poder empresarial, cuya legitimidad de “origen” -incluso constitucional- no se discute, pero sí se debe ponderar más seriamente la de ejercicio.

No nos resuelve esta sentencia de la sala social del TS la importante cuestión de los efectos de la nulidad de la prueba tecnológica en la calificación del despido, cuando medien otras pruebas que puedan acreditar la existencia de infracción. Una lástima, pues el caso concreto ofrecía una magnífica oportunidad para ello.

En efecto, la suplicación gallega había anulado la prueba tecnológica, pero no declaró la nulidad del despido, sólo su improcedencia. De haberse estimado vulnerado el derecho fundamental también por la sala social del TS, tendría que haber entrado en dicha cuestión. La rehabilitación de la prueba tecnológica impide obtener respuesta a este importante aspecto de la temática que, como hemos visto, no tiene una respuesta uniforme en suplicación y, en consecuencia, exigirá, más pronto que tarde, de una intervención unificadora, ya que “...no existe jurisprudencia unificadora ni opinión judicial ni doctrinal unánime”.

Hemos visto, al respecto, cómo la STSJ Castilla-La Mancha, 25/2018, de 12 de enero, que recoge otras precedentes, contando ya con sentencias posteriores dirigidas en un mismo sentido, asume la doctrina de la nulidad sólo de la prueba que viola el derecho fundamental. Pero la sala de suplicación vasca, desde 2011 hasta hoy, se inclina por la doctrina de la doble nulidad -de la prueba y del despido-, si bien no suele incluir la indemnización adicional. Una medida de justicia resarcitoria y disuasoria ex art. 183 LRJS que sí incorporan recientes sentencias de instancia, que aplican la contemporánea jurisprudencia social: la violación de un derecho fundamental conlleva automáticamente indemnización, fijándose la cuantía conforme al “baremo sancionador”, si no media lesión biológica (ej.: SJS

Madrid n. 19, 453/2017, 17 de noviembre, que recuerda, para la cuantificación del daño, el deber de ponderar un criterio legal -indemnización íntegra y disuasoria- y otro jurisprudencial -resarcimiento automático y validez del recurso a la norma sobre infracciones y sanciones para su determinación prudencial²⁷⁻)

A mi juicio, es evidente que la vulneración del derecho fundamental a través de pruebas tecnológicas contrarias a la privacidad de los trabajadores exige reparación específica, a través, cuando menos, de indemnización, también por la función disuasoria de la misma ex art. 183 LRJS. Más complejo es dar respuesta a si tal nulidad de la prueba contamina toda la decisión extintiva. Por lo que aquí más interesa, el impacto de la jurisprudencia del TEDH, parece claro que ésta se orienta a reconocer una indemnización por daño moral -pírrica, lamentablemente-, sin perjudicar la suerte del resto del proceso, como el *caso Ribalta* enseña claramente.

5. IMPACTO DEL TEDH EN EL LEGISLADOR PROYECTADO: LA CARTA DE “CIUDADANÍA LABORAL DIGITAL RESPONSABLE”

Si las novedades de la jurisprudencia del TEDH en materia de privacidad del trabajador son manifiestas, y los contrastes con la jurisprudencia nacional también -aún menor de lo que reivindicán ciertas posiciones maximalistas-, pero el TS se resiste al más mínimo reajuste de su Derecho de precedentes, por estimarlo conforme con aquélla *¿no debe ser el tiempo del legislador para convertir la nueva palabra jurisprudencial del TEDH en palabra de ley nacional, tan augurada doctrinalmente (idealismo) como ausente (realismo jurídico)? ¿No ha llegado la hora esa anhelada intervención legal, que ponga fin a la función de suplencia jurisprudencial, modernizando nuestro Derecho legislado, corrigiendo las múltiples lagunas y contradicciones persistentes, aumentando la seguridad jurídica del Derecho de precedentes, cada vez más imprevisible?*

Sin entrar ahora en la mayor o menor dosis de realismo, o al contrario de falacia, de este análisis²⁸, que parece fiar siempre las soluciones de todos los problemas a un legislador mesiánico y completo, casi taumatúrgico, que todo lo vería, lo sabría y lo resolvería con su acción, cuando es bien sabido que ni la calidad de

