ISSN: 1696-3083, Revista Galega de Dereito Social -2ª ET- (13,2021), pp. 9-30
http://www.revistagalegadedereitosocial.gal

LA PRUEBA EN EL PROCESO LABORAL: ALGUNOS PUNTOS CRÍTICOS RECIENTES ∗

IGNACIO GARCÍA-PERROTE ESCARTÍN
Magistrado de la Sala de lo Social del Tribunal Supremo
Catedrático de Derecho del Trabajo de la UNED (s.e.)

RESUMEN
El editorial aborda algunas importantes cuestiones críticas sobre la prueba en el proceso laboral, examinando la jurisprudencia sobre la materia, especialmente la más reciente. Se analiza, así, la naturaleza de prueba documental del correo electrónico; la repercusión de la prueba ilícita sobre la calificación del despido; el control empresarial sobre los dispositivos digitales de los trabajadores; la videovigilancia; y la geolocalización.
Palabras clave: correo electrónico, prueba ilícita, despido, dispositivos digitales, videovigilancia, geolocalización.

ABSTRACT
The editorial analyses some key topics in connection with evidence produced during labour proceedings, reviewing the applicable case law and, in particular, focusing on the most recent resolutions on these matters. Among others, the editorial deals with the nature of emails as documents in the proceeding; the effects of an unlawfully obtained evidence on the qualification of a dismissal; the companies' control of the IT devices provided to their employees; vídeo surveillance in the workplace; and geolocalization in the context of employment relationships.

∗Este editorial se publicará también en el *Liber Amicorum* en memoria de Aurelio Desdentado Bonete que están preparando Jesús R. Mercader Uguina y Ana de la Puebla Pinilla.

Recibido: 26/11/2021; Aceptado: 20/12/2021

Keywords: email, unlawful evidence, dismissal, IT devices, vídeo surveillance, geolocalization.

RESUMO
O editorial aborda algunhas importantes cuestións críticas sobre a proba no proceso laboral, examinando a xurisprudencia sobre a materia, especialmente a máis recente. Analízase, así, a natureza de proba documental do correo electrónico; a repercusión da proba ilícita sobre a cualificación do despedimento; o control empresarial sobre os dispositivos dixitais dos traballadores; a videovixiancia; e a xeolocalización.
Palabras chave: correo electrónico, proba ilícita, despedimento, dispositivos dixitais, videovixilancia, xeolocalización.

SUMARIO

1. FUENTES DE PRUEBA Y MEDIOS DE PRUEBA

Partiendo de la diferenciación entre fuentes de prueba y medios de prueba, podría decirse que las primeras -las fuentes- son *numerus apertus*, mientras que los segundos -los medios-, serían, más bien, *numerus clausus.*

Como se sabe y se recordará más adelante, los apartados 1 y 2 del artículo 299 de la Ley de Enjuiciamiento Civil (LEC) establecen los medios de prueba. Lo mismo hacen los artículos 90.1 (en su segundo inciso, al que igualmente se hará referencia enseguida) y 91 y 95 de la Ley reguladora de la jurisdicción social (LRJS).

Pero el artículo 299.3 LEC dispone que "*cuando por cualquier otro medio no expresamente previsto en los apartados anteriores de este artículo pudiera obtenerse certeza sobre hechos relevantes, el tribunal, a instancia de parte, lo admitirá como prueba, adoptando las medidas que en cada caso resulten necesarias*."

Parece, pues, que se admiten otros medios de prueba, además de los enunciados en los apartados 1 y 2 del artículo 299 LEC. Sin embargo, el artículo 90.1 LRJS prevé que "*las partes, previa justificación de la utilidad y pertinencia de las diligencias propuestas, podrán servirse de cuantos medios de prueba se encuentren regulados en la Ley para acreditar los hechos controvertidos o necesitados de prueba*". Se parte, así, de que los medios de prueba son únicamente los que están «*regulados en la Ley.*»

2. MEDIOS DE PRUEBA

Sea como fuere, los ya mencionados apartados 1 y 2 del artículo 299 LEC enuncian los medios de prueba de que se podrá hacer uso en juicio.

