El presente volumen pretende analizar, a través de cuatro trabajos concretos, el cambio de paradigma que la revolución tecnológica ésta provocando en el proceso. Se abordan así, por un lado, dos temas que si bien traen causa de realidades extraprocesales de gran relevancia jurídica, dejan sentir su efecto en el proceso planteando cambios y reflexiones de profundo calado: uno, el valor probatorio que puede alcanzar la información digital obtenida por el empresario (audios, videos, correos electrónicos…) en el ejercicio de su potestad de control sobre el trabajador; y otro, el impacto que van a generar en el proceso los nuevos mecanismos de protocolos computerizados de transacción y de registro basados en tecnología blockchain.

Pero la irrupción tecnológica afecta también a la propia Administración de Justicia. Y, en ese sentido, dos estudios de los contenidos en el presente volumen profundizarán, por un lado en el uso (y la protección) de los datos personales en el seno del proceso; y, por otro, en la exclusión que origina la brecha digital en el acceso a la Justicia por parte de determinados colectivos ciudadanos: singularmente quienes afectados por condiciones económicas desfavorables (pobreza) y por razones edad (personas mayores) van a tener un nulo o muy limitado acceso y/o manejo de las nuevas realidades tecnológicas.

Títulos de Cuadernos digitales. Derecho y Nuevas Tecnologías:

1. *Derecho internacional privado, contratación internacional en internet y régimen jurídico del comercio electrónico.*
2. *La digitalización en los procedimientos administrativos y en los procedimientos contencioso-administrativos.*

DIPUTACIÓN DE ALICANTE

CENID CENTRO DE INTELIGENCIA DIGITAL PROVINCIA DE ALICANTE

LEGALTECH UNIVERSITAS Miguel Hernández

C.M.: 75095

ISBN: 978-84-1124-783-2

9 788411 247832

TECNOLOGÍA Y PROCESO. PROBLEMAS PROCESALES EN UN MUNDO DIGITAL

OLGA FUENTES SORIANO
COORDINADORA

JOSÉ ANTONIO PÉREZ JUAN
FRANCISCO JAVIER SANJUÁN ANDRÉS
DIRECTORES CUADERNOS DIGITALES. DERECHO Y NUEVAS TECNOLOGÍAS

INCLUYE LIBRO ELECTRÓNICO **THOMSON REUTERS PROVIEW™**

THOMSON REUTERS ARANZADI

TECNOLOGÍA Y PROCESO. PROBLEMAS PROCESALES EN UN MUNDO DIGITAL

THOMSON REUTERS ARANZADI

OLGA FUENTES SORIANO
Coordinadora

TECNOLOGÍA Y PROCESO. PROBLEMAS PROCESALES EN UN MUNDO DIGITAL

Olga Fuentes Soriano
Eloy Velasco Núñez
Manuel Richard González
Paloma Arrabal Platero

Cuadernos Digitales. Derecho y Nuevas Tecnologías

Directores
JOSÉ ANTONIO PÉREZ JUAN
FRANCISCO JAVIER SANJUÁN ANDRÉS

THOMSON REUTERS
ARANZADI

Primera edición, 2022

THOMSON REUTERS PROVIEW™ eBOOKS
Incluye versión en digital

Proyecto ***"Abogacía Digital: Derecho y Nuevas Tecnologías"*** *referencia DIPU1.21X-3* que forma parte del *Convenio de colaboración* entre la Excma. Diputación Provincial de Alicante y la Universidad Miguel Hernández, en el marco de la *Transformación digital de la Provincia de Alicante* (**CENID, Centro de Inteligencia Artificial de la Provincia de Alicante**, iniciativa de la Diputación y las Universidades de Alicante y Miguel Hernández).

Editorial Aranzadi, S.A.U.
Camino de Galar, 15
31190 Cizur Menor (Navarra)
ISBN: 978-84-1124-781-8
DL NA 1080-2022
Printed in Spain. Impreso en España
Fotocomposición: Editorial Aranzadi, S.A.U.
Impresión: Rodona Industria Gráfica, SL
Polígono Agustinos, Calle A, Nave D-11
31013 – Pamplona

Índice

Página

Página

Página

Thomson Reuters ProView. Guía de uso

Capítulo 1

El valor probatorio de la información digital captada por el empresario: grabaciones y comunicaciones electrónicas[1]

Olga Fuentes Soriano

Catedrática de Derecho Procesal
Universidad Miguel Hernández (Elche. España)

SUMARIO: I. INTRODUCCIÓN. II. LA VIDEOVIGILANCIA EMPRESARIAL. 1. *Derechos fundamentales afectados*. 2. *Exigencias probatorias de la grabación de la actividad laboral: STEDH López Ribalda II*. 3. *La compleja unificación de doctrina tras López Ribalda II: el TS se pronuncia; consecuencias*. III. EL CONTROL EMPRESARIAL DE LAS COMUNICACIONES Y DE LOS DISPOSITIVOS INFORMÁTICOS PUESTOS A DISPOSICIÓN DEL TRABAJADOR. IV. LA EVOLUCIÓN DE LA REGLA DE EXCLUSIÓN ANTE LAS NUEVAS PRUEBAS TECNOLÓGICAS. V. BIBLIOGRAFÍA.

1. Este trabajo forma parte del proyecto de investigación "Empresa y Proceso. Cooperación e investigación" (PID2020-119878GB-I00) obtenido en el marco del "Programa Estatal de generación de conocimiento y fortalecimiento científico y tecnológico del Sistema de i+d+i y del Programa Estatal de I+D+i orientada a los retos de la sociedad", del Ministerio de Ciencia e innovación. He tenido oportunidad de discutir su contenido con el profesorado del área Derecho Procesal de las Universidades de Alicante, Castilla-La Mancha (Cuenca) y Miguel Hernández en diversos seminarios; quiero, en esta nota, dejar constancia de mi agradecimiento por las valiosas reflexiones que surgieron en todos y cada uno de ellos. Asimismo, agradezco particularmente las acertadas sugerencias que, tras la lectura del trabajo, me trasladaron Antonio Sempere Navarro (Catedrático de Derecho del Trabajo y de la Seguridad Social y Magistrado del Tribunal Supremo –Sala Cuarta–), Mercedes Fernández López (Profesora Titular de Derecho Procesal de la Universidad de Alicante) y Paloma Arrabal Platero (Profesora Ayudante Doctora de la Universidad Miguel Hernández).

RESUMEN

El desarrollo tecnológico pone en manos del empresariado la posibilidad de adoptar medidas que le permitan controlar la actividad laboral con muy bajo coste y escasa inversión si bien afectando, en ocasiones gravemente, los derechos fundamentales de los trabajadores. Encontramos en este ámbito medidas como (*v.gr.*) la instalación de videocámaras o el control del uso que el trabajador realiza de los medios informáticos que el empresario ha puesto a su disposición. El objetivo de este trabajo es hallar el límite que permita conjugar los intereses de ambos; así como clarificar la paradójica situación generada en los últimos años en los que, al hilo de nuestra evolución jurisprudencial, ha podido llegar a afirmarse que una misma prueba válida para sustentar un despido en el ámbito social, ha sido considerada nula para fundamentar una condena penal, por haber sido obtenido con vulneración de derechos fundamentales.

PALABRAS CLAVE

Prueba prohibida; regla de exclusión; derechos fundamentales; videovigilancia; control empresarial; secreto de las comunicaciones; protección de datos; derecho al propio entorno virtual.

I. INTRODUCCIÓN

Los vaivenes jurisprudenciales a que asistimos en los últimos años sobre la posible admisión de la prueba obtenida con vulneración de derechos fundamentales han encontrado propicio caldo de cultivo en la virtualidad probatoria de las pruebas tecnológicas. En justicia, cabría admitir que la inseguridad que generan las diversas interpretaciones susceptibles de encontrar amparo en el art. 11.1 LOPJ son muy anteriores al auge tecnológico; pero no es menos cierto que algunos rasgos característicos de las evidencias digitales han acelerado el proceso de deconstrucción de la prueba prohibida y la teoría de los frutos del árbol envenenado.

Si en el trasfondo de la prueba prohibida subyace la idea de que la verdad no puede obtenerse a cualquier precio, la necesidad de reconocer procesal y penalmente la evidencia delictiva que ponen de manifiesto determinadas pruebas (*v.gr.* el video con la grabación de un delito) obliga a articular mecanismos que permitan su toma en consideración. De este modo, como he sostenido en alguna ocasión, ni

la verdad puede obtenerse a cualquier precio, ni puede obviarse sin mayor consideración[2].

En mi opinión, hubo un detonante que asestó un golpe mortal en la línea de flotación de la prueba prohibida como mecanismo de protección de los derechos fundamentales. Se trató de la STS (Sala 2.ª) 528/2014, de 16 de junio, en la que el TS reconoce que una prueba (unos correos electrónicos obtenidos por el empresario) que es válida para fundamentar el despido de un trabajador en el orden social, no es válida para fundamentar su condena en el orden penal (¡la misma prueba!), por haber sido obtenida con vulneración de derechos fundamentales. Aunque a profundizar sobre ello se dedicará el epígrafe 3 de este trabajo, cabe señalar ahora que este diferente valor que el TS reconoció a una información probatoria obtenida con vulneración de derechos fundamentales (admisible en lo Social; inadmisible en lo Penal) obligaba a repensar el fundamento de la prueba prohibida, para plantearnos si la deriva jurisprudencial nos acercaba ya, decididamente, a ese carácter disuasorio (*deterrent effect*) que subyace en el modo en el que, en el Common Law, se justifica la regla de exclusión probatoria[3].

Entiendo que, en esta reorientación jurisprudencial, hay dos factores que han jugado un rol fundamental: uno, el fácil acceso de los particulares, a través de mecanismos tecnológicos, a informaciones (potenciales pruebas) incriminatorias que, aunque pueden haber sido obtenidas con una ¿leve, cierta, ligera? vulneración de derechos fundamentales, proporcionalmente al daño que infligen, lo son con muy escasa lesión; y otro, el amparo que en el entorno laboral, dichas pruebas encuentran en la potestad de control del empresario legislativamente garantizada. Precisamente esto es lo que ha convertido a este entorno laboral en el escenario clave para ensayar la protección de los derechos fundamentales a través de mecanismos distintos al de la exclusión probatoria.

En el presente trabajo trato de recoger algunas reflexiones sobre la evolución que la teoría de la prueba prohibida ha experimentado como mecanismo de protección de los derechos fundamentales, a la luz de esta particular situación que se genera, precisamente, en el ámbito

2. *Vid*. "La prueba prohibida aportada por particulares, a la luz de las nuevas tecnologías", en *Derecho Probatorio y otros estudios procesales. Liber Amicorum Vicente Gimeno Sendra*, (ASENCIO MELLADO, Dir.), Ed. Castillo de Luna, Madrid, 2020.

3. Sobre el fundamento y evolución de la regla de exclusión probatoria en los países del Common Law y los matices que lo separan respecto del de la teoría de la prueba prohibida que consagra el art. 11.1 LOPJ puede verse CUADRADO SALINAS, C., *Fundamento y efectos de la exclusión de la prueba obtenida con vulneración de derechos fundamentales,* Tirant lo Blanch, Valencia, 2021.

social pero cuya trascendencia se ha proyectado en todos los órdenes jurisdiccionales.

II. LA VIDEOVIGILANCIA EMPRESARIAL

El auge tecnológico alcanzado en el S. XXI pone en manos de los ciudadanos la posibilidad de grabar, con un coste mínimo –nótese que es tecnología ínsita en cualquier Smartphone o Tablet, al margen de mecanismos de mayor sofisticación–, escenas cotidianas, de carácter laboral, público o privado que pueden resultar enormemente valiosas llegado el momento de acreditar una actuación determinada o la realización de una conducta ilícita, o incluso delictiva; pero sin necesidad de ir tan lejos, ponen al alcance de la ciudadanía potentes instrumentos de control que, a cambio, van a entrar en colisión –o cuanto menos en tensión– con diversos derechos fundamentales de las personas grabadas.

Desde esta perspectiva, la aportación de una videograbación como material probatorio para acreditar el acometimiento de una conducta determinada, va a poner de manifiesto una paradoja jurídica y socialmente, de difícil solución: por un lado ese video puede ser el reflejo inequívoco –"la prueba" en términos coloquiales, no estrictamente legales– de una conducta jurídicamente desviada y, consecuentemente, socialmente reprobable; y, sin embargo, pese a la evidencia, es posible que acabe sin alcanzar valor probatorio alguno cuando, por la forma en que se llevó a cabo su grabación, hubiera sido obtenida con vulneración de derechos fundamentales (piénsese en el derecho a la intimidad, a la privacidad, al secreto de las comunicaciones o a la protección de datos, entre otros posibles, de la persona grabada)[4].

Esa es, precisamente, la consecuencia que impone la regla de exclusión probatoria: la expulsión del proceso de aquella prueba obtenida con vulneración de derechos fundamentales. Huelga, no obstante, insistir hoy en el hecho de que son muchas las excepciones que, con el fin de hacer justicia en el caso concreto, la Jurisprudencia ha ido encontrando para salvar aquellas pruebas que, aun obtenidas con indirecta

4. He tratado esta cuestión en algunos trabajos previos, pero en lo que se refiere, concretamente, a la prueba digital, puede verse "Vídeos, comunicación electrónica y redes sociales: cuestiones probatorias", Revista Práctica de Tribunales núm. 135, noviembre-diciembre: La prueba pericial en el proceso civil: proposición y valoración, Wolters Kluwer, 1 de noviembre de 2018.

vulneración de derechos fundamentales, reflejan una evidencia tal de la comisión del hecho delictivo que no permiten al juez obviar su valoración. Su toma en consideración ha sido justificada con argumentos tales como la convalidación de la prueba por el afectado (*v.gr.* reconociendo los hechos), la conexión de antijuricidad o la buena fe en su obtención, entre otros[5]. En realidad, es tal la extensión alcanzada por esta nueva tendencia a permitir una interpretación flexible en relación con la posibilidad de valorar la prueba obtenida con vulneración de derechos fundamentales que se ha llegado a justificar no sólo la toma en consideración de la prueba indirectamente obtenida sino, incluso, la de la prueba directa siempre y cuando su utilización no determine la vulneración del derecho a un proceso con todas las garantías (art. 24.2 CE)[6].

5. Del análisis de las posibles respuestas que no pasan, necesariamente, por la expulsión del proceso de la prueba obtenida con vulneración indirecta de los derechos fundamentales he tenido ocasión de ocuparme en "La prueba prohibida. Viejos problemas procesales de las nuevas tecnologías" (Coord. PRIORI POSADA. G.), *Justicia y proceso en el S,XXI. Desafíos y tareas pendientes*, Ed. Palestra, Perú, 2019.

6. Es, en suma, la conclusión a la que llega el TC en la Sentencia que resuelve el conocido como Caso Falciani (STC 97/2019, de 16 de julio). En su FJ 5 se sostiene que el art. 11.1 LOPJ "no se refiere a cualquier violación de derechos fundamentales sino (…) a la proscripción de utilizar instrumentalmente medios de investigación que lesionen estas titularidades primordiales (…). El sentido específico de la garantía del proceso debido incluida en el art. 24.2 CE es así, el de proteger a los ciudadanos de la violación instrumental de sus derechos fundamentales que ha sido verificada, justamente para obtener pruebas. (…) Fuera de tales supuestos, esto es, cuando no existe una conexión o ligamen entre el acto determinante de la injerencia en el derecho fundamental sustantivo y la obtención de fuentes de prueba, las necesidades de tutela de dicho derecho son ajenas al ámbito procesal y pueden sustanciarse en los procesos penales o civiles directamente tendentes a sancionar, restablecer o resarcir los efectos de la vulneración verificada en aquél" (STC 97/2019, de 17 de julio; FJ 5.°). Abundando en esta idea, se indica asimismo en la Sentencia que "la constatación de la violación originaria del derecho fundamental sustantivo (en este caso, del derecho a la intimidad) no determina por sí sola, sin embargo, la automática violación del derecho a un proceso con todas las garantías (art. 24.2 CE), generando la necesidad imperativa de inadmitir la correspondiente prueba. La apelación al art. 24.2 CE sería superflua si toda violación de un derecho fundamental sustantivo llevara consigo, per se, la consiguiente imposibilidad de utilizar los materiales derivados de ella. Si así fuera, la utilización de tales materiales dentro del proceso penal sería, de por sí, una violación del derecho sustantivo mismo (en este caso la intimidad) sin que el recurso al art. 24.2 CE para justificar la exclusión tuviera ninguna relevancia o alcance. Nuestra doctrina, como ya se ha expuesto, no impone semejante automatismo, sino que lleva, antes bien, a la realización de un juicio ponderativo de los intereses en presencia". Sobre pocos temas se

En todo caso, y dejando para un momento posterior el análisis de estas nuevas tendencias interpretativas en torno a la prueba prohibida, sí conviene destacar al objeto del presente trabajo que, uno de los ámbitos en los que las grabaciones están suscitando una mayor controversia ha pasado a ser, sin duda, el ámbito laboral. En él, mientras que, por un lado, la potestad de control del empresario sobre la buena marcha de la empresa ampara el uso –o, cierto uso– de estas grabaciones, por otro lado, el derecho a la intimidad o a la protección de datos del trabajador ampara su rechazo –o, cierto rechazo–. Así, mientras que el empresariado ha encontrado en este sistema una legítima fuente de control, extraordinariamente económica y fiable; los trabajadores han visto en él una clara amenaza a su derecho a la intimidad, vulnerado por la presencia constante y continua de ese ojo controlador omnipresente que vigila silenciosamente sus movimientos y actuaciones privadas, por mucho que producidas en un entorno laboral.

Con el fin de conciliar ambos intereses, a la paulatina elaboración de una línea jurisprudencial indicando qué tipo de grabaciones no tenían por qué resultar atentatorias a la intimidad del trabajador[7], se sumó la doctrina del TEDH acuñando la expresión "expectativa razonable de intimidad" para delimitar con ella la línea roja que marcaba su

ha escrito tanto en los últimos tiempos como sobre el caso Falciani resuelto por esta Sentencia; la cita, en consecuencia, de trabajos de referencia sería inagotable. Para una posición crítica sobre los efectos de la posición que en ella se sostiene *vid*., por todos, ASENCIO MELLADO, J.M., "La STC 97/2019, de 16 de julio. Descanse en paz la prueba ilícita", Diario La Ley, Núm. 9499, Sección Tribuna, 16 de Octubre de 2019. Por mi parte, desde posiciones más conciliadoras con las nuevas tendencias jurisprudenciales, he tenido ocasión de pronunciarme en "La prueba prohibida aportada por particulares, a la luz de las nuevas tecnologías", en, Ed. Castillo de Luna, Madrid, 2020. Y, desde luego, una clara y elocuente justificación doctrinal y didáctica de la tesis sostenida por la STS 116/2017, 23 de febrero de 2017 (posteriormente avalada por la STC 97/2019, de 16 de julio, que nos ocupa) puede encontrarse en el trabajo publicado por el propio ponente de la misma: MARCHENA GÓMEZ. M., "Prueba ilícita y reglas de exclusión: los matices introducidos por la Sala Penal del Tribunal Supremo en la Sentencia 116/2007, 23 de febrero (Caso Falciani)", en *Derecho Probatorio y otros estudios procesales. Liber Amicorum Vicente Gimeno Sendra,* cit. pp. 1181 a 1199.

7. En principio, no tendrá por qué resultar afectada la intimidad del trabajador cuando las grabaciones tengan lugar en espacios comunes de la empresa destinados exclusivamente al desarrollo de las obligaciones contractuales del trabajador, *v.gr.*, cajas registradoras de un supermercado…; a diferencia de las mayores controversias que suscita la posible grabación en un despacho que aun siendo de la empresa está destinado a un uso individual (STS 239/2014, de 1 abril) o, desde luego la prohibición de su uso en espacios tales como aseos o vestuarios (STS 620/1997, de 5 de mayo).

vulneración. A partir de esta construcción, se entendió que la posibilidad de recurrir a la instalación de cámaras y a sus consiguientes grabaciones en el entorno laboral no vulneraba el derecho a la intimidad de los trabajadores siempre que dichas grabaciones respetaran la "expectativa razonable de intimidad" que en función del caso concreto, cada trabajador podía esperar[8].