²⁷ Para un completo e innovador análisis de esta evolución jurisprudencial, a cargo de diversos profesionales de la jurisdicción y la abogacía, así como de la academia científica, vid. el monográfico sobre “*Nuevos fragmentos de “justicia resarcitoria” en el orden social: persistentes lagunas y antinomias*”. RTSS-CEF, N. 421, abril 2018, pp. 97-144

²⁸ Apela a ese legislador, tras asumir el contraste entre la doctrina constitucional y la del TEDH, Casas Baamonde, M.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*”, Editorial Derecho de las Relaciones Laborales, febrero de 2018. De “idealismo utópico” habla, en cambio, Lousada Arochena, J.F. “Derecho fundamental a la protección de datos personales vs. Facultad empresarial de video-vigilancia”. En AAVV (Dir. Efrén Borrajo). “*Controversias vivas del nuevo Derecho del Trabajo*”, La Ley, Madrid, 2015, p. 415.

las leyes de este tiempo suele brillar ni es suprimible el juicio valorativo inherente a toda interpretación, parece claro que ha llegado el día de tal intervención, imperativo de modernización inexcusable en nuestra era digital. Y para dar concreción práctica a este requerimiento legislativo resulta de interés referir al *proyectado art. 20 bis ET*, que la norma básica laboral incorporaría de ver finalmente la luz el Proyecto de Ley de protección de datos (LPDP), en la versión propuesta por su nuevo Título X, debido a la Enmienda del Grupo Socialista -hoy en el Gobierno-. En un solo precepto laboral se propone incluir una suerte de carta de derechos fundamentales de ciudadanía laboral digital responsable en las empresas, especificando en este ámbito los derechos de ciudadanía digital en general. Junto al reconocimiento del “derecho a la desconexión digital” -vinculado no sólo a la privacidad, sino también a la salud laboral-, tendría un especial protagonismo el “derecho a la intimidad digital” (arts. 86 y 88 proyectada nueva LPDP).

Aunque tampoco podemos entrar aquí en un aspecto tan relevante del futuro Derecho Legislado de protección de la privacidad del trabajador, sí es útil, incluso necesario, a fin de ponderar la verdadera innovación jurídica de esa regulación propuesta, de llegar a buen puerto (con la publicación de la norma tal y como ahora está tramitándose), compararla con la estudiada jurisprudencia del TEDH. Una comparación importante porque, a mi juicio, en línea con lo que sostiene un reciente y autorizado sector doctrinal²⁹, esta reforma legislativa no tendría más sentido que convertir en Derecho legislado lo que ahora es Derecho jurisprudencial, por obra y arte del TEDH. No sólo llama (1) a una *política*, mejor pactada, de usos socio-económicamente responsables de dispositivos digitales (GPS, cámaras de vigilancia, auditorías informáticas, etc.), mediante Códigos de Conducta incluidos en convenios, sino también a (2) un *deber de información previa* útil, tienen el código genético del TEDH, en particular de la *sentencia Barbulescu*, *sin perjuicio de eventuales excepciones en aras de la efectividad de los derechos de los empleadores* -libertad de empresa, tutela judicial efectiva-, según los precedentes *Köpke y Libert*.

Quizás pueda desilusionar la escasa ambición de esta reforma; pero no puede sorprender, porque 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 acompasar el ritmo del Derecho, habitualmente lento, y el del cambio tecnológico, usualmente vertiginoso, a fin de evitar que una norma nazca ya envejecida. Ciertamente, la protección de la privacidad del trabajador en el entorno de las tecnologías digitales (incluidas las redes sociales -web 2.0: toda utilidad o servicio de Internet sustentado en una base de datos que puede ser modificada por los usuarios, en su contenido y/o en su forma de presentarlos-), ocupan hoy un papel notable en la vida de un buen número de personas, por lo

²⁹ Vid. Miñarro Yanini, M. “La “Carta de derechos digitales” para los trabajadores del Grupo Socialista en el Congreso: un análisis crítico ante su renovado interés”. RTSS-CEF, 424, julio 2018, pp. 104-105.

tanto también de trabajadores, por lo que afecta de forma profunda a su esfera de privacidad, incluso de su mayor intimidad. En última instancia, las bases de datos en las que se basa corresponden a informaciones clásicamente protegidos por los derechos a la intimidad y a la propia imagen, como derechos inherentes a la personalidad, en el plano de las relaciones civiles, y como derechos fundamentales, en el plano de las relaciones de ciudadanía -no solo política, sino social-.