El tenor literal de estos dos apartados del artículo 299 LEC es el siguiente:

"*1. Los medios de prueba de que se podrá hacer uso en juicio son:*

1.º Interrogatorio de las partes.

2.º Documentos públicos.

3.º Documentos privados.

4.º Dictamen de peritos.

5.º Reconocimiento judicial.

6.º Interrogatorio de testigos.

2. También se admitirán, conforme a lo dispuesto en esta Ley, los medios de reproducción de la palabra, el sonido y la imagen, así como los instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, relevantes para el proceso."

A destacar la referencia que el artículo 299.2 LEC hace a los:

- "*medios de reproducción de la palabra, el sonido y la imagen.*"

Y a los:

- "*instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase.*"

Por su parte, y en sentido coincidente, el artículo 90.1 LRJS menciona a los:

- "*procedimientos de reproducción de la palabra, de la imagen y del sonido.*"

Y al:

- "*archivo y reproducción de datos*."

Precisando el artículo 90.1 LRJS que estos medios de prueba "*deberán ser aportados por medio de soporte adecuado y poniendo a disposición del órgano jurisdiccional los medios necesarios para su reproducción y posterior constancia en autos*", previsión esta última que seguramente no sea ya tan necesaria al disponer generalmente los juzgados de lo social de estos medios.

3. NATURALEZA DE LOS MEDIOS DE PRUEBA DEL ARTÍCULO 299.2 LEC Y DEL ARTÍCULO 90.1 LRJS: ALGUNOS PRECEDENTES

Mayor importancia práctica tiene determinar si los medios e instrumentos a que hacen referencia el artículo 299.2 LEC y el artículo 90.1 LRJS son medios autónomos de prueba o, por el contrario, se pueden insertar en el concepto, si se quiere amplio, de documento. Como se sabe bien, solo si se acepta lo segundo, tales medios e instrumentos podrán fundar la revisión de hechos probados en suplicación y casación [artículos 193 b) y 207 d) LRJS].

Con anterioridad a la LEC del año 2000, cabe citar, en primer lugar, la STS 17 junio 1996 (rec. revisión 1611/1995), en la

que se examina sobre la posible autonomía que podría tener la fotografía incluida en un informe de detective, respecto de este informe, que no deja de ser una prueba testifical. El ponente de esta sentencia fue Aurelio Desdentado Bonete, a quien tanto se echa de menos, y en ella se decía pioneramente lo siguiente:

"*La doctrina no es pacífica sobre el tratamiento que, como medio de prueba, hay que atribuir a estas formas de reproducción de la imagen: para quienes sostienen que, en la noción de documento, lo fundamental es la existencia de un objeto que incorpora una representación con posible valor probatorio y que puede ser trasladado a presencia judicial e incorporado a las actuaciones, las fotografías serían un documento. Pero para la tesis que considera que la noción de documento debe limitarse a las declaraciones de voluntad manifestadas por escrito, estaríamos ante una forma especial de reconocimiento judicial, en la que la imagen del objeto que el juez examina se independiza de ese objeto y puede ser presentada en el acto de juicio, aunque lo representado, en cuanto acción pasada, haya desaparecido.*"

En segundo lugar, la STS (1ª) 523/1999, 12 junio 1999 (rec. 2930/1994), entendió que unas cintas magnetofónicas aportadas debían someterse al régimen establecido para los documentos.

Con posterioridad a la LEC, y con fundamento en la diferencia entre los apartados 1 y 2 del artículo 299 LEC, las SSTS 16 junio 2011 (rec. 3983/2010), 26 de noviembre de 2012 (rec. 786/2012) y 31/2020, 15 enero 2020 (rec. 166/2018, FD quinto, 3) se inclinaron por atribuir naturaleza autónoma -distinta de la prueba documental-, a los medios de reproducción de la palabra, el sonido y la imagen, así como a los instrumentos de archivo y reproducción de datos.

Sin embargo, las SSTS 12 febrero 2013 (rec. 254/2011) y 29 enero 2019 (rec. 12/2018) no cuestionaron la idoneidad de unos correos electrónicos para sustentar una pretensión revisora casacional, aunque finalmente desestimaron la solicitud.