En este sentido, especialmente elocuentes resultan las consideraciones de la STS 239/2014, de 1 de abril, cuando distingue entre la afectación que, sobre el derecho a la intimidad de los trabajadores, produce la instalación de cámaras en una empresa distinguiendo entre las que se colocan frente a las cajas registradoras y las que se ubican en un despacho, sin haber cursado aviso previo a su usuario. Al respecto, sostiene dicha Sentencia que "las cámaras de grabación fueron instaladas al menos en dos lugares diferentes. En uno de ellos estaba la caja registradora, de la que se tomaba el dinero. Del contenido de la sentencia resulta que a ese lugar tenían acceso todos los trabajadores o, al menos, la generalidad de los mismos (…). No puede pretenderse una expectativa razonable de intimidad en un lugar de acceso común dentro del desarrollo de las funciones que a cada trabajador le encomiende la empresa dentro de la relación laboral. En ese caso, el poder de dirección del empresario, con sus facultades anejas, no incide sobre el derecho a la intimidad de los trabajadores al colocar cámaras de grabación en zonas comunes y de acceso generalizado en las que se desarrolla la actividad laboral general de la empresa. Otra cosa ocurre con las cámaras que se instalaran en el despacho del acusado (…) en principio, un despacho individual es una dependencia atribuida a una determinada persona, de la que depende el consentimiento para facilitar el acceso visual o personal de terceros al mismo. Por ello, en líneas generales, puede afirmarse que el titular del mismo tiene una expectativa razonable de intimidad dentro de su despacho, que puede verse vulnerada si se instalan cámaras de grabación sin su conocimiento".

La "expectativa razonable de intimidad" que el trabajador afectado por la grabación pudiera tener en relación con su actuación privada en el entorno laboral, se convirtió así en un criterio de ponderación de la

8. La teoría –o el test articulado por el propio TEDH– de la "expectativa razonable de privacidad" encuentra sus primeros reconocimientos en la STEDH de 5 de junio de 1997 (asunto *Halford v. the United Kingdom*) alcanzando una formulación más evolucionada en la STDH de 26 de julio de 2007 (asunto *Peev. V. Bulgaria* –con cita de jurisprudencia anterior–) que se mantiene en la actualidad.

proporcionalidad de la medida de control que en sí misma supone la grabación.

Pero, como se ha avanzado con anterioridad, junto a la expectativa razonable de intimidad, jurisprudencialmente se ha asentado ya un conjunto de requisitos que el empresario habrá de tomar en consideración para que la instalación de videocámaras no atente contra los derechos del trabajador. Ese será el objeto de las páginas que siguen, no sin antes hacer siquiera una breve referencia a cuáles son esos derechos fundamentales potencialmente afectos o susceptibles de afectación.

1. DERECHOS FUNDAMENTALES AFECTADOS

Conviene empezar destacando la vertiginosa evolución experimentada a este respecto en los últimos años; así, cuando se analiza la potencial lesividad del control empresarial, de la posible vulneración del derecho a la intimidad del trabajador se ha pasado a considerar violentado su derecho a la protección de datos e incluso su derecho a la construcción de un entorno virtual propio que le define e identifica como persona (el derecho –hasta hace poco, desconocido– "al propio entorno virtual"; especialmente susceptible de afectación no tanto por las grabaciones de video cuanto por el acceso a otros dispositivos tecnológicos –por ejemplo, de comunicación o seguimiento– puestos por el empresario a disposición del trabajador, como se reflejará en el epígrafe siguiente)[9].

La potencialidad invasiva de las nuevas tecnologías y del propio uso de las redes sociales con los flujos de información que por ellas transitan ha relegado el derecho a la intimidad, a la protección de unas parcelas de nuestra vida privada de las que escapan estas nuevas formas de intromisión. De otro modo expresado, la concepción tradicional del derecho a la intimidad se ha mostrado insuficiente para dar cobertura a nuevas formas de invasión en la privacidad de las personas que suponen un plus de gravedad y, por tanto, de lesión frente a las tradicionalmente conocidas. Así, junto al derecho a la intimidad, fue tomando forma el derecho a la protección de datos o el derecho a la autodeterminación informativa, considerado como un derecho distinto

9. De este tema me he ocupado con detalle en el estudio sobre "La afección de Derechos Fundamentales en un contexto tecnológico: del derecho a la intimidad al Derecho al propio entorno virtual", en "La prueba prohibida…", cit., epígrafe 2.

del anterior del que, aun compartiendo con él objetivo –garantizar la vida privada–, difiere en las posibilidades de control que concede al ciudadano sobre sus propios datos personales[10].

Más allá, pues, de la protección del derecho a la intimidad, los distintos ordenamientos reconocen hoy, también, un derecho de los ciudadanos a decidir qué uso pueden hacer –o no hacer– los terceros, de los datos personales obtenidos a través de mecanismos o plataformas tecnológicas. De este modo, el derecho a la protección de datos confiere a los ciudadanos un conjunto de facultades decisorias sobre el uso o el destino que cabe dar a los datos personales a que hubieran podido acceder terceros como consecuencia de la existencia y constancia de dichos datos en la red[11].

Pero este derecho, que cobrará especial relieve, como se verá a continuación, para determinar el valor que pueden alcanzar grabaciones concretas captadas por el empresario en el entorno laboral, se ve completado todavía con un derecho, en fase de consolidación en la actualidad, conocido como el derecho "al propio entorno virtual". Bajo este último, encuentra protección la lesión que una persona pudiera

10. En España, el derecho a la protección de datos o a la autodeterminación informativa encuentra anclaje constitucional en el art. 18.4 CE al establecer que "la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos". En relación con el proceso de construcción y consolidación de este derecho, especialmente interesantes resultan las SSTC 254/93 de 20 de julio; 11/98, de 13 de enero y 292/2000, de 30 de noviembre. Una vez consagrado el mismo, *vid*., entre otras, STC 29/2013, de 11 de febrero para su especial reconocimiento. Por su parte, en paralelo y en íntima conexión se ha construido también el concepto de "libertad informática" que ha sido definida, de forma ya consolidada, por el TC como el derecho a controlar el uso de los datos insertos en un programa informático (habeas data) y comprende, entre otros aspectos, la oposición del ciudadano al hecho de que determinados datos personales sean utilizados para otros fines diferentes de aquél legítimo que justificó la obtención (SSTC 11/1998, FJ 5.°, 94/1998, FJ 4.°).

11. En palabras del TC "Este derecho fundamental a la protección de datos, a diferencia del derecho a la intimidad del art. 18.1 CE, con el cual comparte el objetivo de ofrecer una protección constitucional eficaz de la vida privada personal y familiar, atribuye al titular una serie de facultades que consiste, en la mayor parte, en el poder jurídico de imponer a terceros la realización o la omisión de determinados comportamientos la regulación concreta de los cuales tiene que establecer la Ley, aquella que, de acuerdo con el art. 18.4 CE, tiene que limitar el uso de la informática, bien desarrollando el derecho fundamental a la protección de datos (art. 81.1 CE), bien regulando el ejercicio (art. 53.1 CE)". STC 292/2000, de 30 de noviembre. FJ 5.°.

padecer en su intimidad y privacidad como consecuencia de la intromisión de un tercero en sus dispositivos de navegación y comunicación por internet; dicha intromisión permite un rastreo de la actividad virtual de un sujeto que posibilita la reconstrucción de una imagen fiel de su perfil a partir de la unión de datos dispersos que si bien, por sí solos, pudieran no tener una relevancia fundamental a estos efectos, unidos e interrelacionados, permiten acceder a una fotografía exacta de la personalidad del afectado (*v.gr*. el historial de navegación, los contactos con los que ha tenido comunicación, el horario de conexión…). Es, precisamente, esa reconstrucción de la imagen personal realizada por un tercero a partir de la actividad desplegada por las redes y el uso que de la misma se pueda hacer, lo que trata hoy de encontrar protección en el seno de este nuevo derecho al propio entorno virtual[12].

Nótese, por último, que la evolución jurisprudencial acaecida en la búsqueda de una adecuada protección de los derechos e intereses en conflicto dentro del mundo de la tecnología digital, ha llevado a reconocer también la existencia de un derecho a la intimidad social o a la "vida privada social", que se proyecta más allá del círculo íntimo personal y que abarca también a las relaciones laborales. Se reconoce de esta manera, que el derecho a la privacidad comprende, también, una vertiente social que protege al individuo frente a injerencias que le impidan mantener una libre comunicación o relación con sus semejantes y que, en el ámbito laboral, podrían venir dadas por el ejercicio del control empresarial sobre la actividad del trabajador[13]. De ahí, pues, la

12. ARRABAL PLATERO lo define como "un derecho fundamental de creación jurisprudencial que está actualmente en fase de asentamiento, que encuentra su legitimación en el derecho a la privacidad que reconoce el artículo 8 CEDH y que engloba, por tanto, la protección de diversos derechos de diferente significado constitucional que pueden –y suelen– concurrir en un mismo dispositivo, como el derecho a la intimidad del artículo 18.1 CE –aplicable para la protección del listado de contactos o de fotografías, entre otros–, el derecho al secreto de las comunicaciones reconocido en el artículo 18.3 CE –garantía de las comunicaciones a través de sistemas de mensajería por ejemplo– o el derecho a la protección de datos que se ubica en el artículo 18.4 CE que ampara, entre otros, los datos de geolocalización". ARRABAL PLATERO, P., *La Prueba Tecnológica: aportación, práctica y valoración*, Tirant Lo Blanch, Valencia, 2020, pp. 167-168. En el mismo sentido puede consultarse también, de la propia autora, "El Derecho fundamental al propio entorno virtual y su incidencia en el proceso", en *Era digital, Sociedad y Derecho*, Tirant lo Blanch, Valencia, 2020.

13. Sostiene el TEDH en su sentencia conocida como Barbulescu II (STEDH 2017, 61 (Gran Sala) Caso Barbulescu contra Rumania, de 5 septiembre 2017. Apartados 70 y 71) que "(…) el Tribunal considera útil recordar que la noción de 'vida privada' es un concepto amplio que no se presta a una definición exhaustiva (*Sidabras*

necesidad de someter dicho control a determinados límites que garanticen estos distintos derechos susceptibles de ser afectados[14]; y, en este sentido, sostiene el TEDH que las restricciones establecidas en la vida laboral afectarán al derecho a la privacidad del art. 8 del CEDH cuando repercuten en la forma en que el individuo forja su identidad social a través del desarrollo de relaciones con otros[15].

Concretados así, los derechos fundamentales del trabajador susceptibles de quedar afectados por los distintos mecanismos de control que el empresario pudiera instalar en la empresa, cabría distinguir –al menos– dos escenarios posibles: La instalación de cámaras y

---

y Džiautas contra Lituania (TEDH 2004, 55), núms. 55480/00 y 59330/00, ap. 43, TEDH 2004-VIII). El artículo 8 del Convenio (RCL 1999, 1190, 1572) protege el enriquecimiento personal (*KA y AD contra Bélgica* (TEDH 2005, 15), núms. 42758/98 y 45558/99, ap. 83, 17 de febrero de 2005), ya sea en forma de desarrollo personal *Christine Goodwin contra Reino Unido (PROV 2002, 181176)* [GS], núm. 28957/95, ap. 90, TEDH 2002-VI) o de autonomía personal, que refleja un importante principio subyacente en la interpretación de las garantías del artículo 8 (*Pretty contra Reino Unido* (TEDH 2002, 23), núm. 2346/02, ap. 61, TEDH 2002-III). El Tribunal reconoce que toda persona tiene derecho a una vida privada, lejos de la injerencia no deseada de otros (*Smirnova contra Rusia* (PROV 2003, 162895), núms 46133/99 y 48183/99, ap. 95, TEDH 2003-IX (extractos)). También 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 (*Niemietz contra Alemania* (TEDH 1992, 77), 16 de diciembre de 1992, ap. 29, Serie A núm. 251-B). Así, el artículo 8 garantiza un derecho a la 'vida privada' en sentido amplio, que 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 (*Bigaeva contra Grecia* (TEDH 2009, 61), núm. 26713/05, ap. 22, 28 de mayo de 2009, y *Özpınar contra Turquía* (TEDH 2010, 103), núm. 20999/04, artículo 45 in fine, 19 de octubre de 2010).

El Tribunal considera que el concepto de 'vida privada' puede incluir actividades profesionales (*Fernández Martínez contra España* (TEDH 2014, 35) [*GS*], núm. 56030/07, ap. 110, TEDH 2014 (extractos), y *Oleksandr Volkov contra Ucrania* (TEDH 2013, 79) núm. 21722/11, apartados 165-166, TEDH 2013) o actividades que tengan lugar en un contexto público (*Von Hannover contra Alemania* (TEDH 2012, 10) (núm. 2) [GS], núms. 40660/08 y 60641/08, ap. 95, TEDH 2012)".

14. En este ámbito cobra un especial sentido el derecho a la desconexión digital introducido por la LO 3/2018, de protección de datos y garantía de los derechos digitales (art. 88). Sobre este derecho y su vertiente como defensa de la privacidad del trabajador puede verse FERNÁNDEZ ORRICO, J., "Desconexión digital en el ámbito laboral: un derecho emergente de los trabajadores", en *Era Digital Sociedad y Derecho*, FUENTES SORIANO, Dir.), Tirant lo Blanch, Valencia, 2020, pp. 581 y ss.
15. *Vid*. STEDH Barbulescu II, apartado 71.

consiguiente grabación de imágenes, por un lado, que afectará, esencialmente, al derecho a la protección de datos del trabajador; y, por otro, el control de sus comunicaciones y/o el control del uso que el trabajador hace de internet y las redes sociales que, en su caso, atentaría contra su derecho al propio entorno virtual (más allá, pues, del estricto derecho al secreto de las comunicaciones)[16].

En relación con el primer escenario apuntado y, por tanto, con la instalación de cámaras de grabación en la empresa –quedará para un momento posterior, el control de los dispositivos informáticos puestos a disposición del trabajador– ha resultado trascendental la STEDH (Gran Sala) de 17 de octubre de 2019 en el asunto López Ribalda contra España y el cambio de orientación de la misma respecto del previo pronunciamiento del propio Tribunal (Sección Tercera) sobre ese mismo asunto. Al estudio de esta nueva doctrina dedicaremos las páginas que siguen.

2. EXIGENCIAS PROBATORIAS DE LA GRABACIÓN DE LA ACTIVIDAD LABORAL: STEDH LÓPEZ RIBALDA II

Los hechos que se enjuician en el asunto López Ribalda y otros contra España son, de forma muy resumida, los siguientes:

Ante la existencia de un desfase contable en la cuenta de pérdidas y ganancias de un supermercado y la consiguiente sospecha de unos hurtos acaecidos en el mismo, el empresario instala diversas cámaras, unas visibles y otras ocultas, para el control de la actividad laboral de los trabajadores, informando a estos, tan solo, de la existencia de las cámaras visibles. Constatados los hurtos por las grabaciones y reproducidas éstas ante las empleadas afectadas, se procede a su despido que, tras ser por ellas recurrido, es considerado ajustado a Derecho tanto ante el juzgado de lo social, cuanto ante el TSJ. En ambas sentencias se aceptaron como prueba las grabaciones, al entender que habían sido legítimamente obtenidas. Ante el TEDH las recurrentes alegaron vulneración del derecho a la intimidad, por un lado, y vulneración del derecho a un proceso justo por la valoración probatoria

16. Una visión exhaustiva de los posibles dispositivos de control de la actividad laboral, los derechos afectados y los protocolos, mecanismos o exigencias para una válida instalación o aplicación de los mismos puede verse en FERNÁNDEZ ORRICO, J., *Criterios sobre uso de dispositivos tecnológicos en el ámbito laboral. Hacia el equilibrio entre el control empresarial y la privacidad del trabajador*, Tirant lo Blanch, Valencia, 2021.

de las grabaciones que consideraron obtenidas ilícitamente, por otro. En el primer pronunciamiento de dicho Tribunal sobre esta causa (STEDH, Sección Tercera, de 9 de enero de 2018; *López Ribalda and others Vs. Spain*), se entendió que las grabaciones realizadas con las cámaras ocultas afectaban a la vida privada de las recurrentes en tanto en cuanto lesionaban el derecho a la protección de sus datos personales, que cabe entender incluido en el anterior. Así, y en la medida en que la imagen personal es un conjunto de datos visuales digitalmente tratado, la obtención de la misma, mediante la instalación de cámaras ocultas en el lugar de trabajo sin una información previa a los sujetos potencialmente afectados, lesiona, directamente, este derecho fundamental. La clave de la lesión se centra, para esta sentencia del TEDH, en la opacidad de la medida (la instalación de cámaras ocultas) y la consiguiente ausencia de una información clara y precisa sobre qué cámaras se habían instalado y qué finalidad se perseguía con las grabaciones. El hecho, por otra parte, de no contar con esta información impidió a los trabajadores afectados –según la Sala Tercera del TEDH– ejercitar los derechos que la normativa de protección de datos les reconocía provocando así una importante limitación de las garantías legalmente previstas.

Sin embargo, cuando, como consecuencia de la evolución procesal del asunto, el propio TEDH tiene ocasión de analizar de nuevo el caso –esta vez ante la Gran Sala; en la sentencia que se conoce como López Ribalda II[17]–, concluye que no hubo vulneración alguna, ni del derecho a la vida privada que regula el art. 8.1 CEDH, ni del derecho a un proceso justo, regulado en el art. 6.1 de ese mismo cuerpo legal.

La discrepancia entre las dos sentencias de este tribunal (López Ribalda I –Sala Tercera TEDH– y López Ribalda II –Gran Sala–) se centró, fundamentalmente, en lo que al establecimiento de las cámaras ocultas se refiere y a la posible invasión de éstas en la privacidad de los afectados por la grabación: mientras que la Sala Tercera del TEDH en López Ribalda I, interpretó que las demandantes tenían derecho a ser informadas previamente, de modo expreso, claro e inequívoco sobre la instalación de cámaras de videovigilancia, la finalidad de las grabaciones y a quién se dirigen estas[18]; la Gran Sala de ese mismo Tribunal, en López Ribalda II, consideró –en un vuelco doctrinal de

17. STEDH, Gran Sala, de 17 de octubre de 2019.

18. Literalmente, reconoce el derecho de las demandantes a ser informadas previamente y de forma precisa e inequívoca sobre "la existencia de un fichero o tratamiento de datos de carácter personal, sobre la finalidad de la recogida de estos y

profundo calado– que las sospechas por el empresario de que se estaban cometiendo graves irregularidades justificaba la instalación de cámaras ocultas.

Las consecuencias derivadas de una y otra posición jurisprudencial resultan diametralmente opuestas: mientras que según la tesis sostenida en López Ribalda I las grabaciones se consideran ilegítimas –por no haberse informado de la instalación de las cámaras– y, por tanto, cabe amparar las pretensiones de las recurrentes en este sentido; en López Ribalda II se justifica esa ausencia de información y se convalida la instalación de cámaras por el empresario teniendo por válidas las grabaciones obtenidas y desestimando, por tanto, las pretensiones de las recurrentes[19].

Al margen de las críticas que este viraje jurisprudencial pueda merecer y que se expondrán más adelante, un factor especialmente relevante de esta STEDH –López Ribalda II– es el acogimiento a una suerte test de proporcionalidad (conocido como "test Barbulescu")[20] que, valorando

---

de los destinatarios de la información" (STEDH, Sección Tercera, López Ribalda y otros contra España).

19. El alcance que puede tener una prueba obtenida con vulneración de derechos fundamentales en la calificación de la nulidad de un despido ex art. 55.5 ET es un problema de carácter ciertamente colateral con el que pretende ser objeto de estudio del presente trabajo. Ello no obstante la importancia del mismo y, en su interpretación, de la STC (sala primera) 61/2021, de 15 de marzo, merece, al menos, esta llamada de atención. Como con acierto se sostiene en la misma (FD 5.°) "no puede confundirse el despido con violación de derechos fundamentales, con el despido en el que ha habido una lesión de los derechos fundamentales en el proceso de obtención de la prueba". Y, al estudio de la Jurisprudencia existente sobre la materia dedica parte del fundamento jurídico de referencia.

20. Este "test" es la extrapolación de la doctrina del propio TEDH sentada en el asunto Barbulescu II contra Rumanía, como se verá más adelante en este mismo trabajo. Así lo manifiesta la propia STEDH cuando reconoce que "115. En la sentencia Bărbulescu, el TEDH estableció un cierto número de requisitos que debe cumplir cualquier supervisión de la correspondencia y las comunicaciones de los empleados para no violar el Artículo 8 del Convenio (véase Bărbulescu, citado anteriormente, § 121). También concluyó en esa sentencia que, para garantizar el cumplimiento efectivo de esos requisitos, los empleados en cuestión deben tener acceso a un recurso ante un órgano judicial independiente con jurisdicción para determinar, al menos en esencia, si se cumplieron las condiciones pertinentes (*ibid*., § 122).

    116. El Tribunal considera que los principios establecidos en la sentencia Bărbulescu, algunos de los cuales provienen de la decisión de Köpke, que se referían a hechos similares a los del presente caso, son extrapolables, *mutatis mutandis*, a las circunstancias en el que un empleador puede implementar medidas de vídeo vigilancia en el lugar de trabajo. Estos criterios deben aplicarse teniendo en

la conducta de los empresarios respecto del cumplimiento de determinados ítems, permitiría concluir si, efectivamente, la instalación de cámaras y la consiguiente grabación de la actividad laboral puede considerarse vulneradora o no, de la intimidad del trabajador.