Por lo tanto, a una evolución más acelerada de las comunidades virtuales mayores riesgos también. Por enésima vez, la realidad se desarrolla ambivalente y el legislador no puede ser ajeno, aunque eso genere ambigüedad reguladora. De una oportunidad de reconstrucción de una suerte de ágora global para las personas, al modo de una gran plaza donde todas las personas actúan como ciudadanos libres, también, por tanto, responsables, participando en las decisiones y en la crítica (social, política, e incluso económica), cabe igualmente derivar hacia una “plaza de escarnio público”, en el que junto a la crítica más visceral se produce también el máximo exhibicionismo (de la “*intimidad a la extimidad*”). La acumulación de datos personales en esas redes permite que sean procesados, a partir de “Big Data” para ir más allá, de modo que “se reconstruya la personalidad” (gustos, forma de pensar, capacidades, necesidades...), por lo tanto en todas sus facetas, también la laboral. A partir de ahí entraría en juego la “Web 2.0” (inteligente o semántica -añade contenidos propio a partir de los datos compartidos y procesados-)³⁰.

Quien “controla los datos personales” (información) no sólo controla el mercado (multiplicando de esta forma sus ganancias), sino que puede igualmente “controlar a las personas”. El problema es que el “objeto de comercio” (mercancía) es nada menos que “informaciones pertenecientes a la esfera de la personalidad”. Por lo tanto, a medida que crece la dependencia de un mayor número de personas de estos dispositivos o instrumentos tecnológicos (digitales) en las distintas facetas de la vida de la persona, privadas y laborales, diluyéndose la frontera, se hace necesaria una mayor capacitación de las personas en el manejo de esa información propia, a fin de facilitar el control personal y dificultar, en contrapartida, los malos usos, por supuesto también laborales³¹. Aunque este aspecto parece vincularse más con otro derecho fundamental, como es el derecho de crítica asociado a la libertad de expresión, a partir del cual también pueden desarrollarse atentados contra otros derechos fundamentales de la persona del trabajador (por ejemplo en la acoso moral digital o cibernético), los riesgos para la privacidad son evidentes, evidenciando *la vulnerabilidad de la identidad del usuario*³².

³⁰ Vid. O'Reilly, T. “*Qué es Web 2.0. Patrones del diseño y modelos de negocio para la siguiente generación de software*”. En Telos. Cuadernos de Comunicación e Innovación, 2004, pp.13-14.

³¹ Grupo de Trabajo sobre Protección de Datos del Artículo 29. Dictamen 5/2009, sobre las redes sociales en línea. CE, 2009: “*los riesgos visibles...de las redes sociales son solo la punta del iceberg*”.

³² Vid. AEPD-INTC. Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online, 2009.

De ahí la centralidad de la dimensión social -proactiva, no sólo negativa- de la vida privada del trabajador en la empresa acotada por el TEDH. En consecuencia, actuaría como un auténtico contrapoder frente al poder (no sólo de control) empresarial, creando sea mecanismos de auto-tutela (límites) sea obligaciones positivas (deberes de hacer) para el poder empresarial, y viceversa, naturalmente, en aras del inexorable, y complejo, equilibrio entre derechos e intereses legítimos, con clara trascendencia constitucional.

Esto pone en cuestión toda la doctrina constitucional y jurisprudencia nacionales sobre diversos aspectos de esta dimensión de la vida privada en el seno de las empresas y de las relaciones de trabajo que en su seno se contraen. Por supuesto, en relación a cómo han de jugar los “límites de los límites”, esto es, la extensión y límites del poder de información empresarial sobre las conductas y capacidades de la persona de los trabajadores (vertiente negativa o deberes de respeto), pero también respecto de los márgenes de usos particulares de los medios de comunicación propiedad empresarial a fin de hacer realidad ese derecho a la vida en privado. En consecuencia, frente al juicio abstracto y laxo de proporcionalidad del poder de control empresarial se impondrá un juicio más concreto y constrictivo de proporcionalidad, al tiempo que, frente a la opción de prohibición absoluta de usos privados de tales medios propiedad de la empresa, se impondrá el derecho a usos sociales razonables de tales dispositivos, así como a utilizar, también de forma razonable, los propios (“BYOD”).