4. LA IMPORTANCIA DE LA STS 706/2020, 23 JULIO 2020 (PLENO, REC. 239/2018): LA NATURALEZA DE PRUEBA DOCUMENTAL DEL CORREO ELECTRÓNICO

La importante STS 706/2020, 23 julio 2020 (rec. 239/2018), dictada por el Pleno, llega en su fundamento de derecho cuarto a la conclusión de que el correo electrónico tiene naturaleza de prueba documental.

Se sintetizan a continuación los principales razonamientos de esta sentencia:

1) El concepto amplio de prueba documental que maneja la LEC, por ejemplo, en sus artículos 326.3, 327, 333 y 812.1. 1º.

2) El artículo 299.2 LEC se limita a establecer las peculiaridades de estas fuentes de prueba (los medios de reproducción de la palabra, el sonido y la imagen y los instrumentos de archivo y reproducción de datos) porque, a diferencia de los documentos escritos, no basta con dar traslado de estas pruebas a la parte contraria, sino que normalmente es preciso proceder al visionado del vídeo, a la escucha del audio o al examen del instrumento de archivo.

3) El concepto amplio de documento, comprensivo de los electrónicos, es el que impera en el resto del ordenamiento jurídico: artículo 26 CP; art. 230 LOPJ; artículo 24.2 de la Ley 34/2002 de Servicios de la Sociedad de la Información y de Comercio Electrónico; artículo 3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica; artículo 17 bis de la Ley del Notariado de 28 de mayo de 1862; artículo 49.1 de la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español; artículo 76.3 *in fine* del Real Decreto 828/1995, de 29 de mayo, por el que se aprueba el Reglamento del Impuesto sobre Transmisiones Patrimoniales y Actos Jurídicos Documentados; artículo 41.1 del Real Decreto 1671/2009, de 6 de noviembre; y artículo 3 del Real Decreto 263/1996, de 16 de febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado.

4) El avance tecnológico ha hecho que muchos documentos se materialicen y presenten a juicio a través de los nuevos soportes electrónicos, lo que no debe excluir su naturaleza de

prueba documental, con las necesarias adaptaciones (por ejemplo, respecto de la prueba de autenticación).
5) Si no se postula un concepto amplio de prueba documental, llegará un momento en que la revisión fáctica casacional quedará vaciada de contenido si se limita a los documentos escritos, cuyo uso será exiguo.
6) En consecuencia, debemos atribuir la naturaleza de prueba documental a los correos electrónicos (obrantes en las actuaciones).
7) Ello no supone que todo correo electrónico acredite el error fáctico de instancia, al igual que sucede con los documentos privados.
8) Para ello será necesario valorar si se ha impugnado su autenticidad por la parte a quien perjudique; si ha sido autenticado, en su caso; y si goza de literosuficiencia.
De la STS 706/2020 se deriva la importancia que para el correo electrónico pueden tener pruebas, como la pericial y testifical, si se cuestiona su autenticidad, así como la reproducción a presencia judicial de los medios de reproducción de la palabra, de la imagen y del sonido y de los instrumentos de archivo y reproducción de datos (artículo 90.1 LRJS y artículo 299.2 LEC).

5. PRUEBA DE INFORME DE DETECTIVE: ES TESTIFICAL DOCUMENTADA

Como ya se ha anticipado, la prueba de informe de detective tiene naturaleza de prueba testifical documentada, si bien, como vislumbró Aurelio Desdentado en la STS 17 junio de 1996 (rec. revisión 1611/1995), cabría dar autonomía a las fotografías o vídeos que el informe pudiera contener y atribuirles, en caso, la naturaleza de prueba documental.
De conformidad con el artículo 265.1.5º LEC:
"*1. A toda demanda o contestación habrán de acompañarse:*
…
5.º Los informes, elaborados por profesionales de la investigación privada legalmente habilitados, sobre hechos relevantes en que aquéllas apoyen sus pretensiones. Sobre estos hechos, si no fueren reconocidos como ciertos, se practicará prueba testifical".

Un supuesto, relativamente reciente, de informe de detective es el examinado por la STS 155/2020, 19 febrero 2020 (rcud. 3943/2017).