Es de destacar, en este sentido, que –como no podría ser de otro modo– el TEDH parte del respeto a la autonomía de los Estados respecto de la legislación propia en materia de videovigilancia laboral; pero, a partir de ahí, establece cuáles deben ser los factores a considerar por los Tribunales para valorar la proporcionalidad de la medida (la instalación de cámaras y el uso probatorio de las grabaciones) y ponderar, por tanto, su legitimidad. Tales parámetros serán, como se verá a continuación: 1) la información al trabajador sobre la instalación de las cámaras; 2) la información sobre el ámbito y alcance de la grabación: tanto objetivo (espacio/tiempo) cuanto subjetivo (personas potencialmente afectadas y nivel de privacidad que el trabajador puede esperar en ese ámbito concreto); 3) la información sobre las razones que justifican la instalación de cámaras y las grabaciones; 4) el carácter intrusivo de la medida; 5) las consecuencias de las grabaciones para el trabajador: el uso que se les da y si se ajusta al objetivo declarado; y 6) las garantías concedidas al trabajador respecto de las medidas.

Así, sostiene el TEDH que "para garantizar la proporcionalidad de las medidas de videovigilancia en el lugar de trabajo, los tribunales nacionales deben tener en cuenta los siguientes factores cuando sopesan los diversos intereses en competencia:

(i) Si el trabajador ha sido informado de la posibilidad de que el empleador adopte medidas de videovigilancia y de implementación de tales medidas. Si bien en la práctica los trabajadores pueden ser informados de varias maneras, dependiendo de las circunstancias fácticas particulares de cada caso, la notificación normalmente debe ser clara sobre la naturaleza de la videovigilancia y debe darse anterior a su aplicación.

(ii) El alcance de la videovigilancia por parte del empleador y el grado de intrusión en la privacidad del empleado. En este sentido, se debe tener en cuenta el nivel de privacidad en el área que se está vigilando, junto con las limitaciones de tiempo y espacio y la cantidad de personas que tienen acceso a los resultados.

---

cuenta la especificidad de las relaciones laborales y el desarrollo de nuevas tecnologías, que pueden permitir tomar medidas cada vez más intrusivas en la vida privada de los empleados". STEDH (Gran Sala) López Ribalda contra España.

(iii) Si el empleador ha proporcionado razones legítimas para justificar la videovigilancia y el alcance de la misma. Cuanto más intrusiva sea la videovigilancia, mayor será la justificación que se requerirá.

(iv) Si hubiera sido posible establecer un sistema de videovigilancia basado en métodos y medidas menos intrusivos. A este respecto, debe haber una evaluación a la luz de las circunstancias particulares de cada caso en cuanto a si el objetivo perseguido por el empleador podría haberse logrado a través de un menor grado de interferencia con la privacidad del empleado.

(v) Las consecuencias de la videovigilancia para el trabajador sujeto a él. Debe tenerse en cuenta, en particular, el uso que hace el empleador de los resultados de la supervisión y si dichos resultados se han utilizado para lograr el objetivo declarado de la medida.

(vi) Si el trabajador ha recibido las garantías apropiadas, especialmente cuando las operaciones de videovigilancia del empleador son de naturaleza intrusiva. Dichas garantías pueden tomar la forma, entre otras, de proporcionar información a los empleados interesados o a los representantes del personal en cuanto a la instalación y el alcance de la videovigilancia, o una declaración de tal medida a un organismo independiente o la posibilidad de presentar una queja".

Sentado así este "test" con carácter general, su aplicación al caso concreto ofrece algunas conclusiones de sumo interés por cuanto están llamadas a convertirse en fuente interpretativa de futuras sentencias de los Tribunales; españoles –desde luego–, pero también europeos. Así, la Gran Sala del TEDH, en el caso *López Ribalda Vs España*, constató que: 1) los Tribunales Españoles, en sus resoluciones sobre el caso, identificaron adecuadamente los intereses en conflicto: el derecho a la vida privada de las trabajadoras recurrentes y el derecho del empleador a ejercer las potestades de control empresarial en garantía del buen fin de la empresa[21]; 2) identificaron igualmente como razones justificativas de la instalación de las videocámaras, las significativas

21. STEDH Gran Sala, López Ribalda y otros Vs España: "122. El Tribunal comenzaría señalando que los tribunales laborales identificaron los diversos intereses en juego, refiriéndose expresamente al derecho de los demandantes a respetar su vida privada y al equilibrio entre ese derecho y el interés del empleador en garantizar el buen funcionamiento de la empresa ejerciendo sus poderes de gestión. Por lo tanto, determinará cómo esos tribunales tuvieron en cuenta los factores enumerados anteriormente cuando sopesaron estos intereses".

pérdidas registradas en la marcha del negocio[22]; 3) examinaron en la forma debida el alcance de la medida intrusiva –de las grabaciones– (en su dimensión espacio-temporal: atendiendo tanto al ámbito espacial de grabación, con referencia a las personas potencialmente afectadas, cuanto al tiempo durante el que se prolongó la medida), así como el grado de intrusión en la intimidad de las demandantes[23];

22. STEDH Gran Sala, López Ribalda y otros Vs España: "123. Los tribunales nacionales primero determinaron, de conformidad con los requisitos de la jurisprudencia del Tribunal Constitucional, que la instalación de la vídeo vigilancia había sido justificada por razones legítimas, a saber, la sospecha presentada por el gerente del supermercado derivada de pérdidas significativas registradas durante varios meses, que se habían cometido robos. También tuvieron en cuenta el interés legítimo del empleador en tomar medidas para descubrir y sancionar a los responsables de las pérdidas, con el objetivo de garantizar la protección de su propiedad y el buen funcionamiento de la empresa".

23. STEDH Gran Sala, López Ribalda y otros Vs España: "124. Después, los tribunales nacionales examinaron el alcance de la supervisión y el grado de intrusión en la privacidad de los demandantes, concluyendo que la medida era limitada en cuanto a las áreas y al personal que se estaba vídeo vigilando, ya que las cámaras solo cubrían el área de pago, lo que probablemente estar donde ocurrieron las pérdidas, y que su duración no había excedido lo necesario para confirmar las sospechas de robo. En opinión del Tribunal, esta evaluación no puede considerarse irrazonable. Señala que la vídeo vigilancia no cubrió todo el centro de trabajo, sino que se centró en las áreas alrededor de las cajas, donde probablemente se cometieron robos. Las tres demandantes que trabajaban como cajeras fueron vídeo vigiladas por cámaras de CCTV durante su jornada laboral. Como resultado de sus trabajos dentro de la empresa, no pudieron evadir estas grabaciones, que estaban dirigidas a todo el personal que trabajaba en el área de pago, y se operaban permanentemente y sin ninguna limitación (contraste Köpke, citado anteriormente, sobre un solicitante que fue tanto una dependienta como una cajera de la tienda en cuestión, la medida de vídeo vigilancia no cubre la totalidad de su lugar de trabajo). Hasta cierto punto, se encontraron en áreas limitadas (ver, mutatis mutandis, Allan v. The United Kingdom, no. 48539/99, § 35, ECHR 2002 IX, y Perry, citado anteriormente, §§ 39-43). En cuanto a los demandantes cuarto y quinto, las cámaras de CCTV los filmaron cada vez que pasaban por el área de pago.

125. Al mismo tiempo, debe señalarse que las tareas de las demandantes se realizaban en un lugar abierto al público y que implicaba un contacto permanente con los clientes. A este respecto, el Tribunal considera que es necesario distinguir, en el análisis de la proporcionalidad de una medida de vídeo vigilancia, los diversos lugares en los que se llevó a cabo la supervisión, a la luz de la protección de la privacidad que un empleado razonablemente podría esperar. Esa expectativa es muy alta en lugares privados por naturaleza, como inodoros o guardarropas, donde se justifica una mayor protección, o incluso una prohibición total de la vídeo vigilancia (ver, en este sentido, los instrumentos internacionales relevantes citados en los párrafos 61 y 65 arriba). Sigue siendo alta en áreas de trabajo cerradas como oficinas. Es manifiestamente menor en lugares visibles o accesibles para colegas o, como en el presente caso, para el público en general.

4) entendieron –y lo comparte el TEDH– que la medida era "necesaria" conforme a la interpretación que de este requisito realiza el propio TC Español, habida cuenta la elevada cuantía de las pérdidas sufridas[24]; 5) aun admitiendo las importantes consecuencias derivadas de las grabaciones (el despido de las empleadas), para el TEDH adquiere una especial relevancia en la ponderación de intereses, el hecho de que las grabaciones no fueran utilizadas por el empresario para ningún propósito distinto del de descubrir a los responsables del desfase contable padecido por la empresa y aplicar frente a ellos las medidas disciplinarias legalmente previstas[25]; y 6) en lo que respecta a la necesidad de

126. En cuanto al alcance de la medida a lo largo del tiempo, el Tribunal observa que, si bien, como argumentaron los demandantes, el empleador no había establecido de antemano la duración de la vídeo vigilancia, en realidad duró diez días y cesó tan pronto los empleados responsables habían sido identificados. Por lo tanto, la duración de la monitorización no parece excesiva en sí misma (compárese *Köpke*, citado anteriormente, donde no se encontró que una duración de catorce días fuera desproporcionada). Por último, solo el gerente del supermercado, el representante legal de la empresa y el representante sindical vieron las grabaciones obtenidas a través de la videovigilancia impugnada antes de que las propias trabajadoras hubieran sido informados. Teniendo en cuenta estos factores, el Tribunal considera que la intrusión en la privacidad de las demandantes no alcanzó un alto grado de seriedad".

24. STEDH Gran Sala, López Ribalda y otros Vs España: "128. Además, los tribunales nacionales consideraron que, en las circunstancias del caso, no había otro medio para cumplir el objetivo legítimo perseguido y que, por lo tanto, la medida debería considerarse 'necesaria' en el sentido de la doctrina del Tribunal Constitucional. ley (véase el párrafo 33 supra). Incluso si hubiera sido deseable que los tribunales nacionales hubieran examinado de manera más intensa la posibilidad de que el empleador hubiera utilizado otras medidas que implican una menor intrusión en la vida privada de los trabajadores, el Tribunal no puede dejar de notar que el alcance de las pérdidas identificadas por el empleador indicaban que varios trabajadores habían cometido robos y que el suministro de información a cualquier miembro del personal podría haber frustrado el propósito de la vídeo vigilancia, que era, como señalaron esos tribunales, descubrir a los responsables. por los robos, pero también para obtener evidencia para su uso en procedimientos disciplinarios en su contra".

25. STEDH Gran Sala, López Ribalda y otros Vs España: "127. En cuanto a las consecuencias del control impugnado para las demandantes, el Tribunal considera que fueron importantes porque los empleados afectados fueron despedidos sobre la base de las grabaciones obtenidas por ese medio. Sin embargo, observa, como también señalaron los tribunales nacionales, que la vigilancia por vídeo y las grabaciones no fueron utilizadas por el empleador para ningún otro propósito que no fuera descubrir a los responsables de las pérdidas registradas de bienes y tomar medidas disciplinarias contra ellos (compárese con *Peck*, citado anteriormente, §§ 62-63, donde las imágenes grabadas por una cámara CCTV de lugares públicos que mostraban el intento de suicidio del solicitante habían sido distribuidas a los medios de comunicación)".

información previa sobre las medidas de videovigilancia y tras reiterar el TEDH la necesidad de que, con carácter general, dicha información previa, efectivamente, se dé[26], concluye que en el presente caso, obró bien la jurisdicción laboral española al entender que las importantes pérdidas sufridas, así como la imposibilidad de determinar la persona causante de las mismas justificaba la instalación de determinadas cámaras sin información de ello a los trabajadores afectados. A dicho argumento, sumó el TEDH la consideración de que esta exigencia de información constituye un parámetro más de ponderación a tener en cuenta, pero ni se trata del único, ni de una exigencia en sí misma determinante; y, por tanto, concurriendo el resto de factores que avalan la necesidad y proporcionalidad de la medida, las circunstancias del caso presente permiten obviar la exigencia de información previa respecto de la instalación de las cámaras, sobre la base de la existencia de "sospechas razonables" de haberse cometido una infracción grave[27]. Literalmente, sostiene la

26. STEDH Gran Sala, López Ribalda y otros Vs España: "131. El Tribunal observa que, si bien tanto la legislación española como las normas internacionales y europeas pertinentes no parecen requerir el consentimiento previo de las personas que se someten a vídeo vigilancia o, en general, que tienen sus datos personales recopilados, esas normas establecen que, en principio, es necesario informar a las personas interesadas, de forma clara y previa a la implementación, de la existencia y las condiciones de dicha recopilación de datos, aunque solo sea de manera general (véanse los párrafos 47, 60 y 63 anteriores). El TEDH considera que el requisito de transparencia y el consiguiente derecho a la información son de naturaleza fundamental, particularmente en el contexto de las relaciones laborales, donde el empleador tiene poderes significativos con respecto a los empleados y se debe evitar cualquier abuso de esos poderes (ver párrafos 61-62 y 64-65 arriba). Sin embargo, hay que subrayar que la facilitación de información al individuo que se está vídeo vigilando y su alcance, constituyen solo uno de los criterios a tener en cuenta para evaluar la proporcionalidad de una medida de este tipo en un caso dado. No obstante, si falta dicha información, las garantías derivadas de los otros criterios serán aún más importantes".

27. STEDH Gran Sala, López Ribalda y otros Vs. España. Como fundamentación de este argumento puede leerse en la Sentencia que "133. Es cierto que los tribunales laborales no tuvieron en cuenta que el empleador, como alegan las demandantes, no les proporcionó la información previa requerida por la sección 5 de la Ley de Protección de Datos Personales, ya que consideraron que el asunto era irrelevante e incapaz de afectar a la proporcionalidad, en el sentido constitucional, de la medida, siempre que se cumpliesen los demás criterios establecidos por el Tribunal Constitucional. Dada la importancia del derecho a la información en tales casos, el Tribunal considera que solo un requisito primordial relacionado con la protección de intereses públicos o privados importantes podría justificar la falta de información previa.

134. Sin embargo, en las circunstancias específicas del presente caso, teniendo en cuenta particularmente el grado de intrusión en la privacidad de los

Sentencia que "aunque no puede [el TEDH] aceptar la proposición de que, en términos generales, la más mínima sospecha de apropiación indebida o cualquier otro delito por parte de los empleados podría justificar la instalación de videovigilancia encubierta por parte del empleador, la existencia de sospechas razonables de que se ha cometido una mala conducta grave y el alcance de las pérdidas identificadas en el presente caso puede parecer una justificación importante. Esto es aún más cierto en una situación en la que el buen funcionamiento de una empresa está en peligro no solo por la sospecha de mal comportamiento de un solo empleado, sino más bien por la sospecha de una acción concertada por parte de varios empleados, ya que esto crea una atmósfera general de desconfianza en el lugar de trabajo"[28].

Admite, pues, el TEDH, una válvula de escape –no pequeña, por cierto– a la necesaria información previa que el empresario debe dar al trabajador respecto de la instalación de medidas de control de la actividad laboral en el seno de la empresa. Tal y como se avanzó con anterioridad, este punto constituye el eje de fricción entre la posición que inicialmente mantuvo la Sala Tercera del Tribunal cuando examinó el caso (donde constituía esta información previa, una exigencia insalvable) y la posición final sostenida por la Gran Sala, en la sentencia que se analiza. Esta decisión, no exenta de polémica, como se verá, mereció la emisión de un voto particular –firmado por tres jueces[29]– en el que se apunta, como solución, que la única forma posible de salvar esa obligación de informar al trabajador debiera pasar por

---

demandantes (véanse los párrafos 125 a 26 *supra*) y las razones legítimas que justifican la instalación de la vídeo vigilancia, el Tribunal considera que los tribunales sociales pudieron, sin sobrepasar el margen de apreciación otorgado a las autoridades nacionales, considerar que la interferencia con la privacidad de las demandantes fue proporcional (véase, para una situación similar, *Köpke*, citado anteriormente). Por lo tanto, aunque no puede aceptar la proposición de que, en términos generales, la más mínima sospecha de apropiación indebida o cualquier otro delito por parte de los empleados podría justificar la instalación de videovigilancia encubierta por parte del empleador, la existencia de sospechas razonables de que se ha cometido una mala conducta grave y el alcance de las pérdidas identificadas en el presente caso puede parecer una justificación importante. Esto es aún más cierto en una situación en la que el buen funcionamiento de una empresa está en peligro no solo por la sospecha de mal comportamiento de un solo empleado, sino más bien por la sospecha de una acción concertada por parte de varios empleados, ya que esto crea una atmósfera general de desconfianza en el lugar de trabajo".

28. STEDH, Gran Sala, López Ribalda y otros Vs España; parágrafo 134.
29. Los jueces De Gaetano, Yudkivska y Grozev.

establecer la necesidad de recabar la autorización de un tercero tras la comprobación por parte de éste de la existencia de esos "indicios de un incumplimiento grave"[30]. Cuando el incumplimiento grave conlleve la sospecha de una actuación delictiva, entiendo que este tercero legitimado para autorizar la instalación de unas cámaras de vigilancia que pueden afectar a los derechos fundamentales del trabajador no puede ser otro que el órgano judicial, en el seno de una investigación criminal; y, en tal sentido, lo que cabría exigir es que, tras la denuncia, fuera la policía, previa autorización judicial, quien procediera a la instalación de esas videocámaras ocultas[31].

Dicho de otro modo, la medida propuesta por los magistrados disidentes –en mi opinión– debe ser entendida como la exigencia de

30. Literalmente, se sostiene en el voto particular (apartado 10) que "La mayoría señala que 'no puede aceptar la propuesta de que … la más mínima sospecha de apropiación indebida o cualquier otra conducta indebida por parte de los empleados pueda justificar la instalación de una videovigilancia encubierta por parte del empleador', pero no obstante considera que 'la existencia de una sospecha razonable de que se ha cometido una falta grave … puede parecer una justificación de peso' para tal medida (párrafo 134). En nuestra opinión, a falta de un requisito de medidas procesales claras, la existencia de 'una sospecha razonable de que se ha cometido una falta grave' no es suficiente, ya que puede dar lugar a investigaciones privadas y podría utilizarse como justificación en un número inaceptablemente elevado de casos. Si bien, en principio, el requisito de la 'sospecha razonable' es una salvaguardia importante, no es suficiente para proteger los derechos de privacidad cuando se enfrenta a una vigilancia electrónica de carácter encubierto. En circunstancias como las del presente caso, en que un empleador utiliza la vigilancia encubierta por vídeo sin advertir previamente a sus empleados, es necesario establecer medidas procesales adicionales; similares a las que se exigen en virtud del Convenio en el uso de la vigilancia secreta en los procedimientos penales. Los requisitos procesales que permitan una verificación fiable, por un tercero, de la existencia de una 'sospecha razonable de falta grave', y las garantías contra la justificación de que la vigilancia se realice 'a posteriori', deberían ser un requisito en virtud del artículo 8 del Convenio. Sólo con la aplicación de estas garantías procesales podríamos aceptar fácilmente el juicio de la mayoría".

31. Antes incluso de la publicación de la Sentencia López Ribalda II se asumía, razonablemente, la necesaria autorización judicial como la única solución posible, sin que se aprecien cambios que justifiquen esta involución interpretativa "(…)si de lo que estamos hablando no es estrictamente de videovigilancia preventiva sino de la preexistencia de indicios delictivos que señalen a uno o varios trabajadores (un presunto delito de robo continuado a la empresa, por ejemplo), la previa información no sería obligada, como es lógico, pero será el juez quien deba decidir el lugar de instalación y características de estos dispositivos, de acuerdo con el principio de proporcionalidad". MAGRO SERVET, V., "Sobre el valor probatorio de las cámaras de vigilancia en el proceso penal", Diario La Ley, Núm. 9114, Sección Doctrina, 9 de enero de 2018.

jurisdiccionalidad requerida para la limitación de derechos fundamentales; de forma tal que supliera ésta la falta de información al trabajador respecto de la adopción de la medida intrusiva. Según el voto particular que nos ocupa, esta solicitud de autorización –que, entiendo, debe ser judicial– evitaría, por un lado, la existencia de investigaciones arbitrarias y, por otro, los inconvenientes derivados del hecho de que, en caso contrario, la medida tenga que ser justificada por el empresario *a posteriori*; o, de otro modo expresado, cuando es posible que ya se haya llevado a cabo el acto lesivo del derecho fundamental.