Qué duda cabe que la dinámica protectora actual del derecho a la privacidad viene marcada por la evolución comunicativa digital. La conjunción de esta realidad (el plano de observación sociológica de las reglas) y de las reformas legales (el plano de observación normativa), a partir de la nueva valoración social de la cuestión de la protección de datos personales (el plano de observación axiológica), marcará una nueva etapa en la conformación del derecho al respeto de la vida privada y familiar. Y ello en su dimensión internacional (derecho humano), constitucional (derecho fundamental) y civil (derecho de la personalidad), hasta lograr una notable preferencia política y socio-económica, “*mucho más allá de la tradicional protección civil y penal de la esfera privada de una persona*”³³, en general, y del trabajador en particular.

6. LECTURAS SOCIALES “INDIRECTAS” DE LA JURISPRUDENCIA CIVIL DEL TEDH SOBRE PRIVACIDAD

Si bien no podemos ir más allá en el análisis del impacto nacional del reciente Derecho de precedentes europeo sobre la protección de la privacidad del trabajador, tampoco se puede renunciar a dejar constancia de algunas otras manifesta-

³³ Vid. Orozco Pardo, G. *Comentario al artículo 7 CDFUE*. En AAVV (Dirección y Coordinación: Cristina Monereo Atienza- J.L. Monereo Pérez). *La Europa de los Derechos. Estudio sistemático de la CDFUE*. Editorial Comares. Granada. 2012. p. 137.

ciones, aún indirectas, de la dimensión “social” de este derecho “civil”. La fuerza expansiva del mismo puede comprobarse en la STEDH 26 de abril de 2018 (caso ČAKAREVIĆ v. CROACIA, reclamación n. 48921/13). Un trabajador croata, al que el servicio público de empleo reclamó ciertas prestaciones sociales indebidas, invoca para oponerse a tal acción pública de reintegro de prestación por desempleo -si bien realizada en vía civil- tanto “su derecho al disfrute pacífico de sus bienes” (derecho de propiedad), como “su derecho al respeto de su vida privada”. Aunque el TEDH resuelve el asunto de forma favorable al trabajador en atención al derecho de propiedad -derecho patrimonial por antonomasia que ha consolidado una vertiente social determinante en el TEDH-, acepta plantear la cuestión también sobre el derecho a la privacidad, lo que negaba el gobierno croata, si bien no hace mayores consideraciones jurídicas porque entiende aplicables los mismos argumentos que para el derecho de propiedad que acaba de proteger³⁴.

Más interés práctico presenta el uso social expansivo que de este derecho civil y de su jurisprudencia europea ha hecho la sala social del TS español, en contra de la interpretación de su sala civil (STS, 1ª, 6 de febrero de 2014, rec. 245/2012), para las prestaciones de seguridad social -y los correlativos permisos parentales en las relaciones de trabajo- de “maternidad subrogada”. Si bien el TEDH acepta la legitimidad de la prohibición de este tipo de maternidad, validando las normas nacionales que la prohíben y las prácticas administrativas que impiden consolidar este tipo de vínculos familiares (STEDH de 24 de enero de 2017, caso Paradiso y Campanelli contra Italia), siempre y cuando quede garantizada la protección del interés superior del menor (a través, por ej., de la adopción o la acogida), la sala social del TS ha dado -incomprensiblemente- una lectura social maximalista a esta jurisprudencia y deriva la necesidad de equiparar su protección en el ámbito social (últimamente STS, 4ª, 347/2018, 22 de marzo).

Desde el prisma que aquí interesa, la relación de esta cuestión con el derecho a la protección de la vida privada y familiar ex art. 8 CEDH, el presupuesto fundamental seguido por la jurisprudencia nacional se concreta, erradamente, del siguiente modo:

“Las normas en materia de protección de la maternidad han de ser interpretadas a la luz del principio general del interés superior del menor que se integra en el núcleo familiar con el progenitor o progenitores que le prestan atención y cuidados parentales, conforme a lo establecido en el art. 8 CEDH... designio que ha de prevalecer y servir de orientación para la solución de cualquier duda exegética, así como de acuerdo a la «realidad social del tiempo en que han de ser aplicadas, atendiendo fundamentalmente al espíritu y finalidad de aquella» (art. 3.1 del Código Civil -CC -)”.

³⁴ El TEDH no duda en darle la protección asentada en el derecho a la propiedad, porque, debiéndose el percibo indebido a una decisión administrativa errónea, para la que no hay contribución alguna del actuar del perceptor, la revocación necesaria para el interés general debe dirigirse hacia el futuro (ex nunc), pero no hacia el pasado (ex tunc), pues tiene una expectativa legítima de conservación, en virtud del artículo 1 del Protocolo núm. 1 (protección de la confianza legítima y del estado de necesidad -y de salud-).