En el caso, se declaró la procedencia del despido con base en un informe de detective, en el que es el detective quien fuerza una entrevista de trabajo con un abogado durante su jornada de trabajo. La sentencia de suplicación admite dicha prueba contra el criterio del juzgado, quien la consideró prueba ilícita sin efecto probatorio, y modificó un hecho probado con base al informe escrito del detective, que considera prueba documental.

La STS 155/2020 concluyó que la admisión de la prueba no fue ajustada a derecho, al tratarse de una prueba ilícita.

Pero lo que interesa aquí subrayar es que la STS 155/2020 estableció que no cabe modificar hechos probados con informes escritos de detectives, que no tienen la condición de pruebas documentales sino de prueba testifical.

Como se ha anticipado, ya la citada STS 17 junio 1996 (rec. revisión 1611/1995), de la que fue ponente Aurelio Desdentado, advertía que la posible naturaleza documental podría atribuirse, en su caso, a las fotografías, pero no al informe del detective "*que es sólo la expresión escrita de la declaración del testigo, es decir, un testimonio documentado sin más valor que el testifical según reiterada y conocida doctrina*".

6. CARGA DE LA PRUEBA

Los apartados 1 a 3 y 5 a 7 del artículo 217 LEC, sobre "*carga de la prueba*", tienen el siguiente tenor literal:

"*1. Cuando, al tiempo de dictar sentencia o resolución semejante, el tribunal considerase dudosos unos hechos relevantes para la decisión, desestimará las pretensiones del actor o del reconviniente, o las del demandado o reconvenido, según corresponda a unos u otros la carga de probar los hechos que permanezcan inciertos y fundamenten las pretensiones.*

2. Corresponde al actor y al demandado reconviniente la carga de probar la certeza de los hechos de los que ordinariamente se desprenda, según las normas jurídicas a

ellos aplicables, el efecto jurídico correspondiente a las pretensiones de la demanda y de la reconvención.
3. Incumbe al demandado y al actor reconvenido la carga de probar los hechos que, conforme a las normas que les sean aplicables, impidan, extingan o enerven la eficacia jurídica de los hechos a que se refiere el apartado anterior.
4. …
5. De acuerdo con las leyes procesales, en aquellos procedimientos en los que las alegaciones de la parte actora se fundamenten en actuaciones discriminatorias por razón del sexo, corresponderá al demandado probar la ausencia de discriminación en las medidas adoptadas y de su proporcionalidad.
A los efectos de lo dispuesto en el párrafo anterior, el órgano judicial, a instancia de parte, podrá recabar, si lo estimase útil y pertinente, informe o dictamen de los organismos públicos competentes.
6. Las normas contenidas en los apartados precedentes se aplicarán siempre que una disposición legal expresa no distribuya con criterios especiales la carga de probar los hechos relevantes.
7. Para la aplicación de lo dispuesto en los apartados anteriores de este artículo el tribunal deberá tener presente la disponibilidad y facilidad probatoria que corresponde a cada una de las partes del litigio."

Un ejemplo reciente de la aplicación del criterio de la disponibilidad y facilidad probatoria del apartado 7 del artículo 217 LEC puede encontrarse en la STS 1114/2020, 11 diciembre 2020 (rcud. 1482/2018). De interés es, asimismo, rechazando su aplicación, la STS 874/2021, 8 septiembre 2021 (rcud. 1866/2020).

Por su parte, las SSTS 874, 875 y 876/2021, 8 septiembre 2021 (rcuds. 1866/2020, 2543/2020 y 2554/2020, respectivamente) y 876/2021, 9 septiembre 2021 (rcud. 2143/2019) establecen que la carga de la prueba de la transmisión de una unidad productiva, en tanto que constitutiva para la estimación de la demanda y de conformidad con el artículo 217.2 LEC, le corresponde a la parte demandante.

7. PRUEBA LESIVA DE DERECHOS FUNDAMENTALES: LA NOVEDAD DE LA STC 61/2021, 15 MARZO

Como es bien sabido, y de conformidad con los artículos 11.1 de la Ley Orgánica del Poder Judicial, 287.1 LEC y 90.2 LRJS, y por citar este último precepto, no se admitirán pruebas que tuvieran su origen o que se hubieran obtenido, directa o indirectamente, mediante procedimientos que suponga violación de derechos fundamentales o libertades públicas.