Ciertamente y como bien detectan los jueces disidentes, la postura mayoritariamente sostenida en la Sentencia legitimará la adopción de medidas lesivas para los trabajadores cuya justificación dependerá exclusivamente de la interpretación subjetiva del empleador respecto de la concurrencia de indicios o sospechas de incumplimiento grave. La necesidad de autorización judicial, como proponen, paliaría –al menos– el riesgo descrito; aunque, en mi opinión y como trataré de explicar, no solucionaría el problema. Así, aun aceptando como mal menor dicha propuesta, es evidente que no se evitaría con ella la necesidad de probar –si bien con carácter previo a la instalación de las cámaras– las "sospechas razonables de que se ha cometido una infracción grave".

Pero el problema, como avanzaba, es que no se aborda, en realidad, el fondo de la cuestión. La justificación de la posible instalación de mecanismos de control de la actividad laboral encuentra apoyatura en las potestades de dirección que el ordenamiento reconoce al empresario a fin de garantizar la buena marcha de la empresa; pero la clave, en un Estado de Derecho, residirá en determinar dónde debe ponerse el límite a esas potestades de dirección y control. En principio, y partiendo de la base de que la investigación y persecución de la presunta comisión de hechos delictivos se encuentra encomendada a las autoridades judiciales y policiales, lo que habrá que dilucidar es si lo que se quiere es permitir al empresario velar y asegurar el buen funcionamiento de su empresa u otorgarle potestades de investigación criminal que van más allá de su cometido. Porque si, como parece razonable, la aspiración es la primera –otorgarles potestades de dirección que garanticen la buena marcha de la empresa–, qué duda cabe que una puntual información a los trabajadores de las medidas de control adoptadas frente a la presunta comisión de determinados hechos que ponen en peligro el correcto funcionamiento del negocio, terminará, presumiblemente, con dicha actuación desviada. Si además, ante la presunta

comisión de un hecho delictivo, el empresario interpone –como es su obligación– la correspondiente denuncia ante las autoridades competentes iniciándose así la pertinente investigación, e informa de ello a los trabajadores, razón de más para entender que cesarán en esa presunta actividad desviada. Y si pese a ello, persisten en la misma, deberán ser las autoridades competentes (policiales y judiciales) las que en el seno de esa investigación oficial –como no podría ser de otro modo–, determinen, en su caso, la comisión de los hechos delictivos. Investigación en la que podrán –y deberán– valerse de todos los medios lícitos, adoptados siempre por las vías constitucionalmente previstas cuando entra en juego la posible afectación de derechos fundamentales.

La aspiración, pues, de la previsión normativa de la potestad de control del empresario[32] no es –no debe ser– permitir que éste adopte funciones pseudopoliciales en el seno de su empresa, sino garantizar, que dentro del conjunto de las instituciones y con pleno respeto a las competencias de cada una, el empresario podrá tomar iniciativas de control sobre la actividad laboral de sus trabajadores a fin de asegurar la buena marcha del negocio. Esas iniciativas de control deberían, aun con cierto margen de flexibilidad derivado de las peculiares características de las relaciones laborales, someterse al marco general de la legítima actuación entre particulares. Y el empresario, ni está habilitado para desempeñar funciones de investigación policial, ni tendría por qué estarlo. Razonable sería, pues, volver a la interpretación inicial del TEDH (caso López Ribalda Vs. España; Sala Tercera –sentencia conocida como *López Ribalda I*–) y entender necesaria e ineludible la exigencia de información previa y detallada sobre las medidas de control que el empresario vaya a adoptar frente a los trabajadores de la empresa.

Por otra parte, solo una solución como la propuesta daría cobertura a hechos –difíciles de entender por la sociedad y fundamento de Sentencias enormemente controvertidas– tales como la grabación y por tanto, detección casual de una actuación determinada para la que la cámara no había sido instalada. Frente a la posible alegación por el afectado de que la grabación lesiona su derecho a la intimidad es fácil en tal caso justificar el hallazgo casual del incumplimiento ilícito o,

32. El art. 20.3 del Estatuto de los Trabajadores en España, establece que "el empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad y teniendo en cuenta, en su caso, la capacidad real de los trabajadores con discapacidad".

incluso, del hecho delictivo en su caso y, en consonancia, el pleno valor probatorio de la grabación[33].

Por otra parte, conviene insistir en que, hasta el momento, se había venido abriendo paso una fundamentada línea jurisprudencial que consideraba admisibles determinadas pruebas aportadas por particulares cuando, aun afectando a derechos fundamentales, su obtención no hubiera sido buscada con fines procesales; es decir, cuando no se hubieran obtenido con la finalidad de preconstituir prueba en un ulterior proceso[34]. La doctrina del TEDH en el caso que nos ocupa apunta directamente contra la línea de flotación de esta tendencia jurisprudencial; de forma tal que, a partir de este momento, se entenderá justificado que un particular –el empresario; que no deja de ser un particular– se entrometa y lesione la intimidad de un tercero –el trabajador–, si lo hace con la intención de probar la comisión de un hecho delictivo respecto del que tiene sospechas fundadas. Porque, nótese, que con la doctrina de la Sentencia López Ribalda II encuentra amparo la investigación de aquellos hechos que, constituyendo un incumplimiento contractual grave presentan, también, apariencia delictiva. El cambio de concepción está, pues, servido: de empresario a Sheriff; la pregunta es… ¿Y la policía? ¿Dónde queda la labor de investigación criminal?

33. Esta es hoy la solución adoptada por la legislación española de protección de datos, cuando establece que: "Los empleadores podrán tratar las imágenes obtenidas a través de sistemas de cámaras o videocámaras para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respectivamente, en el artículo 20.3 del Estatuto de los Trabajadores y en la legislación de función pública, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo. Los empleadores habrán de informar con carácter previo, y de forma expresa, clara y concisa, a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de esta medida.

    En el supuesto de que se haya captado la comisión flagrante de un acto ilícito por los trabajadores o los empleados públicos se entenderá cumplido el deber de informar cuando existiese al menos el dispositivo al que se refiere el artículo 22.4 de esta ley orgánica".

    Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, art. 89.1 (Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo).

34. Se profundizará sobre ello en el último epígrafe de este mismo trabajo. Nótese, no obstante, que ejemplo paradigmático de ello cabe encontrar en la admisión probatoria de la conocida como "lista Falciani", anteriormente referida. Admisión probatoria constatada tanto por el TS (STS 116/2017, de 23 de Febrero), cuanto por el TC (STC 97/2019, de 16 de julio).

Llegados a este punto, no me queda sino manifestar la total conformidad con el análisis manifestado por los jueces disidentes en el voto particular de la sentencia que nos ocupa: "el empleador tenía dos objetivos legítimos: en primer lugar, quería impedir nuevos robos, para lo cual habría bastado con una advertencia sobre el sistema de videovigilancia instalado. En segundo lugar, quería averiguar quién era el responsable de las pérdidas que había sufrido en los últimos meses; en este caso, la notificación previa de la videovigilancia visible y encubierta no habría sido útil. No obstante, como el robo cometido era un delito, el empleador podría y debería haber acudido a la policía antes de adoptar esas medidas por iniciativa propia. La necesidad de dilucidar un delito no justifica la investigación privada, ni siquiera en forma de videovigilancia encubierta, que constituye una medida excesivamente intrusiva y un abuso de poder. Al no condenar ese comportamiento cometido por particulares, el Tribunal alienta a los particulares tomarse la justicia por su mano. En cambio, corresponde a las autoridades competentes adoptar las medidas adecuadas, ya que están mejor equipadas, tanto en lo que respecta a sus facultades para aplicar determinadas medidas como a su responsabilidad y obligaciones de seguir las orientaciones sobre lo que es necesario en una situación como la actual"[35].

Por las razones apuntadas, pues, de "franco retroceso" cabría calificar el giro interpretativo dado por la Gran Sala del TEDH en el caso López Ribalda II al admitir como excepción a la necesidad de información previa a los trabajadores, respecto de las medidas de control adoptadas por el empresario, la concurrencia de "sospechas razonables" de haberse cometido "una infracción grave".

Con posterioridad a la Sentencia López Ribalda II (y por tanto, sin posibilidad de tener reflejo en ella) entró en vigor en España la LOPD[36], en cuyo art. 89.1 apartado 2 se ha querido ver una solución concreta al problema descrito[37]. Tras regular el mencionado precepto

35. Apartado 9, voto particular STEDH (Gran Sala) López Ribalda contra España, de 17 de octubre de 2019.

36. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

37. Pueden leerse así interpretaciones según las cuales el precepto (art. 89.1 apartado 2 LOPD) "contiene una precisión que se ajusta casi de manera mimética al supuesto que nos ocupa [STEDH López Ribalda II] al precisar que si se capta la comisión de un delito flagrante el deber de informar se entiende cumplido cuando exista un dispositivo al que se refiere el artículo 22.4 de la propia norma".

la posibilidad de los empleadores de tratar las imágenes obtenidas, siempre que hubieran informado de la instalación de las cámaras "con carácter previo, y de forma expresa, clara y concisa, a los trabajadores o los empleados públicos y, en su caso, a sus representantes", establece el apartado 2, a renglón seguido, que "en el supuesto de que se haya captado la comisión flagrante de un acto ilícito por los trabajadores o los empleados públicos se entenderá cumplido el deber de informar cuando existiese al menos el dispositivo al que se refiere el artículo 22.4 de esta ley orgánica"; es decir, la pegatina, adhesivo o cartel informativo, que hace pública la instalación de las cámaras.

Resulta evidente que la regulación descrita pretende dar cobertura a las posibles grabaciones casuales de flagrantes hechos delictivos, captados por una cámara instalada en un lugar determinado con otra finalidad diversa. Se trata de evitar así que la posible falta de información sobre su instalación para el control de hechos delictivos deje impune la comisión de un delito flagrante.

Sin embargo, en el caso que nos ocupa (López Ribalda), lejos de encontrarnos ante la captación casual de la comisión de un hecho delictivo por unas cámaras instaladas para otro fin, nos encontramos con que las cámaras, ocultas (o, mejor, "ocultadas"), se instalaron, justamente, con esa finalidad –grabar la perpetración de una infracción que se sabía delictiva–; y, precisamente por ello, se omitió cualquier posible información sobre las mismas a los trabajadores, a fin de poderlas captar en el momento justo en el que procedieran a la comisión de los hurtos sospechados.

Entender que el art. 89.1 apartado 2 de la LOPD podría ser aplicable a supuestos como el descrito supondría interpretar que con tal regulación se ha querido dar cobertura a la posible grabación de hechos delictivos captados por cámaras ocultas, instaladas sin informar a los trabajadores, asumiendo que la publicidad que otorga la pegatina supliría la falta de consentimiento del trabajador en estos casos. Lejos de sumarme a tal interpretación, entiendo que quienes la sostienen han pasado por alto el relevante dato de que, en tales supuestos, las cámaras han sido instaladas por el empleador, precisamente, ante la sospecha de la comisión de un hecho delictivo y con el fin de grabar su

En este sentido SÁNCHEZ QUIÑONES, L., "La rectificación del TEDH en la doctrina López Ribalda", disponible en http://www.legaltoday.com/practica-juridica/publico/proteccion_de_datos/la-rectificacion-del-tedh-en-la-doctrina-lopez-ribalda, fecha última consulta: 20 de mayo de 2020.

perpetración. No se trataría, pues –de darse–, de la captación casual de la comisión de un hecho delictivo; sino de la captación de unos hechos querida y buscada por el empleador, instalando subrepticiamente sistemas de grabación de la actividad laboral de los trabajadores.

De conformidad con la lectura que creo que debe darse al voto particular de la STEDH López Ribalda II anteriormente comentado, al proponer la autorización de la instalación de cámaras por un tercero (órgano judicial) a la vista de la justificación de los motivos en que se sustenta, entiendo que cuando un empleador tiene sospechas de la comisión de unos hechos delictivos en el seno de su empresa, debe ponerlo en conocimiento de la autoridad competente –es, además, su obligación legal[38]– que será quien, llegado el caso, solicite autorización judicial para instalar sistemas de videovigilancia en el marco de ese control de carácter penal. Lo contrario es confundir la potestad de control que el art. 20.3 del ET otorga al empresario, con la asunción de potestades pseudopoliciales que, en ningún momento, el ordenamiento jurídico le concede. Si las sospechas que albergara el empresario no lo fueran de la comisión de hecho delictivo alguno, sino de un incumplimiento grave (o no grave) por parte de los trabajadores, lejos de compartir la doctrina sentada por López Ribalda II, entiendo que la potestad de control que el art. 20 ET otorga al empresario le autorizaría a instalar todas aquellas cámaras que para la buena marcha de la empresa considere; si bien, en todo caso, previa información de las mismas en los términos y con la amplitud que la jurisprudencia, hasta el momento había venido exigiendo.

Llegados a este punto y a fin de evitar confusiones, conviene poner de manifiesto los matices diferenciales que existen entre la instalación de cámaras en situaciones como las descritas (por el empresario, para grabar la actividad de los trabajadores a fin de garantizar la buena marcha de la empresa) y la instalación de cámaras de seguridad cuya finalidad primordial es, precisamente garantizar la seguridad privada[39]. Las imágenes captadas por estas últimas cámaras, instaladas conforme a las exigencias de la normativa vigente de seguridad privada

38. Más allá de la genérica obligación legar de denunciar la comisión de hechos delictivos (art. 259 ELCrim) esa es la interpretación que cabría dar a la obligación de denunciar del profesional que tuviere conocimiento de la comisión de un delito (art. 262 LECrim).

39. Sobre el tema puede verse DURÁN SILVA, C., "Análisis de la licitud de la imagen atendiendo al sujeto que la capta", en *Era Digital Sociedad y Derecho*, (FUENTES SORIANO, Dir.), Tirant lo Blanch, Valencia, 2020, pp. 455 y ss.

y protección de datos, que reflejen la comisión de un hecho delictivo, pueden ser aportadas al proceso –aun habiendo sido captadas por un particular– y alcanzar valor probatorio, considerando la grabación aportada como si de una prueba documental se tratara (art. 726 LECrim). En este sentido se ha pronunciado la STS 649/2019, de 20 de diciembre[40] al establecer que "el objetivo esencial de la instalación de videocámaras es el de la prevención del delito (…) *[que encuentra]* cobertura legal art. 41 de la Ley 5/2014, de 4 de abril, de Seguridad Privada; Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana y su sometimiento a un cierto control administrativo por parte de la Agencia Española de Protección de datos, cuyo incumplimiento dará lugar a correcciones administrativas, pero que, como se ha expuesto, no invalida las imágenes que capten a efectos procesales si no invaden derechos fundamentales, las filmaciones aportadas por particulares son susceptibles de convertirse en prueba documental (art. 726 LECrim) en el proceso penal, siempre que cumplan requisitos como:

– no vulnerar derechos fundamentales como el de la intimidad o la dignidad de la persona al captarlas[41],

40. En lo que ahora interesa, entre los hechos que la Sentencia considera probados se encuentran las labores de vigilancia de una joyería que la coimputada realizó desde el coche en los días previos al robo, a partir de las grabaciones efectuadas por las cámaras de seguridad que había instaladas en dicha joyería. En este sentido, alega que la grabación de su conducta los días anteriores y posteriores a los hechos enjuiciados mediante los sistemas de videovigilancia en el interior y exterior de la joyería, vulneran su derecho a la intimidad y a la propia imagen. Argumenta que estos sistemas permiten grabaciones que no solo abarcan el espacio inmediatamente exterior a los establecimientos, sino que incluso graban a las personas que transitan por vías públicas por lo que considera que dichas captaciones no respetan la intimidad de estos viandantes.

41. Argumenta la STS en relación con la inexistencia de vulneración de los derechos fundamentales aludidos estableciendo que "no existe, por ello, una invasión de un derecho constitucional como el de la propia imagen capaz de conseguir una nulidad de la prueba obtenida por el simple hecho de que la imagen de una persona encausada o investigada en una fase previa de investigación policial, y, luego, en el proceso penal se ha obtenido con el tratamiento de los datos realizados a instancia de las fuerzas y cuerpos de seguridad del Estado en una cámara de grabación instalada con arreglo a la Ley de protección de datos. Precisamente, el tratamiento de sus datos es legítimo y correcto su uso adecuado por parte por parte de las fuerzas y cuerpos de seguridad del Estado y, en consecuencia, ello no provoca una injerencia en el derecho fundamental a la propia imagen capaz de afectar a la materia probatoria del proceso penal" (STS 649/2019, de 20 de diciembre; FJ 3).

– y hacerlo en espacios, lugares o locales libres y públicos, y dentro de ellos nunca en espacios considerados privados (como los aseos, vestuarios) sin autorización judicial, de forma que la captación de imágenes de personas sospechosas recogidas de manera velada o subrepticia, en los momentos en los que se supone se está cometiendo un hecho delictivo, no vulnera ningún derecho, estando permitida, por el mayor interés social de la persecución y prueba del delito que la simple captación de la imagen de la persona del delincuente".

En todo caso, volviendo a las grabaciones captadas por cámaras colocadas para el control de la buena marcha de la empresa, lo cierto es que lejos de estar ante una posición definitiva podemos considerar "en construcción" la doctrina en torno a su posible valor probatorio.

En el momento de escribir estas líneas contamos ya, en España, con los primeros pronunciamientos del TS sobre la aplicación de la doctrina López Ribalda a las grabaciones empresariales y su alcance probatorio; *v. gr.*, la STS 817/2021, de 21 de junio, dictada por la Sala de lo Social. Pero, lo cierto, es que se aplica para contextos y situaciones que no coinciden exactamente con los que originariamente motivaron la STEDH de referencia. El asunto López Ribalda se pronunciaba sobre –como se ha analizado– la posibilidad de valorar las grabaciones de unas cámaras que el empresario había puesto de forma deliberadamente oculta a la vista y conocimiento de sus trabajadores, una vez que había tenido sospechas de la comisión por parte de estos, de determinados incumplimientos contractuales graves (y aparentemente delictivos). Como se verá seguidamente, no coinciden estos hechos con los de la Sentencia que se comentará a continuación; pero la traslación de esta doctrina terminará permitiendo una mayor flexibilización en cuanto a la exigencia de información que, sobre las grabaciones, el empresario debe dar a los trabajadores. Se asume así, como se verá, que, básicamente, cualquiera que sea la forma por la que un trabajador conozca o pueda conocer la existencia de cámaras de grabación deja cubierta –o cumplida– la exigencia de información sobre su instalación que pesa sobre el empresario; se admite, pues, un cierto relajo en la necesidad de informar al trabajador, no solo sobre la propia existencia de cámaras, sino también sobre el objetivo con el que han sido instaladas y la finalidad que se dará a las grabaciones.

Al análisis de esta Sentencia, así como a la previsión de sus posibles consecuencias se dedicarán las páginas que siguen.

3. LA COMPLEJA UNIFICACIÓN DE DOCTRINA TRAS LÓPEZ RIBALDA II: EL TS SE PRONUNCIA; CONSECUENCIAS

A partir de la STEDH López Ribalda II y su reflejo en nuestros Tribunales, numerosos van a ser los casos que lleguen al Tribunal Supremo para unificación de doctrina. Es lo que ha sucedido, como se ha anunciado en el epígrafe anterior, con el asunto resuelto por la STS 817/2021, de 21 de junio (Sala 4.ª).

En esta Sentencia se estima el recurso de casación interpuesto, con la consiguiente anulación de la Sentencia del TSJ (Sala Social) y la revocación de la Sentencia del Juzgado de lo Social núm. 40 de Madrid, a fin de que se celebre un nuevo juicio en el que se admita la prueba denegada. Tanto el Juzgado de lo Social, cuanto el TSJ inadmitieron como prueba las grabaciones de las cámaras de seguridad del parking de IFEMA, aportadas para fundamentar el despido de un trabajador de la empresa Securitas Direct. El despido se declaró improcedente y Securitas Direct recurrió en casación para unificación de doctrina alegando sobre la admisión de la prueba y aportando, como Sentencia de contraste, contradictoria con la del TSJ, la STS 77/2017, 31 de enero de 2017. Como se ha anticipado, el TS estima el recurso, anula las Sentencias anteriores y ordena que vuelva a celebrarse el juicio, practicándose la prueba de las grabaciones[42].