A partir de este razonamiento -que en nada tiene que ver con la jurisprudencia del TEDH, como se acaba de mencionar, que rechaza identificar el interés superior del menor con mantener la relación de maternidad subrogada-, concluye -también de una forma incorrecta, a mi juicio- un mandato de trato igual de la maternidad subrogada en relación a la maternidad -natural o jurídica-, pues "... con independencia de que la maternidad subrogada no figure como tal y de forma expresa en el elenco de situaciones previstas", pugnaría:

"...con la lógica más primaria que se deniegue la prestación en los supuestos de gestación por sustitución cuando se reconocería *ex lege* si el solicitante se hubiera limitado a adoptar o a acoger a los menores..." (FJ Segundo, punto 2, 2º in fine).

Pero ¿qué lógica tan primaria es esa que no admite discusión? Recuérdese que el Derecho español prohíbe esa modalidad de gestación (nulidad de pleno derecho del contrato de gestación por sustitución ex art. 10 de la Ley 14/2006, de 26 de mayo), y que lo protegido es el cuidado del menor, no el modo concreto de llevarlo a cabo. Quizás no está de más recordarle a la Sala social del TS lo que realmente la Gran Sala del TEDH -que aquélla no se digna referir, ignorando este precedente por completo- ha dicho a este respecto:

"...no se puede establecer la existencia de unos lazos familiares que deban ser protegidos por el Derecho cuando esos lazos se han constituido en violación de la ley"

En este planteamiento es unánime el TEDH. Varios votos concurrentes añaden, además, desde un plano más axiológico, al tiempo que realista:

"la maternidad subrogada, en todas sus modalidades, es contraria a la dignidad humana porque trata a la gestante y al niño como medios al servicio del cumplimiento de los deseos de los contratantes, y no como fines en sí mismos".

Tampoco aquí se ajusta la sala social del TS a la jurisprudencia europea más reciente en materia, aunque en este caso tenga un sentido "proteccionista", falsamente "progresista". En todo caso, sí sirve para ilustrar la capacidad expansiva e innovadora en lo socio-laboral de este clásico derecho civil

7. EPITOME: EN BUSCA -PERMANENTE- DEL JUSTO EQUILIBRIO

Pero tradicional, clásico o moderno, una realidad es incuestionable: tanto la legislación como la jurisprudencia están llamados a procurar la "justa conciliación" entre la protección de los derechos fundamentales (en este caso a la privacidad) y los beneficios económicos del desarrollo tecnológico, también en la gestión laboral. De ahí, la necesidad más de perfeccionamiento que de profunda renovación de los conceptos jurídicos. La era digital realiza un "nuevo contexto" para "viejos" derechos, añadiéndole nuevas vertientes, pero sin que por ello lleve

a una “revolución” en el arsenal de conceptos y métodos jurídicos. Entre ellos está la técnica de la ponderación de derechos, tan sabia y prudentemente desarrollada por el TEDH en esta materia.

Cierto, ponderar derechos y libertades fundamentales -entre las que están hoy la propiedad y la libertad de empresa, guste más o menos a los laboristas- no es tarea fácil respecto de derechos como la privacidad, complicándose mucho más cuando se trata de contextos complejos y singulares, como el laboral. Por eso, la función judicial siempre consistirá, diga lo que diga concretamente el Derecho Legislado, en hallar, para cada caso, el justo equilibrio entre tales derechos fundamentales. Por supuesto, los jueces deben conocer mejor qué alcance tienen los desarrollos tecnológicos, para evitar resolver identificando sin más la nueva realidad virtual como si fuese solo equivalente a la analógica precedente (los archivos del ordenador como si fuesen archivos en papel). Pero también deben asumir nuevos usos sociales (incluidos los privados y familiares) que derivan de tal desarrollo respecto de los dispositivos tecnológicos productivos. De ahí la necesidad de más diálogo y cooperación y menos conflicto -entre tribunales³⁵-.

³⁵ Vid. A. LAZARI. «El paradigma conceptual de los jueces tejedores», en J. DIEZ-HOCHLEITNER y otros (coord.). Últimas tendencias en la jurisprudencia del TJUE (2008-2011), La Ley, Madrid, 2012, pp. 209-236.