Es justo mencionar la importancia que tuvo la doctrina sentada en la STC 114/1984, 29 noviembre, y que se llevó a los preceptos mencionados.

Aunque tiene su origen en un procedimiento penal, es útil la sistematización que hace la STC 97/2019, 16 de julio, sobre los "*principios generales de la doctrina constitucional sobre la prueba ilícita" (FJ 2) y los "elementos del juicio de ponderación. Evolución de la doctrina constitucional" (FJ 3).*

Pero, desde la perspectiva jurídico laboral, una relevante novedad se halla en la STC 61/2021, 15 marzo, sobre la repercusión que tiene una prueba ilícita (monitorización del ordenador de una trabajadora que vulneró su derecho a la intimidad y al secreto de las comunicaciones, proclamados en los artículos 18.1 y 18.3 de la Constitución; CE) sobre la calificación del despido.

En apretada síntesis, la doctrina de la STC 61/2021, 15 marzo, puede expresarse así:

-Desde la perspectiva del artículo 24.1 CE, la STC 61/2021 acepta como interpretación fundada en Derecho y no arbitraria de la legalidad ordinaria la realizada por la Sala de lo Social del Tribunal Superior de Justicia de Madrid, que calificó el despido como improcedente y no como nulo, aunque el Tribunal Constitucional (TC) señala que no es la única interpretación posible, siempre desde la perspectiva de la interpretación de la legalidad ordinaria, que no le corresponde realizar al TC.

-Previamente, la STC 61/2021 rechaza que de los artículos 18.1 y 18.3 CE emane de forma inexorable que la calificación del despido en estos casos haya de ser la nulidad.

8. LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES Y GARANTÍA DE LOS DERECHOS

DIGITALES (LOPDGDD) Y LA JURISPRUDENCIA PREVIA DEL TRIBUNAL EUROPEO DE DERECHOS HUMANOS (TEDH), TC Y TRIBUNAL SUPREMO (TS)

Termina este rápido repaso sobre algunos puntos críticos recientes de la prueba en el proceso laboral con la breve exposición de los controles empresariales que permite la LOPDGDD y de la reveladora jurisprudencia previa del TEDH, TC y TS.

8.1. DISPOSITIVOS DIGITALES DE LOS TRABAJADORES Y CONTROL EMPRESARIAL (ARTÍCULO 87 LOPDGDD)

De conformidad con el artículo 87 LOPDGDD, "*los trabajadores ... tendrán derecho a la protección de su intimidad en el uso de los dispositivos digitales puestos a su disposición por su empleador*". El empleador podrá acceder a los contenidos derivados del uso de medios digitales facilitados a los trabajadores "*a los solos efectos de controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la integridad de dichos dispositivos"*. Los empleadores deberán establecer "criterios de utilización" de los dispositivos digitales respetando en todo caso los estándares mínimos de protección de su intimidad de acuerdo con los usos sociales y los derechos reconocidos constitucional y legalmente. En su elaboración deberán participar los representantes de los trabajadores. El acceso por el empleador al contenido de dispositivos digitales respecto de los que haya admitido su uso con fines privados requerirá que se especifiquen de modo preciso los usos autorizados y se establezcan garantías para preservar la intimidad de los trabajadores, tales como, en su caso, la determinación de los períodos en que los dispositivos podrán utilizarse para fines privados. Los trabajadores deberán ser informados de los criterios de utilización a los que se ha hecho referencia.

Conviene precisar, no obstante, de acuerdo con la jurisprudencia a la que a continuación se hará referencia, que, aunque el artículo 87.3, párrafo último, LOPDGDD no lo explicita, la obligación empresarial de información no es solo de los criterios de utilización de los dispositivos digitales, sino que se extiende a que se tenga que informar adicionalmente

de que la empresa controlará ("monitorizará") que los trabajadores cumplen con aquellos criterios de utilización, incluso en los supuestos de prohibición de uso para fines privados.