Los hechos, muy resumidamente, son los siguientes: IFEMA había contratado con Securitas Direct los controles de seguridad. Como consecuencia de ello, un trabajador de Securitas Direct en el parking de IFEMA tenía el cometido de ver los bajos de los coches con un espejo y cumplimentar los impresos de requisas aleatorias. Hubo sospechas de que durante un periodo determinado el trabajador no cumplió con su obligación, pese a que los partes de requisas sí aparecían cumplimentados. Coincidía esto con que, poco tiempo antes de las fechas referidas, se habían actualizado los protocolos de seguridad dada la alerta de posibles atentados terroristas y, que además, pocos meses antes la policía había enviado un correo electrónico a Securitas Direct recordándole que, a la vista de los recientes atentados de Berlín, las medidas de seguridad debían ser las correspondientes al nivel de alerta 4 (esto ocurrió en diciembre de 2016 y los hechos que se enjuician en febrero

42. Con posterioridad, también sobre hechos íntimamente relacionados (acaecidos en las mismas fechas, por otros trabajadores de Securitas Direct en el Parking de IFEMA), puede verse la STS (sala cuarta) 60/2022, de 25 de enero, dictada, igualmente para unificación de doctrina.

de 2017: dos meses después). Del visionado de las cámaras de seguridad del aparcamiento (que son de IFEMA, no de la empresa Securitas Direct, a la que pertenecía el trabajador –aquí un primer escollo a efectos probatorios–) se desprende claramente que, en esas fechas, el vigilante no efectuó los controles a que venía obligado y de cuya (falsa, por tanto) realización dejó constancia. El trabajador es despedido y el Juzgado de lo Social declara el despido improcedente sin admitir la práctica de la prueba del visionado de las grabaciones por considerar que se había obtenido vulnerando derechos fundamentales. El TSJ confirma la Sentencia y el TS la revoca obligando a que se celebre de nuevo el juicio con admisión de la prueba[43].

El Juzgado de lo Social inadmitió la prueba aplicando la doctrina del TEDH en el caso Barbulescu II –ya citada en este trabajo– en lo que a la exigencia de informar al trabajador respecta[44].

Posteriormente, el TSJ de Madrid ratificará esta decisión de inadmisión sumando la aplicación al caso, de la doctrina sentada por el TEDH en la Sentencia –también citada ya en este trabajo– López Ribalda I. Considera el TSJ que "el sistema de video vigilancia era conocido por el trabajador por evidente y notorio", pero afirma que "su finalidad no era la de control de la actividad laboral de la contratista sino la de control de acceso general al recinto de IFEMA" y que el trabajador no fue "informado de forma expresa, precisa e inequívoca de la finalidad de la recogida de sus datos personales"[45].

Recuérdese que la tesis sostenida por el TEDH en López Ribalda I fue, precisamente, la de que el derecho a la protección de datos, en lo

43. Sobre la existencia de contradicción entre la Sentencia del TSJ de Madrid y la STS de 2107 que la parte alegó como contradictorio para la unificación de doctrina (STS 77/2017, 31 de enero de 2017), véase el FJ Segundo, apartado 5) de la Sentencia.

44. Nótese que de las tres SSTEDH que resultan de aplicación al caso (Barbulescu II, López Ribalda I y López Ribalda II), la Sentencia Barbulescu II es la única publicada en el momento de dictarse la Sentencia del Juzgado de lo Social: la STEDH Barbulescu II es de 5 septiembre de 2017 y la Sentencia del Juzgado de lo Social de Madrid es de 12 de septiembre de 2017 (7 días después que Barbulescu II). Anótese, ya, que, por su parte y en relación con el resto de Sentencias que marcan el *iter* procesal del caso, la del TSJ de Madrid es de 28 de septiembre de 2018 (posterior, pues a López Ribalda I –que es de 9 enero de 2018– pero anterior, todavía, a López Ribalda II que no se dictará hasta un año después –17 octubre 2019–) y la del TS, dictada para unificación de doctrina, de 21 de junio de 2021. Ésta última es, pues, la única que pudo tomar en consideración la STEDH López Ribalda II.

45. Así consta en el FJ Primero, STS 817/2021 de 21 de junio.

que al tratamiento de imágenes respecta, exige dar a conocer al trabajador, no sólo que va a ser grabado, sino también con qué finalidad va a serlo y cuál va a ser el fin o el destino posible de la grabación. Esto último es lo que, según el TSJ, no concurrió en el presente caso.

Será, finalmente, el TS quien entienda que la doctrina aplicable al caso había de ser la sostenida por el TEDH en la Sentencia López Ribalda II, con el consiguiente vuelco que ello supuso respecto del fondo de la resolución: "Era desde *[¿luego?]* lógico y razonable que, cuando se dictó la sentencia recurrida, el TSJ de Madrid se atuviese a la doctrina de la STEDH de 9 de enero de 2018 (López Ribalda I) o que incluso considerara –así parece deducirlo implícitamente– que la STEDH López Ribalda I podía matizar la doctrina de la STC 39/2016, 3 de marzo de 2016. Pero, tras la STEDH (Gran Sala) 17 octubre 2019 (López Ribalda II), lógicamente no cabe ya aplicar la doctrina de la STEDH de 9 de enero de 2018 (López Ribalda I)"[46].

Los argumentos en los que la STS 817/2021 fundamenta la admisibilidad de las grabaciones serán los siguientes:

En primer lugar, frente al entendimiento del Juzgado de lo Social y del TSJ, de que la grabación vulneraba derechos fundamentales por la ausencia de información dada al trabajador, el TS interpretó que siendo cierto que no se le informó específicamente de la instalación de esas cámaras, la realidad era que el trabajador lo conocía por cuanto su existencia era un hecho "público y notorio".

Como bien puede apreciarse, el TS está rebajando, claramente, el nivel de exigencia respecto de la información que hay que dar al trabajador sobre la posibilidad de grabar su actividad laboral; y, con ello, el nivel de protección de sus derechos fundamentales. De conformidad con esta interpretación, lo relevante pasa a ser, no tanto la información que la empresa específicamente da al trabajador, sino el conocimiento que, efectivamente, el trabajador tiene sobre la existencia de las cámaras de grabación; y en apoyo de esta nueva doctrina, la STS que ahora se comenta, trae a colación dos resoluciones fundamentales: por un lado, la STC 39/2016 de 3 de marzo que, según señala, "reduce las exigencias informativas que se deben facilitar al trabajador y que consisten, en esencia, en que conozca de la existencia de la videovigilancia"[47]

46. STS 817/2021 de 21 de junio (FJ 3.°).

47. FJ 3.° ap. 4.°, STS 817/2021. Nótese también que la STC 39/2016, 3 de marzo de 2016 que el TS considera aplicable al caso, se aplicó igualmente en la Sentencia

y, por otro, la STEDH López Ribalda II, que –como se ha tenido ocasión de analizar– rebaja también dichas exigencias[48]. En conclusión, sostiene la STS 817/2021 que "en este sentido, no es determinante que los hechos imputados al trabajador fueron anteriores a las anteriores informaciones y autorizaciones, aspecto en el que se fija la sentencia recurrida, que, como venimos diciendo, tiene como guía la STEDH 9 de enero de 2018 (López Ribalda I). Desde la perspectiva que aquí interesa, lo relevante es si el trabajador sabía que existían cámaras de videovigilancia y en el presente supuesto sí lo sabía"[49].

---

de contraste (STS 77/2017, 31 de enero de 2017[47]). En esta última, la empresa en la que el trabajador prestaba servicios tenía un sistema de videovigilancia instalado por razones de seguridad, siendo el trabajador conocedor de dicho sistema, sin que se le hubiera informado del destino que pudiera darse a las imágenes o que pudieran ser utilizadas en su contra. El 4 de octubre de 2013 la empresa le entregó carta de despido por transgresión de la buena fe contractual, fraude, deslealtad y abuso de confianza, alegando la manipulación de los tickets y el hurto de diferentes cantidades en fechas concretas, aportando como prueba las imágenes obtenidas por el sistema de videovigilancia. El TS estima el recurso de casación interpuesto considerando válidas las grabaciones y obligando a la celebración de un nuevo juicio en el que se practicara la prueba de las grabaciones denegada tanto por el Juzgado de lo Social cuanto por el TSJ vía recurso de suplicación.

48. Este descenso en el nivel de protección de los derechos fundamentales, instaurado con la STC 39/2016, así como el giro que supuso respecto de las posiciones sostenidas hasta el momento, ha sido constatado también por la doctrina. *Vid*. SEMPERE NAVARRO, A., "Un apunte sobre la grabación mediante cámaras (Al hilo de la STS-CIV 600/2019 de 7 noviembre)", Revista Aranzadi Doctrinal, ISSN 1889-4380, Núm. 2, 2020. Sostiene el autor que "La doctrina se modifica sustancialmente por la STC 39/2016, de 3 de marzo (caso Bershka), reformulando lo que se entiende por derecho fundamental a la autodeterminación informativa, con un significativo descenso en el grado de protección del art. 18.4 CE. Para entender satisfecha la obligación empresarial, es suficiente con el distintivo informativo general de zona videovigilada" al que alude la Instrucción núm. 1/2006, de 8 de noviembre, sin necesidad de comunicar a los trabajadores los ámbitos concretos de control de la prestación laboral a que pueden destinarse las grabaciones de las cámaras. Si no llegara a ofrecerse esa información general, se deriva que, en tal caso, la instalación de videovigilancia por parte de la empresa no determinaría automáticamente la vulneración del art. 18.4 CE, sino que, por el contrario, la legitimidad constitucional de la medida empresarial vendría determinada por la superación o no del principio de proporcionalidad.

49. Nótese que en el caso analizado por la STS 817/2021, se había informado al trabajador de la existencia de la grabación y se había solicitado su consentimiento para el tratamiento de las imágenes con posterioridad al acaecimiento de los hechos que se enjuician. Precisamente, es por esta información dada *a posteriori*, por lo que en aplicación de la STEDH López Ribalda I, el TSJ consideró que la prueba era inadmisible. Sin embargo, cuando el asunto llega al TS, lo que sostiene éste es que la doctrina López Ribalda I aparece superada por la Sentencia

En segundo lugar, fundamenta el TS la admisión de las grabaciones de las cámaras de videovigilancia de IFEMA, en que cumplían éstas con todas las exigencias de proporcionalidad requeridas tanto por la doctrina del TC, cuanto por la del TEDH. Sostiene, en suma, que se trató de "una medida justificada, idónea, necesaria y proporcionada al fin perseguido"[50].

Es de hacer notar que el análisis de la proporcionalidad de la medida en el presente asunto reviste una importancia capital; más allá de para justificar la decisión en el caso concreto, para entender la distancia que separa estos hechos de aquellos que se resuelven en la STEDH López Ribalda II. En el caso que nos ocupa, que la medida sea, efectivamente, proporcionada –razonamiento que comparto– legitimaría en sí mismo su aplicación, sin tener que recurrir a la doctrina López Ribalda II cuya automática traslación tan peligrosa va a resultar para los derechos fundamentales, cuanto para el conjunto del ordenamiento si, finalmente, se consolida.

La tesis sostenida por el TEDH en la Sentencia López Ribalda II nace, como se vio, de un supuesto diametralmente distinto al que aquí se analiza: las grabaciones en López Ribalda II se obtienen de una cámaras, deliberadamente ocultadas a los trabajadores, instaladas por un particular –empresario– con la finalidad de descubrir un delito respecto del cual tenía fundadas sospechas previas. Legitimar tal actuación supone otorgar al empresario poderes o competencias pseudopoliciales difícilmente admisibles en el conjunto del ordenamiento a la vista de las funciones del proceso penal y del ejercicio del *ius puniendi* del Estado. En el caso presente, sin embargo, lo que el TS propone es valorar las grabaciones obtenidas por unas cámaras instaladas públicamente, con una finalidad de prevención general que coincide, además, con la finalidad del cometido que tiene el vigilante de seguridad. Los matices entre uno y otro caso son, pues, muy diferentes.

Los argumentos que trae a colación el TS en esta sentencia (STS 817/2021), para justificar la proporcionalidad de las grabaciones y,

---

de la Gran Sala (López Ribalda II) y por la interpretación que cabe hacer a la luz de la STC 39/2016 (curiosamente, anterior a López Ribalda I y a Barbulescu), que rebajan el nivel de exigencia en la información que el empresario ha de dar al trabajador.

50. "La prueba de la reproducción de lo grabado por las cámaras de videovigilancia era, así, una medida justificada, idónea, necesaria y proporcionada al fin perseguido, por lo que satisfacía las exigencias de proporcionalidad que imponen la jurisprudencia constitucional y del TEDH". STS 817/2021, FJ 3.ª, ap. 4.°.

por tanto considerar su posible valor probatorio giran en torno a los siguientes[51]:

A. La potestad de control del empresario. Sobre la base de su reconocimiento legal se concede al empresario un margen de actuación que legitima la utilización de las grabaciones descritas.

B. El derecho a la prueba. En tanto en cuanto recae sobre el empresario la carga de probar el incumplimiento de las obligaciones laborales alegado en la carta de despido, vetar esas grabaciones es tanto como vulnerar su derecho constitucional a la prueba.

C. La proporcionalidad de la prueba. Especial mención merece en este ámbito el hecho de que la grabación obtenida coincidiera en su objetivo y finalidad con el propio cometido del trabajador; las cámaras, públicamente instaladas por IFEMA, tenían como finalidad la de controlar el cumplimiento de las normas de seguridad del recinto y el trabajador, por su parte, debía controlar, asimismo, el cumplimiento de las normas de seguridad para el acceso al recinto.

D. La existencia de intereses públicos en el caso. El incremento coyuntural de la amenaza terrorista justificaba un control eficaz y exhaustivo de las medidas de seguridad.

"En consecuencia [concluye el TS], la prueba de videovigilancia debió de admitirse porque se adecuaba a la doctrina de la STC

51. Debe tenerse adicionalmente en cuenta, en este sentido, que "es al empresario a quien le corresponde 'la carga de probar la veracidad de los hechos imputados en la carta de despido como justificativos del mismo' (artículo 105.1 LRJS), por lo que lógicamente tiene derecho a utilizar 'los medios de prueba pertinentes para su defensa' (artículo 24.2 CE), precepto este último cuya infracción denuncia expresamente el recurso de casación para la unificación de doctrina. Y, en el presente supuesto, se trataba de unas cámaras de seguridad de acceso al recinto ferial de IFEMA, conocidas por el trabajador, que podían permitir acreditar el incumplimiento de las normas de seguridad del acceso al recinto por el vigilante de seguridad, cuyo cometido era, precisamente, cumplir con esas normas de seguridad. Securitas tenía un interés legítimo amparado en sus facultades empresariales de control y en la carga de la prueba que sobre ella recaía a la hora de probar la veracidad de los hechos reprochados al trabajador. Concurrían también intereses públicos de gran importancia derivados del incremento de la amenaza terrorista, intereses que se podían ver seriamente comprometidos por un deficiente control de seguridad en el acceso al recinto ferial. Además, en el presente supuesto, coincide plenamente la finalidad de las cámaras de videovigilancia con el objeto de la prestación de servicios del trabajador: controlar la seguridad en el acceso a IFEMA. No es como en otros supuestos de videovigilancia en que la prestación de servicios del trabajador no tiene directamente como objeto garantizar la seguridad" 4.°.

39/2016, 3 de marzo de 2016, y de la STS 77/2017, 31 de enero de 2017 (Pleno, rcud 3331/2015), respetaba las exigencias jurisprudenciales de proporcionalidad y era necesaria para poder acreditar la veracidad de los hechos imputados al trabajador"[52].

En tercer lugar y en relación con la admisión de la prueba de las grabaciones, especial importancia reviste, por último, el argumento de que, que la prueba no sea nula no implica que la empresa no pueda ser responsable ante la Agencia de protección de datos por incumplimiento de la normativa: "Como señala la STEDH (Gran Sala) 17 octubre 2019 (López Ribalda II), el hecho de que, como igualmente ocurría en el supuesto enjuiciado por el TEDH, la prueba no fuera nula desde la perspectiva de la impugnación judicial de la sanción disciplinaria impuesta al trabajador, no impide que la empresa pueda ser responsable en el ámbito de la legislación de protección de datos, de manera que las allí demandantes tenían otras medidas a su disposición, como la denuncia ante la agencia o el órgano responsable de la protección de datos o el ejercicio de acciones judiciales, pues la protección de datos en el marco de la videovigilancia en el lugar de trabajo puede garantizarse por diversos medios, que pueden corresponder sin duda al derecho laboral, pero también al derecho administrativo, civil o penal, medios estos últimos que las allí demandantes optaron por no utilizar. O, como igualmente recuerda entre nosotros la STS 77/2017, 31 de enero de 2017 (Pleno, rcud 3331/2015), esgrimida como sentencia referencial en el actual recurso, la admisión de la prueba denegada no es incompatible con la posible denuncia a la Agencia Española de Protección de Datos por las infracciones que se hubieran podido cometer desde la óptica de la mencionada normativa de protección de datos"[53].

La importancia de este argumento reside en que, de consolidarse el mismo como tendencia jurisprudencial –y todo apunta a que así será–, la protección de los derechos fundamentales ya no va a canalizarse por la vía de la sanción procesal –nulidad de la prueba como prescribe el art. 11.1 LOPJ– sino por la vía de la exigencia de responsabilidad (civil, penal, administrativa…) a la persona que los vulnera.

A la vista de las anteriores consideraciones convendría apuntar ya algunas conclusiones que contribuyan a precisar y clarificar la actual situación:

52. STS 817/2021, FJ 3.ª, ap. 5.°.
53. STS 817/2021, FJ 3.°, ap. 5.°.

1. Pese a que el TS, en su Sentencia 817/2021 manifieste aplicar la doctrina del TEDH plasmada en la Sentencia López Ribalda II, los supuestos de hecho que se resuelven en ellas contienen, en realidad, matices diferenciales de notoria importancia. Este dato se torna particularmente relevante a la vista de la negativa trascendencia que puede tener la extensión automática de la doctrina sentada por el TEDH en dicha Sentencia, comentada ya en páginas anteriores de este trabajo. En este sentido, es de hacer notar que el razonamiento efectuado por el TS sobre la proporcionalidad de la prueba en el asunto de referencia, convierte su admisión en justificada y razonable sin necesidad de acudir a la doctrina López Ribalda II, totalmente cuestionable por cuanto supone la justificación de: a) una intromisión velada del empresario en DF del trabajador; b) la legitimación del empresariado para adoptar actitudes investigadoras de hechos delictivos que, en puridad, competen a los órganos oficiales de la investigación criminal.
2. La STS 817/2021 constata la cada vez más asentada tendencia jurisprudencial a valorar la admisión o inadmisión de una prueba que afecte a derechos fundamentales, en función de las circunstancias del caso concreto. Las pruebas ya no se excluyen del proceso por resultar vulneradoras de derechos fundamentales. La regla de exclusión probatoria dependerá de las circunstancias del caso y no así de que, objetivamente considerada, una prueba determinada se haya obtenido o no, con vulneración de derechos fundamentales. A esta situación, se ha llegado a través de diversas vías confluyentes: A) Rebajando el nivel de protección de los derechos fundamentales (piénsese, por ejemplo, en el derecho a la protección de datos en el ámbito laboral: ya no es necesario "informar" al trabajador de que va a ser grabado, sino que basta con que el trabajador "conozca" –y dentro de poco bastará con que pudiera conocer o debiera haber conocido, de haber obrado con una mínima diligencia– que iba a ser grabado; B) Analizando, por la vía de la proporcionalidad, las consecuencias de la admisión probatoria en el caso concreto. Así, según esta nueva tendencia jurisprudencial será posible admitir una prueba en cuya obtención se hubieran vulnerado derechos fundamentales si, por ejemplo, el daño causado hubiera sido nimio y los beneficios de su valoración, sin embargo, fueran relevantes.

3. Esta interpretación supone que los derechos fundamentales ya no van a encontrar protección sólo por la vía de la sanción procesal –de la nulidad y, por tanto, inutilizabilidad de la prueba, como proscribe el art. 11.1 LOPJ–. Coexistirá con ella otro mecanismo de protección que permitirá salvar la prueba buscando dar protección al derecho fundamental vulnerado por la vía de exigir responsabilidad (civil, penal, administrativa…) a quien lo lesionó.

4. A la vista de las conclusiones anteriores, será absolutamente relevante que las sanciones a imponer como consecuencia de la obtención de una prueba con vulneración de derechos fundamentales resulten rotundamente disuasorias; y, por supuesto, se cumplan. De lo contrario a las empresas les saldrá "más barato" y desde luego, mucho "más cómodo" vulnerar los derechos fundamentales que respetarlos. Si se trata, en suma –y esa es la (triste) conclusión–, de poner precio a los derechos fundamentales, ese precio ha de ser alto, ejemplar y efectivo.

5. Esta situación, que parece admitir justificación desde la perspectiva de las fuentes de prueba aportadas por particulares, en modo alguno puede ser extrapolada al ámbito de la investigación oficial. Se genera así una diferencia, hasta hace poco tiempo inexistente en el Ordenamiento, respecto de la nulidad o de la exclusión de la prueba obtenida con vulneración de derechos fundamentales: es posible que, cuando se trate de un particular, en atención a la proporcionalidad y a los fines con los que ha sido obtenida la prueba, quepa, en algún caso concreto, justificar su admisión; sin embargo, en las investigaciones oficiales, el Estado ha de adaptarse a las normas de desarrollo de cada concreto derecho fundamental, así como a la interpretación consolidada sobre las exigencias generales requeridas para su limitación (legalidad, jurisdiccionalidad, proporcionalidad y garantías en la ejecución de la restricción)[54]; de forma tal que, cuando se exige autorización judicial, tendrá necesariamente que contar con ella para proceder a la grabación, sea de comunicaciones o de imágenes, como en el caso que no ocupa.