Puede ser de interés recordar la importante jurisprudencia del TEDH, del TC y del TS recaída con anterioridad a la LOPDGDD. La ausencia de regulación legal, entre nosotros, de los derechos digitales ha hecho que la jurisprudencia tuviera el protagonismo cuasi exclusivo en la configuración de esos derechos.

Lo primero que hay que recordar es que, con anterioridad a la LOPDGDD, ya la jurisprudencia exigía de las empresas que tuvieran una política clara sobre el uso de los medios informáticos y del control del respeto a dicha política y que dicha política hubiera sido comunicada a los empleados. Se trata, principalmente, de las SSTS 26 septiembre 2007 (rcud. 966/2006), 8 marzo 2011 (rcud. 1826/2010), 6 octubre 2011 (Sala General, rcud. 4053/2010, con voto particular) y 119/2018, 8 febrero (rcud. 1121/2015). La verdad es que la STS 26 septiembre 2007, de la que fue ponente Aurelio Desdentado, es -y sigue siendo- una sentencia clave que sentó una doctrina que no solo continúa plenamente vigente, sino que es la que sustancialmente se ha llevado a los textos legales.

La manera de «*romper*» o modular la «*expectativa de privacidad*», a la que hace referencia, por ejemplo, la todavía importante STEDH, 3 de abril de 2007 (Copland), es precisamente la existencia de esa clara y comunicada política que puede incluir la prohibición del uso privado de los dispositivos o permitir un uso moderado y que, como se ha advertido, ha de advertir que la empresa fiscalizará que se cumple la política establecida. El criterio de que la prohibición de uso privado lleva implícita la facultad de control empresarial ha de entenderse matizada por la STEDH, 5 de septiembre de 2017 (Barbulescu II).

Como es sabido, la jurisprudencia constitucional sentó desde el primer momento el criterio de que los trabajadores pueden ejercer sus derechos fundamentales en la empresa, si bien con las modulaciones o atemperaciones que sean

imprescindibles o indispensables (principio de proporcionalidad) para preservar los derechos empresariales. La jurisprudencia consideró que el artículo 20.3 ET, en conexión con los artículos 33 y 38 CE, ampara el control empresarial en el que están en juego los derechos de los trabajadores reconocidos en los apartados 1, 2, 3 y 4 del artículo 18 CE.

Esta doctrina se fue construyendo en las SSTC 241/2012, 17 diciembre, y 170/2013, 7 octubre, STEDH 5 de septiembre de 2017 (Barbulescu II) y en las ya citadas SSTS, si bien conviene reiterar la cita de la STS 119/2018, 8 febrero, porque ya tiene en cuenta la STEDH Barbulescu II.

La STC 241/2012, 17 diciembre (con voto particular), enjuició un supuesto en el que existía una prohibición para uso privado, por lo que el TC aprecia que no había expectativa alguna de privacidad. Las demandantes de amparo instalaron un programa, en el que hacían comentarios despectivos de empleados y superiores, en un ordenador que era accesible a cualquiera, por lo que declara el TC que no podía estar en juego el secreto de las comunicaciones. A las trabajadoras se les impuso una sanción muy liviana.

Por su parte, la STC 170/2013, 7 octubre, declaró que el acceso del empleador a determinados correos electrónicos del trabajador, que revelaban que transmitía indebidamente información reservada empresarial, no vulneró los derechos a la intimidad y al secreto de las comunicaciones del trabajador (artículo 18.1 y 3 CE). Para la STC 170/2013, el trabajador no podía tener una razonable expectativa de confidencialidad ni de privacidad (el convenio colectivo prohibía el uso privado) y el control empresarial respetó la proporcionalidad constitucionalmente exigida. En efecto, para el TC el control empresarial fue justificado, puesto que existían sospechas de un comportamiento irregular del trabajador; la medida era idónea para la finalidad pretendida por la empresa (si el trabajador revelaba a terceros datos empresariales de reserva obligada); y, en fin, la medida era necesaria, dado que el contenido o texto de los correos electrónicos serviría de prueba de la citada irregularidad ante la eventual impugnación judicial de la sanción empresarial, sin que fuera suficiente el mero acceso a otros elementos de

la comunicación como la identificación del remitente o destinatario, que por sí solos no permitían acreditar el ilícito indicado. Finalmente –concluye el TC–, la medida podía entenderse como ponderada y equilibrada; al margen de las garantías con que se realizó el control empresarial a través de la intervención de perito informático y notario, el TC parte de que la controversia a dirimir se ceñía a los correos electrónicos aportados por la empresa como prueba en el proceso de despido.

La importante STEDH, Gran Sala, 5 de septiembre de 2017 (Barbulescu II), que revoca la previa STEDH 12 de enero de 2016 (Barbulescu I) –citada por la STC 39/2016, de 3 marzo, y que coincidía con la doctrina de las SSTC 241/2012 y 170/2013– concluye que a los tribunales rumanos les faltó determinar, en particular, si el Sr. Barbulescu había sido previamente advertido por su empleador de las posibilidades de que sus comunicaciones en Yahoo Messenger podrían ser monitorizadas (lo que debe hacerse antes de que se inicien las actividades de control) y, de otro lado, que no había sido informado de la naturaleza y extensión del control o del grado de intrusión en su vida privada y correspondencia. Adicionalmente, la STEDH, 5 de septiembre de 2017, entendió que los tribunales rumanos fallaron a la hora de determinar, en primer lugar, las concretas razones que justificaban la introducción de las medidas de control; y, en segundo lugar, si el empleador podía haber usado medidas menos intrusivas. La STEDH, 5 de septiembre de 2017, hace un acopio de la regulación supranacional, internacional y comparada, de las obligaciones positivas que emanan para los Estados del artículo 8 del CEDH y, aunque reconoce, de un lado, que "*el empleador tiene un legítimo interés en asegurar el buen funcionamiento de la empresa y que ello puede hacerse estableciendo mecanismos para verificar que los empleados realizan sus tareas profesionales adecuada y diligentemente y, de otro, que los tribunales rumanos identificaron correctamente los intereses en presencia y los principios legales aplicables (necesidad, finalidad, transparencia, legitimidad, proporcionalidad y seguridad)*", reprocha a los tribunales rumanos lo que se ha dicho. El TEDH

rechaza las indemnizaciones por daños materiales y morales pedidas por el Sr. Barbulescu.

Posteriormente, la STEDH, 22 de febrero de 2018, (Libert c. Francia) (nº 588/13) consideró que no hubo ninguna violación de la vida privada de un empleado de los ferrocarriles franceses (SNCF, empresa pública, frente a lo que ocurría en el caso Barbulescu, lo que puede ser relevante desde la óptica de las obligaciones negativas y positivas de los Estados) que fue despedido de la empresa después de que la consulta de su ordenador profesional revelara el almacenamiento de archivos pornográficos y falsos certificados llevados a cabo en beneficio de terceros. El recurrente se quejaba de que su empleador había abierto sin su presencia ficheros del disco duro de su ordenador, lo que sería una vulneración del artículo 8 del CEDH. Los órganos judiciales franceses consideraron procedente su despido, razonando que, salvo que los identifique expresamente como personales (opción privado en *outlook*) (en este caso, se requiere en derecho francés la presencia del empleado), cabe presumir que los correos son profesionales. Y, si lo son, el empresario puede verlos; este es el derecho francés. El TEDH concedió mucha importancia al hecho de que el demandante no había identificado ese fichero como privado o personal en *outlook*.

En el caso, se establecía el uso estrictamente profesional, si bien se toleraba una utilización privada puntual; el recurrente contrarió «*masivamente*» estas instrucciones y no puede pretender –se dice con amparo en alguna sentencia francesa– que todo el disco duro es personal. El control estaba previsto por la ley (se afirma), y el TEDH examina la finalidad legítima (protección de los derechos de otro o de los demás; en este caso los del empleador; se remite a Barbulescu, 127: interés legítimo del empresario en asegurar el buen funcionamiento de la empresa lo que le permite controlar a sus empleados) y la necesidad en una sociedad democrática (imperiosa y proporcionada). Al demandante, por sus funciones (encargado de la supervisión general), le es exigible un comportamiento ejemplar. El TEDH concluye que las autoridades internas no excedieron el margen de apreciación que les corresponde.