54. ASENCIO MELLADO, J.M., "Los derechos fundamentales en el proceso penal", *Derecho procesal penal*, (Dir. ASENCIO MELLADO y Coord. FUENTES SORIANO), Tirant lo Blanch, Valencia, 2020, p. 157 a 161.

III. EL CONTROL EMPRESARIAL DE LAS COMUNICACIONES Y DE LOS DISPOSITIVOS INFORMÁTICOS PUESTOS A DISPOSICIÓN DEL TRABAJADOR

En el análisis de las potestades de control que el empresario puede desplegar sobre la actividad laboral del trabajador, junto a las grabaciones se incluye también, no exento de conflicto, el control sobre las comunicaciones que éste hubiera efectuado a través de los diversos dispositivos, plataformas o aplicaciones que la empresa hubiera puesto a su disposición. Al estudio del ejercicio y extensión de este posible control se dedicarán las páginas que siguen tomando como inevitable punto de partida la referencia al ya citado caso Barbulescu (resuelto definitivamente por el TEDH), incluyendo los distintos pronunciamientos habidos al respecto y, por supuesto, el fallo final de la Gran Sala que cristaliza en la STEDH de 5 de septiembre de 2017 (*Asunto Barbulescu Vs Rumania*)[55].

55. En el asunto Barbulescu contra Rumanía, la Gran Sala del TEDH revoca, en su Sentencia de 5 septiembre 2017, la dictada inicialmente por la Sección 4.ª (12/01/2016) del propio Tribunal y estima la demanda interpuesta por el Sr. Barbulescu. Entiende la Gran Sala que las pruebas utilizadas para fundamentar el despido del Sr. Barbulescu (utilización de mensajería instantánea para uso personal en el centro de trabajo) se obtuvieron por parte del empresario, violentando sus derechos fundamentales. Así, de forma extraordinariamente resumida y en lo que ahora interesa, los hechos del caso son los siguientes: el Sr. Barbulescu fue despedido por haber utilizado, durante el tiempo de trabajo, el correo electrónico con fines personales. Se interceptaron y transcribieron sus comunicaciones por la empresa arrojando como resultado que, efectivamente, había mantenido contactos personales con su hermano y con su novia. Barbulescu interpuso demanda frente a le empresa, ante el Tribunal del Condado de Bucarest alegando: 1) que las conversaciones telefónicas o por correo electrónico que un empleado realiza desde su puesto de trabajo están cubiertas por el concepto de "vida privada" y "correspondencia", y que por tanto gozan de la protección del artículo 8 del Convenio, y 2) que el despido era ilegal ya que al vigilar sus conversaciones y al acceder a su contenido, su empleador había infringido la legislación penal. El tribunal del condado consideró el despido ajustado a Derecho (los argumentos esgrimidos pueden consultarse en el Hecho 28 de la STEDH, Gran Sala, de 5 septiembre 2017). Barbulescu recurre en apelación: El Tribunal de apelación desestima el recurso (los argumentos esgrimidos pueden consultarse en el Hecho 30 STEDH). Recurre ante el TEDH y su recurso resulta desestimado por la por la Sección 4.ª del TEDH en su sentencia de 12 de enero de 2016). Finalmente, será la Gran Sala, en la Sentencia conocida como Barbulescu II la que declarará el nulo valor probatorio de los mensajes captados y aportados por el empresario al proceso, por considerar la potestad de control sobre la actividad laboral del trabajador que se ejerció por el empresario sin haberle informado previamente ni de

Efectivamente, el objetivo principal perseguido por la Gran Sala en el presente caso fue el de concretar los términos en que pueden entenderse cohonestados, de un lado el derecho del trabajador a que se respete su vida privada y su correspondencia, y de otro el de la empresa a comprobar que la actividad profesional de sus empleados es ejercida con corrección y de forma adecuada a sus directrices[56]. Con el fin de buscar el punto de encuentro entre ambos derechos, el TEDH afianza determinados criterios –acuñados ya en su conjunto como el "test Barbulescu"– que, de cumplirse, justificarán la licitud probatoria de la información obtenida por el empresario en esa investigación, eventualmente realizada amparándose en su potestad de control. Básica y resumidamente[57], los parámetros que, en función de dicha doctrina, los Tribunales deberían ponderar son los siguientes: 1) la información dada al trabajador sobre la posibilidad de supervisar sus comunicaciones –información clara y previa al establecimiento de las medidas de control–; 2) la información sobre el ámbito y alcance del control a efectuar: tanto objetivo (espacio/tiempo) cuanto subjetivo (personas potencialmente afectadas y nivel de privacidad que el trabajador puede esperar en ese ámbito concreto); 3) la información sobre las razones que justifican la vigilancia de las comunicaciones y el acceso a su contenido; 4) la proporcionalidad del carácter intrusivo de la medida (la justificación de no poder conseguir el mismo objetivo con otras medidas de control menos invasivas); 5) las consecuencias de la supervisión para el trabajador: el uso que se dará a la información obtenida y si se ajusta al objetivo declarado; y 6) las garantías concedidas al trabajador respecto de las medidas[58].

---

las condiciones en las que debían utilizarse los dispositivos tecnológicos puestos a su disposición, ni del posible control o supervisión (alcance y naturaleza de la supervisión, o lo que es lo mismo, medios, procedimientos y finalidad) que pudiera éste desplegar sobre el uso de los mismos.

56. Así resume la STS 119/2018, de 8 de febrero de 2018 (FJ 7.°), el núcleo de la cuestión tratada por la Gran Sala en la STEDH 5 de septiembre de 2017, conocida como Barbulescu II.

57. Para mayor profundidad, *vid*. el epígrafe anterior de este mismo trabajo.

58. Literalmente, la STEDH sostiene que: "(…) Los tribunales nacionales deben velar porque el establecimiento por una empresa de medidas para vigilar la correspondencia y otras comunicaciones, sea cual sea su alcance y duración, vaya acompañado de garantías adecuadas y suficientes contra los abusos (véase, *mutatis mutandis, Klass y otros contra Alemania*, 6 de septiembre de 1978 (TEDH 1978, 1), ap. 50, serie A, núm. 28, y *Roman Zakharov (PROV 2015, 292490)*, precitada, apds. 232-234) 120.

El Tribunal es consciente de que la situación está cambiando rápidamente en este ámbito. Sin embargo, considera que la proporcionalidad y las garantías

procesales contra el carácter arbitrario son elementos esenciales. En este contexto, las autoridades nacionales deberían tener en cuenta los siguientes factores:

i) ¿El empleado ha sido informado de la posibilidad de que el empleador tome medidas para supervisar su correspondencia y otras comunicaciones, así como la aplicación de tales medidas? Si bien en la práctica esta información puede ser comunicada efectivamente al personal de diversas maneras, según las especificidades fácticas de cada caso, el Tribunal considera que, para que las medidas puedan ser consideradas conforme a los requisitos del artículo 8 del Convenio (RCL 1999, 1190, 1572), la advertencia debe ser, en principio, clara en cuanto a la naturaleza de la supervisión y antes del establecimiento de la misma.

ii) ¿Cuál fue el alcance de la supervisión realizada del empleador y el grado de intrusión en la vida privada del empleado? A este respecto, debe hacerse una distinción entre el control del flujo de comunicaciones y el de su contenido. También se debería tener en cuenta si la supervisión de las comunicaciones se ha realizado sobre la totalidad o sólo una parte de ellas y si ha sido o no limitado en el tiempo y el número de personas que han tenido acceso a sus resultados (véase, en este sentido, la sentencia *Köpke*, precitada). Lo mismo se aplica a los límites espaciales de la vigilancia.

iii) ¿El empleador ha presentado argumentos legítimos para justificar la vigilancia de las comunicaciones y el acceso a su contenido (véase, en los apartados 38, 43 y 45 supra, el estado del derecho internacional y europeo en la materia)? Dado que la vigilancia del contenido de las comunicaciones es por su naturaleza un método mucho más invasivo, requiere justificaciones más fundamentadas.

iv) ¿Habría sido posible establecer un sistema de vigilancia basado en medios y medidas menos intrusivos que el acceso directo al contenido de comunicaciones del empleado? A este respecto, es necesario evaluar, en función de las circunstancias particulares de cada caso, si el objetivo perseguido por el empresario puede alcanzarse sin que éste tenga pleno y directo acceso al contenido de las comunicaciones del empleado.

v) ¿Cuáles fueron las consecuencias de la supervisión para el empleado afectado (véase, *mutatis mutandis*, el criterio similar aplicado al examen de la proporcionalidad de una injerencia en el ejercicio de la libertad de expresión protegida por el artículo 10 del Convenio (RCL 1999, 1190, 1572) en *Axel Springer AG contra Alemania (PROV 2012, 46200)* [GS], núm. 39954/08, ap. 95, 7 de febrero de 2012, con las referencias citadas)? ¿De qué modo utilizó el empresario los resultados de la medida de vigilancia, concretamente si los resultados se utilizaron para alcanzar el objetivo declarado de la medida (véase, en este sentido, la sentencia *Köpke*, precitada)?

vi) ¿Al empleado se le ofrecieron garantías adecuadas, particularmente cuando las medidas de supervisión del empleador tenían carácter intrusivo? En particular, estas garantías debían impedir que el empleador tuviera acceso al contenido de las comunicaciones en cuestión sin que el empleado hubiera sido previamente notificado de tal eventualidad.

En este contexto, debe recordarse que, para poder prosperar, las relaciones laborales deben basarse en la confianza entre las personas (sentencia Palomo Sánchez y otros [TEDH 2011, 68], precitada, ap. 76) 121.

Por último, las autoridades internas deben velar para que los empleados, cuyas comunicaciones hayan sido objeto de seguimiento, puedan presentar un recurso ante un órgano judicial que tenga competencia para pronunciarse, al menos en esencia, sobre el cumplimiento de los criterios antes expuestos y la legalidad de las medidas impugnadas (sentencia *Obst*, ap. 45; y *Köpke*, precitada)" (Considerandos 119 a 121 STEDH –Gran Sala– Barbulescu Vs Rumanía, de 5 de septiembre de 2017).

La aplicación de estos parámetros ha sido asumida ya por nuestra Jurisprudencia[59] y, en cierto modo, va a contribuir a poner fin a la tensión que la valoración de la ilicitud de la prueba estaba generando entre la Jurisdicción penal y laboral en España.

El punto de inflexión en esta polémica, vino dado por la STS 528/2014, de 16 de junio. En el asunto por ella analizado, la Sala 2.ª (o de lo Penal) del TS, considera nula la prueba obtenida por el empresario a raíz del examen del ordenador de un trabajador por entender que al haberse realizado dicha intromisión sin autorización judicial vulnera el Derecho al Secreto de las comunicaciones y, por tanto, no puede surtir efectos en el proceso. Sin embargo, en el ámbito laboral y a efectos de justificar el despido del trabajador, la jurisdicción social avaló la valoración probatoria de dicha información por entender que se amparaba en la potestad de control del empresario, legalmente reconocida. La esquizofrenia que provocaba esta interpretación era más que patente, pues resulta difícil asumir que una misma prueba vulnera derechos fundamentales y, en consonancia, no puede ser valorada por la jurisdicción penal a efectos de sostener una eventual condena; pero sí puede ser valorada y surtir efectos, sin embargo, en el ámbito de la jurisdicción social a efectos de fundamentar un eventual despido[60].

Y, lo cierto, es que así lo constató el TS en la sentencia citada (STS 528/2014, de 16 de junio. Sala 2.ª), al sostener que "(…) esta Sala considera conveniente, en aras a fijar una clara doctrina en materia de tanta trascendencia, salir al paso de ciertas afirmaciones rotundas, incluidas en la propia Resolución de instancia a pesar de aquellas iniciales constancias referentes a la irrelevancia de la prueba, tales como las de que '…el ordenador registrado era una herramienta propiedad de la empresa y facilitada por la empresa a don (sic) Rodolfo exclusivamente para desarrollar su trabajo, por lo que entendemos que incluso en aquel supuesto en que pudiera utilizar el ordenador para emitir algún tipo de mensaje de carácter personal, entendemos que al utilizar precisamente un ordenador ajeno, de la empresa, y destinado exclusivamente para el trabajo a la empresa, estaba asumiendo –cediendo– la

59. Último exponente de esta asunción, al momento de escribir estas líneas, es la STS (Sala 2.ª) 132/2022, de 24 de enero.

60. Sobre el tema me he ocupado ampliamente en "La prueba prohibida. viejos problemas procesales de las nuevas tecnologías", en *Justicia y proceso en el S. XXI. Desafíos y tareas pendientes*, PRIORI POSADA. G. (Coord.), Ed. Palestra, Perú, 2019.

falta de confidencialidad –secreto– de las comunicaciones que pudiera tener el señor (sic) Rodolfo utilizando tal terminal informático'. Como la propia Sentencia recurrida nos dice a continuación, son éstos argumentos los utilizados en el ámbito jurisdiccional de lo social, a partir de la importante Sentencia de 26 de Septiembre de 2007, luego seguida y ampliada en sus efectos por otras de la misma Sala Cuarta de este mismo Tribunal, como las de 8 de Marzo y 6 de Octubre de 2011, e incluso la de 7 de Julio de 2010, referida precisamente a estos mismos hechos, aun cuando en su dimensión laboral a la hora de valorar la prueba informática y sus efectos para acreditar las razones de procedencia del despido acordado respecto del recurrente por la empresa PARQUES REUNIDOS S.A., en la que prestaba sus servicios. Criterios contenidos en esas Resoluciones y que no desconocemos que han sido posteriormente avalados por el propio Tribunal Constitucional, en Sentencias como las de 17 de Diciembre de 2012 y 7 de Octubre de 2013, que, a nuestro juicio, han de quedar restringidos al ámbito de la Jurisdicción laboral, ante el que obviamente nuestra actitud no puede ser otra más que la de un absoluto respeto, máxime cuando cuentan con la confirmación constitucional a la que acabamos de referirnos, pero que, en modo alguno, procede que se extiendan al enjuiciamiento penal, por mucho que en éste la gravedad de los hechos que son su objeto, delitos que en ocasiones incluso constituyen infracciones de una importante relevancia, supere la de las infracciones laborales a partir de las que, ante su posible existencia, se justifica la injerencia en el derecho al secreto de las comunicaciones del sospechoso de cometerlas. En efecto, a nuestro juicio, el texto constitucional es claro y tajante cuando afirma categóricamente que: 'Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial'. No contempla, por tanto, ninguna posibilidad ni supuesto, ni acerca de la titularidad de la herramienta comunicativa (ordenador, teléfono, etc. propiedad de tercero ajeno al comunicante), ni del carácter del tiempo en el que se utiliza (jornada laboral) ni, tan siquiera, de la naturaleza del cauce empleado ('correo corporativo'), para excepcionar la necesaria e imprescindible reserva jurisdiccional en la autorización de la injerencia. Tampoco una supuesta 'tácita renuncia' al derecho, como a la que alude la Audiencia al final del párrafo antes transcrito, puede convalidar la ausencia de intervención judicial, por un lado porque obviamente dicha 'renuncia' a la confidencialidad, o secreto de la comunicación, no se produce ni es querida por el comunicante que, de conocer sus consecuencias, difícil es imaginar que lleve

a cabo la comunicación objeto de intervención y, de otra parte, porque ni aun cuando se entienda que la 'renuncia-autorización' se haya producido resultaría operativa ya que, a diferencia de lo que ocurre con la protección del derecho a la inviolabilidad domiciliaria (art. 18.2 CE), nuestra Carta Magna no prevé, por la lógica imposibilidad para ello, la autorización del propio interesado como argumento habilitante para la injerencia. Y es que un régimen de protección tan estricto, en relación con el derecho al secreto de las comunicaciones, sin duda el más enérgico de los que dentro del genérico derecho a la intimidad se contemplan en el repetido artículo 18 de la Constitución Española al excluir cualquier posible supuesto que no contemple la intervención del Juez como tutelador del derecho del investigado, encuentra un lógico fundamento en la gravedad y trascendencia de esta clase de injerencias, en tanto que se introducen y revelan toda clase de aspectos referentes a la privacidad del comunicante, tanto los de interés para la investigación como otros por completo ajenos a ese legítimo interés, dicha injerencia además se produce en una ominosa aunque inevitable situación de absoluta indefensión, por ignorancia coetánea, del sometido a ella y, lo que es aún más decisivo, porque por mucho que el investigado, como en el caso presente, sea empleado de la dueña del instrumento, la incursión en sus comunicaciones produce automática e inmediatamente la injerencia en el correspondiente derecho al secreto de los terceros que con él comunican, ajenos a esa relación con el titular de la herramienta y de sus condiciones de uso"[61].

A tenor de lo dispuesto en esta Sentencia (STS 528/2014, de 16 de junio), no admitía el TS ningún tipo de distinción o matiz que permitiera convalidar, en el ámbito penal, el nulo valor probatorio que le merecía una intervención de comunicaciones practicada sin autorización judicial. Así, cuando la prueba (las comunicaciones de un trabajador obtenidas por el empresario en ejercicio de su potestad de control) había de desplegar su valor en un proceso penal, no aceptaba matices ni respecto de la titularidad del instrumento comunicativo intervenido (ordenador, teléfono, etc. propiedad de tercero ajeno al comunicante –el empresario–), ni respecto del tiempo en el que se utilizó (si fue o no en jornada laboral) ni, tan siquiera, respecto de la naturaleza del cauce empleado ("correo corporativo"). En todos los casos posibles, a la luz de esta Sentencia, entendía el TS que, o la información obtenida como producto de una intervención de comunicaciones lo había sido

61. STS 528/2014, de 16 de junio FJ Primero, Apartado B).

previa autorización judicial, o no podría alcanzar valor probatorio en el ámbito del proceso penal; llegando incluso a apuntar la posibilidad de que en los supuestos de "tácita renuncia" por el trabajador al secreto de sus comunicaciones, tampoco la información aportada al proceso podría alcanzar valor probatorio si no se contó, para su obtención, con la pertinente autorización judicial.

Y esta es, precisamente, la posición jurisprudencial que cambia a raíz de la Sentencia Barbulescu II: cuando se trate del ejercicio de las potestades de control del empresario sobre la actividad del trabajador –incluyendo la intervención de las comunicaciones que pudiera mantener a través de los diversos dispositivos informáticos de la empresa–, la clave que convertirá en legítima la posible injerencia de aquél sobre los derechos fundamentales de éste, residirá en la información (cualitativa y cuantitativa) que le hubiera proporcionado sobre el ejercicio de su poder de supervisión. A ello se suma, además, el reconocimiento por el TS de que el derecho afectado por el empleador mediante la supervisión de la actividad que el trabajador pudiera haber desplegado a través de internet, no es tanto el derecho al secreto de las comunicaciones (que requiere de autorización judicial ex art. 18.3 CE) cuanto el derecho, de nueva creación, al propio entorno virtual, anteriormente referido y analizado[62].

La doctrina Barbulescu ha sido reconocida y acogida sin fisuras por nuestros Tribunales y, en consonancia con ella, será, pues, tras la STS 119/2018 (Sala 4.ª) en el ámbito social y la posterior STS (Sala 2.ª)

62. Sobre la importancia que tiene la apreciación por el TS de este nuevo derecho al entorno digital en la evolución del tema que nos ocupa (la posible licitud de la intervención de las comunicaciones del trabajador por el empresario) y el análisis que de ello realiza la STS 489/2918, de 23 de febrero, puede verse DEL MORAL GARCÍA, A., "Prueba ilícita, entorno digital y derechos fundamentales: divergencias entre la jurisprudencia social y la penal", en Era digital Sociedad y Derecho (FUENTES SORIANO, Coord.), Tirant lo Blanch, 2020, pp. 352 a 355. Sostiene el autor, precisamente, que es éste uno de los extremos en los que se basa el TS para superar las diferencias que se establecían en la Sentencia de 2014 ya citada y que se situaban en la base de este distinto tratamiento de la ilegitimidad probatoria en el ámbito laboral y penal. Según manifiesta el autor, en la STS 489/2018, "el Tribunal Supremo entiende que se afectó de forma ilegítima un derecho fundamental, en concreto un derecho de nueva generación que ha venido a ser bautizado como derecho al entorno digital. No se trata ni del derecho al secreto de las comunicaciones, ni la intimidad. Es otro derecho. Eso permite orillar los distingos que hacía la STS antes citada 528/2014, de 16 de junio". DEL MORAL GARCÍA, A., "Prueba ilícita (…)", cit., p. 352.

489/2018, de 23 de octubre, en el ámbito penal cuando, las divergencias sobre el valor probatorio de la información aportada al proceso por el empleador y obtenida en el ejercicio de sus potestades de control, resulten finalmente superadas[63]. Así, y partiendo de la constatación de que no es posible equiparar las exigencias que debe regir la actuación del empresario en el ejercicio de sus facultades de control, con las de los poderes públicos en el ejercicio de sus potestades de investigación, señala el TS en su Sentencia 489/2018 que si bien la licitud de la investigación oficial que supone el acceso a las comunicaciones pasa por la autorización judicial o, en su caso, del investigado; en los supuestos de supervisión laboral, la licitud de la información obtenida por el empresario pasa por el conocimiento que el trabajador hubiera tenido del ámbito, extensión y efectos con que podía ejercitarse dicho poder de supervisión[64]. En lapidaria expresión del propio Tribunal, "el reconocimiento previo, explícito o implícito, de esa facultad del empresario constituye el *punctum dolens*, la clave, en el ámbito de las relaciones

63. Nótese, sin embargo, que la STS 119/2018 trae causa de un recurso de casación para unificación de doctrina en el que la Sentencia que se recurre (STSJ Galicia 30/12/14; confirmatoria del despido improcedente declarado por el Juzgado de lo Social núm. 1 de A Coruña en Sentencia de 14/04/14) no pudo hacerse eco de la doctrina Barbulescu por haber sido dictada con anterioridad. Ello no obstante, el TS recoge y analiza la misma en su FJ 7.ª con el fin de justificar su adecuación constitucional, por un lado, y la legitimidad de la solución alcanzada, por otro. Literalmente puede leerse: "SÉPTIMO. 1. Aunque por obvias razones temporales en el presente procedimiento no se pudo tener en cuenta hasta la fecha la STEDH –Gran Sala– 05/Septiembre/2017 [Caso 'Barbulescu'], parece conveniente que nos refiramos a tan reciente doctrina, no sólo para evidenciar que sus criterios son sustancialmente coincidentes con los de la jurisprudencia constitucional más arriba indicados, sino también que –precisamente por ello– la conducta empresarial de autos pasa holgadamente el filtro de los requisitos que el Alto Tribunal europeo exige para atribuir legitimidad a la actividad de control que acabamos de enjuiciar". Así, en consecuencia con todo ello, el TS entiende que la prueba derivada de la intervención de las comunicaciones realizada por el empresario en este caso concreto, debe considerarse lícitamente obtenida y podría, por tanto, llegar a ser valorada. Literalmente, sostiene el segundo pronunciamiento del fallo: "2.° Estimar el recurso formulado por 'Inditex, SA', atribuyendo plena validez procesal a la prueba derivada del examen del correo electrónico existente en ordenador del trabajador".

64. Según sostiene la citada Sentencia, "En el primer caso *[ámbito laboral]* nos movemos en el marco de una relación contractual entre particulares. La clave estará en si el trabajador ha consentido anticipadamente reconociendo esa capacidad de supervisión al empresario y, por tanto, cuenta con ello; está advertido; es decir, es una limitación conocida y contractualmente asumida. En las relaciones con los Poderes Públicos, sin embargo, no cabe esa 'cesión' anticipada o renuncia previa a ese espacio de intimidad virtual".

laborales. En una investigación penal lo será la autorización judicial o el consentimiento actual".

La Sentencia citada (STS 489/2018, de 23 de octubre) trae causa del recurso interpuesto frente a la condena de un alto directivo de una empresa por delito de apropiación indebida en la que se aportó como prueba (entre otras) la información obtenida como resultado de la intervención de las comunicaciones del trabajador (aportación de unos correos electrónicos) por el empresario. Pese a que la monitorización de los ordenadores se produjo de forma escrupulosa, con un programa que permitía seleccionar los correos y con la intervención de un perito informático a lo largo de todo el proceso de intervención (entre otras muchas cautelas), no consta que en ningún momento el trabajador hubiera sido informado, ni hubiera dado su consentimiento sobre una posible supervisión de sus comunicaciones por parte del empleador. Así, en consonancia con la citada doctrina Barbulescu, el TS considera nula la prueba. Y lo hace sobre la base de esa ausencia consentimiento del trabajador que no es posible deducir, siquiera implícitamente. No será ya la titularidad del ordenador la que legitime la intromisión del empresario en las comunicaciones del trabajador, sino la información que éste facilite sobre el posible ejercicio de su facultad de supervisión, el alcance de la misma, el destino que vaya a dar a la información obtenida y las formas en las que pueda llevar a cabo la intervención. La información y asunción, pues, por el trabajador de esa posibilidad de supervisión se torna ahora en la pieza clave que permitirá apreciar la legitimidad probatoria de las fuentes aportadas por el empresario.

Precisamente, en relación con la información que debe darse al trabajador respecto del ejercicio de la potestad de control por el empresario, surge un elemento importante en la presente sentencia al que cabe prestar una especial atención por cuanto contribuye a debilitar –a mi juicio– la criticable doctrina sostenida por la STEDH López Ribalda II respecto de la grabación de la actividad laboral. He tenido ocasión de pronunciarme críticamente respecto del viraje doctrinal que lleva a la Gran Sala del TEDH a admitir el valor probatorio de unas grabaciones obtenidas mediante la instalación de cámaras ocultas por parte del empresario. Esta posibilidad, atentatoria contra los derechos fundamentales del trabajador y generadora –en mi opinión– de una profunda inseguridad jurídica, al dejar en manos del empresario la ponderación de la gravedad de los hechos (que es lo que justifica la instalación, en su caso, de las cámaras ocultas) encuentra fundamento, según el propio TEDH (Gran Sala), en la doctrina Barbulescu.

La licitud, así, de las grabaciones obtenidas por el empresario mediante la instalación de cámaras ocultas, aparece justificada en la Sentencia López Ribalda II, por la existencia de sospechas de estar cometiéndose graves irregularidades (importantes pérdidas económicas sufridas por la empresa y la imposibilidad de identificar al causante de las mismas). Y se admite que, en la decisión de instalar las cámaras ocultas, tales motivos hayan sido exclusivamente valorados por el empresario que adopta la medida, aun reconociendo que las sospechas de ese incumplimiento grave conllevaba la presunta comisión de un hecho delictivo. Precisamente frente a ello alzan su voz los tres magistrados disidentes que, en el voto particular, insisten en que la instalación de cámaras ocultas sólo encontraría justificación en el marco de un proceso penal incoado ante la sospecha de la comisión de hechos delictivos y previa autorización de un tercero ajeno (autoridad judicial, en mi opinión) que valorará la existencia de los mismos. La justificación, pues, de la medida y la legítima instalación de las cámaras ocultas exigiría, de acuerdo con el voto particular de la STEDH López Ribalda II un examen (judicial, en mi opinión) *ex ante*, de los motivos y no un examen *ex post* que, en ningún caso, evitaría la lesión.

No otra puede ser una solución respetuosa con los derechos fundamentales del trabajador; una solución que cohoneste –efectivamente y como pretendía la Gran Sala en el caso Barbulescu– su derecho a la privacidad con las potestades de control del empresario. Y, precisamente por ello, cuando el TS, en su Sentencia 489/2018, de 23 de octubre, recoge expresamente la aplicación de la doctrina Barbulescu en el ámbito penal, establece que:

"la evaluación de si ha existido vulneración ha de realizarse mediante un juicio *ex ante*: no depende de que efectivamente se hayan obtenido elementos sensibles desde el punto de vista de la privacidad. Y se protege aunque *ex post* se compruebe que solo se han descubierto comunicaciones o efectos a los que debía tener acceso el promotor de la intromisión: que se invada el ordenador usado por una persona y se descubra que solo contiene fotos de quien accede ilegítimamente a él; o que se entre sin autorización en el domicilio del supuesto ladrón para recuperar el móvil sustraído con un método –llamadas al número específico para localizarlo– que va a permitir acceder en exclusiva al efecto que es de titularidad del invasor, no convierte en legítima la intromisión.

La valoración de la legitimidad de la actuación inicial (acceso al ordenador que usaba el querellado) no puede hacerse más que

mediante un juicio ex ante. A esos efectos es indiferente que solo se hayan buscado elementos que tuvieran relación con la actividad mercantil de la empresa o que se haya eludido cuidadosamente adentrarse en cualquier archivo o comunicación en la que se percibiese el más mínimo aroma de vinculación con la intimidad o la privacidad. Esto, que solo es posible dilucidar en un juicio *ex post*, no cambia ni puede cambiar la valoración que se hace *ex ante*.

¿Se puede entrar en un domicilio particular sin consentimiento del titular ni autorización judicial cuando se sabe no ocupado en ese momento y con el único fin de recuperar un efecto robado tiempo antes que está a la vista? No. Sin matices.

¿Se puede acceder a un dispositivo de almacenamiento masivo usado por un empleado con la firme y decidida finalidad de acceder en exclusiva a los archivos relacionados con la empresa? En principio no. Tan solo cuando haya precedido un consentimiento expreso o derivado implícita e inequívocamente del compromiso asumido previamente por el trabajador, será legítima esa actuación. El empleo de una herramienta de filtrado del tipo búsqueda 'ciega' no legitima por sí sola la injerencia (*vid*. voto particular STC 23/2018; la sentencia mayoritaria no aborda esa cuestión).

Limitar los perjuicios de la intromisión a lo estrictamente necesario consiguiendo no afectar a elementos ajenos a la empresa o relacionados con la intimidad del usuario no sirve para revertir en legítima la intromisión *ab initio* ilegítima. Ha de ser una valoración apriorística y no a expensas de los concretos contenidos obtenidos. La ilegitimidad no deriva del contenido obtenido, ni de la forma de acceso más o menos intrusiva, sino del mismo acceso inconsentido y no advertido previamente"[65].

Con posterioridad a esta Sentencia, específica mención merece la aplicación del "test Barbulescu" en la STS 132/2022, a fin de determinar si la aportación de unos correos electrónicos captados por el empresario, vulneraron los derechos fundamentales de los querellados. Tras analizar y dar respuesta, uno o a uno, a los seis interrogantes que el TEDH señaló como parámetros de análisis a la hora de ponderar esa eventual vulneración, concluye que "en el caso el exhaustivo acceso a los contenidos de correo electrónico no vino precedido de ninguna advertencia, no estuvieron presentes las personas afectadas,

65. STS 489/2018, de 23 de octubre, FJ 11.°.

no se identificó previamente una finalidad precisa, vinculada a la propia actividad empresarial desarrollada, no se adoptó ninguna fórmula de atemperación de la extensión subjetiva del acceso y los contenidos documentados fueron, finalmente, utilizados para fundar la acción penal, no solo contra el otro socio sino también contra los propios empleados usuarios de las cuentas de correo. (…) El acceso fue desproporcionado y lesionó los derechos a la privacidad y a la intimidad de las personas afectadas"[66].

En suma, pues, será la información previa dada al trabajador respecto de la posible intromisión que, en el ejercicio de la potestad de control, el empresario puede ejercer sobre sus comunicaciones lo único que, efectivamente, legitimará tal actuación. Cierto es que las exigencias y el alcance de dicha información son amplias y exhaustivas; pero es la contraprestación necesaria que el respeto de los derechos fundamentales del trabajador exige al empresario para ejercitar legítimamente su potestad de control.

Y como conclusión, asumido el necesario conocimiento previo del trabajador respecto de las medidas de control, es de hacer notar que no se aprecia diferencia alguna que justifique un distinto tratamiento para legitimar la intromisión del empresario en las comunicaciones del trabajador o la grabación de su actividad en el centro de trabajo[67]. En ambos casos, los derechos fundamentales afectados (al propio entorno virtual y a la protección de datos respectivamente; juntamente, en su caso, con la privacidad) exigen una información exhaustiva y previa sobre las medidas de intromisión a adoptar por el empresario. En tal sentido, resulta difícil compartir la doctrina sentada por López Ribalda

66. Primer motivo de los fundamentos de derecho, Parágrafo 11. STS 132/2022, de 24 de enero.

67. La información previa al trabajador, el conocimiento exhaustivo de las medidas adoptadas y su consentimiento respecto de éstas, es lo que permite entender salvada la reserva jurisdiccional con la que el art. 18.3 CE garantiza el derecho al secreto de las comunicaciones. *In extenso* sobre el tema *vid*. STS (Sala 4.ª) de 8 de marzo de 2011, ROJ 1323/2011 (con fundamento concreto en la doctrina del TC sobre la materia); y, por supuesto, la ya comentada STEDH Barbulescu II. Contra la posibilidad de otorgar valor probatorio a la intervención de las comunicaciones obtenidas por el empresario sin autorización judicial, aun en los supuestos de información previa analizados, *vid.*, VEGAS TORRES, J., "Sobre la ilicitud de las pruebas obtenidas por las empresas mediante el control de las comunicaciones electrónicas de los trabajadores", en *Derecho Probatorio y otros estudios procesales. Liber amicorum Vicente Gimeno Sendra* (Asencio mellado, Dir.), Castillo de Luna, 2020, p. 1978.

II al considerar legítimas las grabaciones obtenidas a partir de la instalación de unas cámaras ocultas con las que, en realidad, no se buscaban sino pruebas de la comisión de un hecho delictivo, cuando dicho delito no había sido puesto en conocimiento de la autoridad competente, ni se había recabado autorización de ésta que pudiera resultar legitimadora de la intromisión. Aunque ésa haya sido la opción sostenida –en mi opinión, erróneamente– por el TEDH en su Sentencia López Ribalda II, ni tiene un fundamento jurídico claro ni, en modo alguno, deriva –como pretende– de la aplicación de la doctrina Barbulescu, previamente sentada por el propio Tribunal.

IV. LA EVOLUCIÓN DE LA REGLA DE EXCLUSIÓN ANTE LAS NUEVAS PRUEBAS TECNOLÓGICAS

Como se ha tratado de mostrar a lo largo del presente trabajo, la utilización cotidiana de distintos mecanismos tecnológicos, hoy al alcance de todos, favorece la obtención de información que, si bien puede resultar enormemente esclarecedora de una puntual situación de hecho, puede asimismo resultar lesiva de los derechos fundamentales del ciudadano a que dicha información se refiere.

La patente realidad de los hechos que la información así obtenida revela, ha puesto en evidencia la ya cuestionada eficacia del art. 11.1 LOPJ como único mecanismo de protección de los derechos fundamentales[68].

Dado el actual estado de nuestra Jurisprudencia podemos afirmar hoy, con meridiana claridad, que la protección de los derechos fundamentales se va a articular a través de dos mecanismos distintos en función de si la lesión proviene del Estado o de un particular.

La sanción procesal que contempla el art. 11.1 LOPJ castigando con la nulidad a aquella prueba obtenida con vulneración de derechos fundamentales, mantendrá su plena vigencia y aplicación en los supuestos en los que la vulneración proceda de los órganos públicos de investigación[69]. Sin embargo, cuando la actuación proceda de un particular, las

68. Sobre el tema, ARMENTA DEU, T., *La Prueba Ilícita. Un estudio comparado*, Ed. Marcial Pons, 2011. En particular, dedica el capítulo III al estudio de las distintas soluciones ensayadas a nivel comparado en relación con la eficacia de la prueba ilícitamente obtenida.

69. Con rotundidad se expresa la STS 116/2017, de 23 de febrero, cuando sostiene que "la acción vulneradora del agente de la autoridad que personifica el interés del Estado en el castigo de las infracciones criminales nunca puede ser artificialmente

últimas tendencias doctrinales y jurisprudenciales buscan encontrar nuevos caminos –sin rechazar el de la exclusión probatoria, cuando proceda– que flexibilicen tal consecuencia, permitiendo otorgar valor probatorio a la información obtenida si bien, sancionando la actuación lesiva del derecho fundamental por vías diferentes a la del proceso. Elocuente resulta, en este sentido, la afirmación de que la prohibición de valorar las pruebas obtenidas con vulneración de derechos fundamentales "no persigue sobre proteger al delincuente que se ve encausado con el respaldo de pruebas que le han sido arrebatadas por un particular que cuando actuaba no pensaba directamente en prefabricar elementos de cargo utilizables en un proceso posterior"[70].

El conflicto de intereses queda magistralmente resumido por ARMENTA haciendo acopio de algunos "casos no inéditos en nuestros Tribunales: el particular que abre descuidadamente la carta, destinada al vecino y depositada por el cartero, por error, en su buzón, y en la que aparece droga; el robo de una vivienda donde los autores (luego detenidos por la policía) descubren cocaína que se llevan; el empleado que sin contar con consentimiento para ello se adentra con inocente propósito en las dependencias del domicilio de su principal y encuentra el cadáver allí escondido; el hurto de un ordenador en el que se descubre pornografía infantil. Ninguno es puramente imaginario. En todos un particular –actuando a veces de buena fe–, vulnera objetivamente (otra cosa es que en algún caso existiendo antijuricidad no haya culpabilidad) un derecho fundamental (privacidad, en el supuesto del ordenador; inviolabilidad del domicilio, en la entrada en las viviendas; secreto de las comunicaciones al abrir la carta sin advertir el error). Pero lo hace sin perspectiva procesal alguna: actuando sin dolo en algún caso; en otros movido por ánimo de lucro o por motivos ilegítimos o delictivos pero sin horizonte procesal alguno… ¿En todos estos casos hay que acudir al expediente del art. 11.1 LOPJ?"[71].

---

equiparada a la acción del particular que, sin vinculación alguna con el *ius puniendi*, se hace con documentos que más tarde se convierten en fuentes de prueba que llegan a resultar por una u otra circunstancia, determinantes para la formulación del juicio de autoría". (…) "La prohibición de valorar las pruebas obtenidas con vulneración de derechos fundamentales cobra su genuino sentido como mecanismo de contención de los excesos policiales en la búsqueda de la verdad oculta en la comisión de cualquier delito". Posteriormente, en esta misma línea, también SSTS 87/2017, de 19 de abril o 489/2018, de 23 de octubre, entre otras.

70. STS 116/2017, de 23 de febrero.

71. ARMENTA DEU, T., "Prueba ilícita y regla de exclusión: perspectiva subjetiva", Derecho probatorio y otros estudios procesales *Liber amicorum* Vicente Gimeno Sendra (ASENCIO MELLADO, Dir.), Ed. Castillo de luna, 2020, p. 126.

Esa es, efectivamente, la cuestión. La rigidez de aplicar la regla de exclusión probatoria a todo tipo de supuestos por igual, termina planteando situaciones de injusticia material que hacen aconsejable, por tanto, la búsqueda de respuestas a través de mecanismos diferentes. En estos nuevos caminos se adentra tanto la doctrina cuanto la última Jurisprudencia; también, como se verá, las más novedosas tendencias legislativas todavía no fructificadas, sin embargo, en normativa vigente.

Cuando la infracción proviene de un particular que, sin ánimo de preconstituir prueba, se ha hecho con una información útil al proceso, la doctrina apuesta –no siempre unánimemente[72]– por reconocer la relevancia probatoria de dicha información si bien dando protección a los derechos fundamentales desde el derecho sustantivo y a través de la exigencia de responsabilidad al infractor o incluso de mecanismos premiales para quién haya podido ver así vulnerados sus derechos[73].

La Jurisprudencia, por su parte, se inclina ya claramente por salvar la información probatoria así obtenida siempre que se haya podido constatar la "buena fe" en su obtención; entendiendo por "buena fe" que no se obtuvo con intención de preconstituir prueba. Así lo atestigua el TS cuando sostiene que "(…) por tradición, por teleología, por ponderación de derechos fundamentales en tensión y por sus finalidades, el juego de esa norma, de máxima intensidad cuando la violación

72. En contra, por todos, *vid*. ASENCIO MELLADO, J.M., "La STC 97/2019, de 16 de julio".

73. En este sentido, sostiene VELASCO NÚÑEZ que "cabrían también soluciones alternativas, graduables, o compensaciones premiales a favor de quien sufra la ilicitud probatoria, todo en función, bien de la gravedad del ataque, bien del derecho o la libertad fundamental afectada, bien en razón del concreto delito investigado, bien a todos ellos, debiendo resolver el estándar ético básico que el Estado Democrático se fije, si su sanción seguiría siendo la anulación probatoria, o meramente la reducción o compensación de la pena concreta a quien se le haya vulnerado un derecho o libertad fundamental, o si incluso bastaría con imponer una sanción a quien la vulneró sin efecto sobre el valor de la prueba misma". VELASCO NÚÑEZ, E., "Prueba penal prohibida obtenida por particular. Autograbaciones, grabaciones subrepticias y filtraciones de privacidades ajenas en chats y foros" en Revista Aranzadi de Derecho y Proceso Penal, 2019 Núm. 53 (Enero-marzo). Del tema me he ocupado con profundidad en "La prueba prohibida aportada por particulares (…)", *op. cit*. Asimismo, un estudio exhaustivo de la doctrina extranjera sobre la materia puede verse en CUADRADO SALINAS, C., *Fundamento y efectos de la exclusión de la prueba obtenida con vulneración de derechos fundamentales,* Tirant lo Blanch, Valencia, 2021.

proviene de un agente estatal, consiente más modulaciones en el caso de particulares (son frecuentes en el derecho comparado las regulaciones de esta materia que dejan al margen las actuaciones de particulares: U.S.A., Francia, Holanda, México, Bélgica con matices). Por eso la jurisprudencia reciente ha admitido que en el caso de particulares estamos en un terreno más permeable a excepciones (SSTS 87/2017, de 19 de abril o 116/2017, de 23 de febrero). En las relaciones entre particulares, las exigencias de la doctrina de la prueba ilícita son más débiles porque las necesidades de protección y la potencialidad de agresión son en principio, menores. Normalmente basta con las sanciones penales o, en su caso, las reacciones desde el ordenamiento privado. Desde esa óptica, por ejemplo, cuando no se constata en la actuación del particular la finalidad de obtener pruebas para hacerlas valer en un proceso judicial puede eludirse la tajante sanción del art. 11.1 LOPJ en cuanto no está presente la finalidad a que obedece la norma (STS 116/2017, de 23 de febrero). Pero en otros casos, rige el mandato del art. 11.1 LOPJ"[74].

No obstante, se insiste en que la regla de exclusión probatoria sigue rigiendo para aquella información que, aún traída al proceso por particulares, ha sido obtenida con vulneración de derechos fundamentales y con el ánimo evidente de preconstituir prueba. Así lo recuerda la STS (Sala de lo penal) 132/2022, de 24 de enero, cuando establece que "si bien la lesión de un derecho fundamental a consecuencia de una actividad inherente de un particular activa mecanismos reparadores ello no supone que, de forma necesaria, cuando se produzca un efecto reflejo en un proceso judicial resulte siempre de aplicación la regla de exclusión probatoria prevista en el art. 11 LOPJ (…). La regla de exclusión probatoria como manifestación reactiva del sistema de garantías, debe operar, sin duda, con toda la energía, cuando el Estado o los particulares, mediante la infracción del derecho fundamental, acceden a fuentes o medios de prueba y pretenden aprovecharse de su potencial valor incriminatorio (…). El Tribunal constitucional, de manera indirecta –*vid*. a sensu contrario, SSTC 29/84, 56/2003, 97/2019– ha confirmado la operatividad de la regla de exclusión en supuestos en los que los agentes infractores sean particulares, pero siempre que la finalidad fuera la obtención lícita de evidencias o de fuentes probatorias. Por ello, si partimos de la funcionalidad protectora de la regla de exclusión, deberá convenirse en su inaplicación, cuando la lesión del derecho fundamental por particulares aparece desconectada de

74. STS 489/2918, de 23 de octubre.

dicha finalidad –*vid*. TS 116/2017, de 23 de febrero, 546/2019, de 11 de noviembre".

La importancia de la tesis sostenida en la citada sentencia (STS 132/2022, de 24 de enero) reside, además, en que justifica la condena en costas del querellante que fundamentó su acusación en pruebas obtenidas con vulneración de derechos fundamentales y con el fin preciso de hacerlas valer en el proceso. Considera el Tribunal Supremo que la aportación de este tipo de pruebas, obtenidas por la parte con una finalidad exclusivamente incriminatoria y con vulneración, además, de los derechos fundamentales de la otra, denota una mala fe en su actuación procesal que no puede hacerse recaer sobre aquella que ha soportado esa ilegítima actuación. "Adquirirán especial relevancia [sostiene el TS] como marcadores indiciarios de una conducta procesal temeraria o de mala fe, la afirmación de hechos inciertos o falsos dirigidos a confundir al juzgador, la correlativa ocultación de hechos relevantes, la no aportación de medios de prueba de los que se disponga que pudieran favorecer a la persona contra la que se dirige la acción penal y, desde luego, la aportación de medios de prueba que se hayan obtenido vulnerando derechos y garantías constitucionales. (…) Si la infracción del principio de integridad del proceso justifica, nada más y nada menos, la expulsión de evidencias probatorias y el sacrificio de la búsqueda de la verdad parece del todo conforme que su lesión, imputable a la parte que ejerce la acción penal, también se proyecte en la determinación de las consecuencias que pueden derivarse para las personas que han estado sometidas al proceso. Entre estas, la asunción de los costes económicos derivados del mismo. En este sentido, no parece razonable que la persona que ha resultado absuelta de una acusación manifiestamente infundada que, además, pretendía basarse en pruebas obtenidas por la propia parte acusadora con lesiones de sus derechos fundamentales, tenga que soportar los gastos defensivos consecuentes a su indebido sometimiento al proceso. Nuestro modelo procesal reconoce una extraordinaria y amplísima legitimación para el ejercicio de la acción penal por particulares lo que justifica, precisamente, el establecimiento de contrapesos y fórmulas de prevención y sanción del abuso y exceso de su utilización. Entre los que se encuentra la condena en costas, cuando, además, de infundada, la acción presenta rasgos indicativos de instrumentalización abuso"[75].

75. STS (Sala de lo penal) 132/2022, de 24 de enero. Análisis del segundo motivo de casación, apartados 20 y 21.

La aportación, pues, de pruebas obtenidas por un particular con fines exclusivamente incriminatorios y con vulneración, además de los derechos fundamentales de la otra parte, pasará no sólo por la exclusión de dicha prueba del proceso ex art. 11.1 LOPJ, sino por la imposición de las costas procesales cuando la pretensión acusatoria resultara infundada.

Pero, como se ha visto con anterioridad, la exclusión probatoria no es ya el único mecanismo de protección de los derechos fundamentales cuando la actuación vulneradora procede de un particular. Conforme a la última jurisprudencia, la protección de estos derechos es también viable desde la exigencia de responsabilidad al infractor en el ámbito que corresponda[76]. Con claridad lo expresa la STS 132/2022, de 24 de enero, cuando, aun acogiéndose en el caso concreto a la exclusión probatoria manifiesta que "no cabe duda que los derechos fundamentales, y muy en particular los derechos de y a la intimidad reconocidos en el artículo 18 CE, pueden oponerse no solo frente a las injerencias del Estado sino también contra cualquier acto lesivo que provenga de particulares. La indiferencia respecto al agente 'perturbador' resulta coherente con el propio contenido esencial del derecho en juego. Pero el ámbito extendido de protección no significa que las consecuencias y las reparaciones deban ser las mismas con independencia de quién sea el agente infractor. Hay razones sistemáticas y teleológicas que permiten la aplicación de estándares de reparación diferenciados en atención a la condición subjetiva de la injerencia o de la finalidad perseguida con la misma".

Y si enlazamos ahora estas conclusiones finales con el objeto de estudio de este trabajo –el valor probatorio que, en su caso, pueden alcanzar las grabaciones de audio, video u otras pruebas digitales obtenidas por el empresario en el ejercicio de su potestad de control– se observará que dicha validez probatoria requiere de alguna condición previa: que, efectivamente, la información (grabación, en su caso) aportada por el empresario haya sido obtenida o bien "por casualidad" –amparado por la buena fe en su actuación–; o bien, previa información exhaustiva y detallada al trabajador (y su consiguiente aceptación) respecto de los medios, formas y finalidad o destino de dicha información.

76. A título de ejemplo y según se ha visto en este trabajo, así, las SSTS 817/2021, de 21 de junio (Sala 4.ª), o 77/2017, 31 de enero de 2017, hacen compatible la valoración probatoria de la grabación de un trabajador, con la exigencia de responsabilidad ante la Agencia Española de Protección de Datos.

Es por ello que en modo alguno considero justificable –al menos desde la función que tenemos otorgada al proceso penal y la concepción del monopolio estatal en el ejercicio del *ius puniendi*– las situaciones que otorgan al empresario poderes pseudopoliciales de investigación de las potenciales conductas delictivas de sus trabajadores. Esta es la situación que consiente y legitima el TEDH con la Sentencia López Ribalda II al admitir la validez probatoria de las grabaciones de unas cámaras ocultas, puestas por el empresario ante la sospecha de unos incumplimientos graves que conllevaban, además, sospechas de actuación delictiva. Una actuación acorde con el ordenamiento pasaría, en primer lugar, por la denuncia del empresario ante la sospecha de la comisión de un hecho delictivo y, en segundo lugar, por la necesaria autorización judicial para que la policía pudiera instalar unas cámaras de grabación.

Esta tendencia interpretativa sostenida ya, tanto por un mayoritario sector doctrinal cuanto por la última jurisprudencia, parece encontrar amparo, también, a nivel legislativo –o prelegislativo, en puridad–. Así, desde esta perspectiva se ha constatado igualmente la necesidad de regular las diversas excepciones a la nulidad de la prueba obtenida con vulneración de derechos fundamentales, sancionada en el art. 11.1 LOPJ[77].

Como bien conocerá el lector nos encontramos sumidos en una suerte de *día de la marmota* en el que legislatura tras legislatura, los sucesivos gobiernos proclaman –por no decir "prometen"– su voluntad de reformar nuestra ya bicentenaria, vetusta y parcheada Ley de Enjuiciamiento Criminal. De entre los últimos borradores y anteproyectos legislativos es de destacar el esfuerzo sistematizador llevado a cabo por el Anteproyecto de Código Procesal Penal de 2013 al consagrar, tras la genérica prohibición de valorar las pruebas obtenidas con vulneración de derechos fundamentales, las posibles excepciones a esta regla general, con mención expresa de las que resultaran favorables al encausado, las pruebas indirectas que previsiblemente hubieran sido descubiertas

77. Sobre la imperiosa necesidad de abordar legislativamente esta situación, muy ilustrativo resulta el trabajo de DÍEZ-PICAZO "Algunas ideas sobre la prueba ilícitamente obtenida", en el que acota los 12 puntos que –en su opinión– necesariamente el legislador debería plantearse ("si hubiera Ley detallada, nada habría que ponderar, porque ya habría 'ponderado' el legislador" –concluye–). *Vid*. DIÉZ-PICAZO GIMÉNEZ, I., "Algunas ideas sobre la prueba ilícitamente obtenida" en *Derecho probatorio y otros estudios procesales. Liber amicorum Vicente Gimeno Sendra*, (ASENCIO MELLADO, Dir.), Ed. Castillo de Luna, 2020, pp. 586 y ss.

durante el curso de la investigación o las obtenidas por un particular sin ánimo de preconstitución probatoria[78].

Sin embargo, no fue ésta la posición que se consolidó en el siguiente Anteproyecto de Ley de Enjuiciamiento Criminal y que cristalizó en 2020. En él (último texto prelegislativo existente al momento de redactar estas líneas) se da reconocimiento expreso al art. 3 del CEDH al proclamarse que no se admitirán las pruebas que, directa o indirectamente, procedan de actos constitutivos de torturas, tratos inhumanos o degradantes; pero, junto a ello, lo que expresamente se regula son los supuestos en los que no resultará admisible una prueba que vulnera derechos fundamentales. La diferencia con la normativa existente hasta el momento, no es nimia…no se parte ya de la inadmisión de la prueba vulneradora de derechos fundamentales, como regla general; sino de la regulación de los casos en los que se inadmite. Y, se inadmitirá cuando entre el acto de obtención de la prueba y su utilización en el proceso exista una conexión jurídica suficiente. Nótese, además, que se regulan, a continuación, las excepciones a estos supuestos de inadmisión; es decir, que habrá pruebas que aun siendo vulneradoras de derechos fundamentales y aun existiendo conexión jurídica entre su obtención y la utilización en el proceso, se admitirán. Se trata de

78. "Artículo 13. Exclusión de la prueba prohibida

1. No surtirán efecto en el proceso las informaciones o fuentes de prueba obtenidas, directa o indirectamente, con vulneración de derechos fundamentales o las pruebas en cuya práctica se lesionen los mismos. Tales pruebas serán de valoración prohibida.

2. Como excepción a la disposición establecida en el apartado anterior, podrán ser utilizadas y valoradas las pruebas que, sin estar conectadas con un acto de tortura, sean:

a) favorables al encausado; o
b) consecuencia indirecta de la vulneración de un derecho fundamental si, con independencia de la existencia del nexo causal entre la infracción del derecho fundamental y la fuente de prueba, en atención a las concretas circunstancias del caso, se llegue a la certeza de que, conforme al curso ordinario de la investigación, la fuente de prueba hubiera sido descubierta en todo caso; o
c) consecuencia de la vulneración de un derecho fundamental exclusivamente atribuible a un particular que haya actuado sin ánimo de obtener pruebas.

3. La declaración autoincriminatoria del encausado, prestada en el plenario en términos que permitan afirmar su voluntariedad, se entenderá desconectada causalmente de la prueba declarada nula.

4. En cualquier momento en que se constate la existencia de la infracción del derecho fundamental afectado las informaciones o fuentes de prueba o resultados de las pruebas han de ser excluidos del proceso, sin perjuicio de que, rechazada la exclusión, las partes puedan reproducir con posterioridad la petición de declaración de nulidad de la prueba".

los supuestos en los que las partes acusadoras puedan demostrar que habrían llegado a obtener dichas pruebas por otro medio lícito y distinto del utilizado[79]. Ese es, pues, el último destino que el prelegislador ha pensado para la prueba ilícitamente obtenida[80].

Si, como con acierto se ha hecho ver, la historia de la prueba prohibida es la historia de sus excepciones[81], caminamos hacia un futuro en el que la prueba prohibida quiere pasar a ser la excepción.

V. BIBLIOGRAFÍA

ARMENTA DEU, T., "Prueba ilícita y regla de exclusión: perspectiva subjetiva", en *Derecho probatorio y otros estudios procesales Liber amicorum Vicente Gimeno Sendra* (ASENCIO MELLADO, Dir.), Ed. Castillo de luna, 2020.

ARMENTA DEU, T., *La Prueba Ilícita. Un estudio comparado*, Ed. Marcial Pons, 2011.

ARRABAL PLATERO, P., *La Prueba Tecnológica: aportación, práctica y valoración*, Tirant Lo Blanch, Valencia, 2020.

79. Anteproyecto de Ley de Enjuiciamiento Criminal de 2021. Versión para información pública. Accesible en https://www.mjusticia.gob.es/es/AreaTematica/ActividadLegislativa/Documents/210126%20ANTEPROYECTO%20LECRIM%202020%20INFORMACION%20PUBLICA%20(1).pdf.
"Artículo 21. Exclusión de la prueba ilícita.
1. No surtirán efecto las pruebas obtenidas con violación de derechos fundamentales cuando entre el acto de obtención de la prueba y su utilización en el proceso exista una conexión jurídica suficiente.
Se entenderá que dicha conexión existe cuando la violación consumada comprometa, por su índole y características, la equidad e integridad del proceso, cuando por su intensidad suponga un atentado grave contra el derecho fundamental vulnerado o cuando la admisión de la prueba pueda poner en peligro la eficacia general de dicho derecho, favoreciendo violaciones ulteriores.
Serán, no obstante, admitidas dichas pruebas cuando las partes acusadoras puedan demostrar que habrían llegado a obtenerlas por un medio distinto y lícito.
2. En ningún caso se admitirán las pruebas que, directa o indirectamente, procedan de actos constitutivos de torturas, tratos inhumanos o degradantes".

80. Sobre el tema, *in extenso*, GOMEZ AMIGO, L., "Tratamiento procesal de la prueba ilícita en el proceso penal: del régimen actual al Anteproyecto de LECRIM de 2020" en *Reflexiones en torno al Anteproyecto de Ley de Enjuiciamiento Criminal de 2020* (JIMÉNEZ CONDE y FUENTES SORIANO, Dirs.), Tirant lo Blanch, Valencia, 2022, pp. 980 y ss.

81. DIEZ– PICAZO GIMÉNEZ, I., "Algunas ideas sobre la prueba…", cit. p. 583.

ARRABAL PLATERO, P., "El Derecho fundamental al propio entorno virtual y su incidencia en el proceso", en *Era digital, Sociedad y Derecho* (FUENTES SORIANO Dir.), Tirant lo Blanch, Valencia, 2020.

ASENCIO MELLADO, JM., "Los derechos fundamentales en el proceso penal", *Derecho procesal penal*, (ASENCIO MELLADO, Dir. y FUENTES SORIANO, Coord.), Tirant lo Blanch, Valencia, 2020.

ASENCIO MELLADO, J.M., "La STC 97/2019, de 16 de julio. Descanse en paz la prueba ilícita", Diario La Ley, Núm. 9499, Sección Tribuna, 16 de octubre de 2019.

CUADRADO SALINAS, C., *Fundamento y efectos de la exclusión de la prueba obtenida con vulneración de derechos fundamentales,* Tirant lo Blanch, Valencia, 2021.

DEL MORAL GARCÍA, A., "Prueba ilícita, entorno digital y derechos fundamentales: divergencias entre la jurisprudencia social y la penal", en *Era digital Sociedad y Derecho* (FUENTES SORIANO, Dir.), Tirant lo Blanch, 2020.

DÍEZ-PICAZO GIMÉNEZ, I., "Algunas ideas sobre la prueba ilícitamente obtenida" en *Derecho probatorio y otros estudios procesales. Liber amicorum Vicente Gimeno Sendra*, (ASENCIO MELLADO, Dir.), Ed. Castillo de Luna, 2020.

DURÁN SILVA, C., "Análisis de la licitud de la imagen atendiendo al sujeto que la capta", en *Era Digital Sociedad y Derecho*, (FUENTES SORIANO, Dir.), Tirant lo Blanch, Valencia, 2020.

FERNÁNDEZ ORRICO, J., *Criterios sobre uso de dispositivos tecnológicos en el ámbito laboral. Hacia el equilibrio entre el control empresarial y la privacidad del trabajador*, Tirant lo Blanch, Valencia, 2021.

FERNÁNDEZ ORRICO, J., "Desconexión digital en el ámbito laboral: un derecho emergente de los trabajadores", en *Era Digital Sociedad y Derecho*, (FUENTES SORIANO, Dir.), Tirant lo Blanch, Valencia, 2020.

FUENTES SORIANO, O., "La prueba prohibida aportada por particulares, a la luz de las nuevas tecnologías", en *Derecho Probatorio y otros estudios procesales. Liber Amicorum Vicente Gimeno Sendra*, (ASENCIO MELLADO, Dir.), Ed. Castillo de Luna, Madrid, 2020.

FUENTES SORIANO, O., "La prueba prohibida. Viejos problemas procesales de las nuevas tecnologías", en *Justicia y proceso en el S.*

XXI. Desafíos y tareas pendientes, PRIORI POSADA. G. (Coord.), Ed. Palestra, Perú, 2019.

FUENTES SORIANO, O., "Videos, comunicación electrónica y redes sociales. Cuestiones probatorias", Práctica de Tribunales núm. 135, noviembre-diciembre: La prueba pericial en el proceso civil: proposición y valoración, Núm. 135, 1 de noviembre, 2018.

GOMEZ AMIGO, L., "Tratamiento procesal de la prueba ilícita en el proceso penal: del régimen actual al Anteproyecto de LECRIM de 2020" en *Reflexiones en torno al Anteproyecto de Ley de Enjuiciamiento Criminal de 2020* (JIMÉNEZ CONDE y FUENTES SORIANO, Dirs.), Tirant lo Blanch, Valencia, 2022.

MAGRO SERVET, V., "Sobre el valor probatorio de las cámaras de vigilancia en el proceso penal", Diario La Ley, Núm. 9114, Sección Doctrina, 9 de enero de 2018.

MARCHENA GÓMEZ. M, "Prueba ilícita y reglas de exclusión: los matices introducidos por la Sala Penal del Tribunal Supremo en la Sentencia 116/2007, 23 de febrero (Caso Falciani)", en *Derecho Probatorio y otros estudios procesales. Liber Amicorum Vicente Gimeno Sendra*, (ASENCIO MELLADO, Dir.), Ed. Castillo de Luna, Madrid, 2020.

SÁNCHEZ QUIÑONES, L., "La rectificación del TEDH en la doctrina López Ribalda", disponible en http://www.legaltoday.com/practica-juridica/publico/proteccion_de_datos/la-rectificacion-del-tedh-en-la-doctrina-lopez-ribalda, fecha última consulta: 20 de mayo de 2020.

SEMPERE NAVARRO, A., "Un apunte sobre la grabación mediante cámaras (Al hilo de la STS-CIV 600/2019 de 7 noviembre)", Revista Aranzadi Doctrinal, ISSN 1889-4380, Núm. 2, 2020.

VEGAS TORRES, J., "Sobre la ilicitud de las pruebas obtenidas por las empresas mediante el control de las comunicaciones electrónicas de los trabajadores", en *Derecho Probatorio y otros estudios procesales. Liber amicorum Vicente Gimeno Sendra* (ASENCIO MELLADO, Dir.), Castillo de Luna, 2020.

VELASCO NÚÑEZ, E., "Prueba penal prohibida obtenida por particular. Autograbaciones, grabaciones subrepticias y filtraciones de privacidades ajenas en chats y foros" en Revista Aranzadi de Derecho y Proceso Penal, 2019 Núm. 53 (Enero-marzo).