Es imprescindible mencionar, finalmente, la STS 119/2018, 8 de febrero, en la que el TS tiene ya en cuenta la STEDH, 5 de septiembre de 2017 (Barbulescu II). En un supuesto de despido (declarado procedente por el TSJ) en el que la empresa utilizó como prueba (aunque no única) determinados correos electrónicos del trabajador (que revelaban que había recibido dinero de un proveedor), el TS, corrigiendo en este extremo al TSJ, declara que el acceso a esos correos no vulneró ningún derecho fundamental del empleado reconocido en el artículo 18 de la CE. El TS tiene especialmente en consideración el hecho de que la empresa disponía de una política de utilización de medios informáticos en la que se limitaba el uso de tales medios, incluido especialmente el correo electrónico, para fines exclusivamente profesionales. Asimismo, las normas internas informaban con total claridad de la posibilidad de que la empresa supervisara o monitorizara la utilización de tales medios por los empleados. El trabajador conocía estas normas y las aceptaba diariamente al acceder al ordenador que tenía asignado.

Adicionalmente, la revisión del correo electrónico no se llevó a efecto de modo genérico o indiscriminado, sino tratando de encontrar elementos que permitieran seleccionar los correos a examinar, utilizando para ello palabras clave que permitieran inferir en qué correos podría existir información relevante para la investigación. De esta forma, el examen se limitó a los correos pertinentes para la investigación, disponibles en el correo corporativo del empleado, mediante el acceso al servidor alojado en las propias instalaciones de la empresa. Como consecuencia de todo ello, el TS entiende que la investigación se llevó a cabo en estricta conformidad con los cánones constitucionales de idoneidad, necesidad y proporcionalidad.

El TS afirma que las pautas sentadas por el TEDH son sustancialmente coincidentes con las emanadas del TC y del propio TS en su doctrina anterior a la STEDH Barbulescu II.

Todo ello lleva al TS a concluir que la conducta empresarial supera holgadamente el filtro del TEDH y que la revisión del correo electrónico efectuada fue un medio idóneo y necesario para completar la investigación de los hechos que fueron

imputados en la carta de despido del trabajador. El TS entiende que la STC 170/2013, 7 de octubre, es una válida sentencia de contraste y cita también las SSTC 98/2000, 10 de abril, 186/2000, 10 de julio y 241/2012, 17 de diciembre, además de jurisprudencia del TC sobre el derecho a la intimidad.

Son de gran interés, finalmente, las SSTS (2ª, Penal) 489/2018, 23 octubre, y 328/2021, 22 abril 2021 (rec. 715/2020).

8.2. VIDEOVIGILANCIA Y GRABACIÓN DE SONIDOS EN EL LUGAR DE TRABAJO (ARTÍCULO 89 LOPDGDD)

De conformidad con el artículo 89 LOPDGDD, 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 previstas en el artículo 20.3 ET, 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 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 se entenderá cumplido el deber de informar cuando existiese al menos el dispositivo al que se refiere el artículo 22.4 LOPDGDD. De momento, se trata del distintivo de la Instrucción 1/2006, 8 noviembre, de la Agencia Española de Protección de Datos. Se recoge aquí la doctrina de la STC (Pleno) 39/2016, 3 marzo (con votos particulares), a la que enseguida se hará referencia.

En ningún caso -precisa el artículo 89 LOPDGDD - se admitirá la instalación de sistemas de grabación de sonidos ni de videovigilancia en lugares destinados al descanso o esparcimiento de los trabajadores tales como vestuarios, aseos, comedores y análogos.

La utilización de sistemas similares a los referidos en los apartados anteriores del artículo 89 LOPDGDD para la grabación de sonidos en el lugar de trabajo se admitirá únicamente cuando resulten relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo y

siempre respetando el principio de proporcionalidad, el de intervención mínima y las garantías establecidas en las previsiones anteriores. Cierra su regulación el artículo 89 LOPDGDD, estableciendo que la supresión de los sonidos conservados por estos sistemas de grabación se realizará atendiendo a lo dispuesto en el artículo 22.3 LOPDGDD.

También en videovigilancia es de interés recoger la importante jurisprudencia del TEDH, del TC y del TS recaída con anterioridad a la LOPDGDD.

Las sentencias relevantes son las SSTC 98/2000, 10 abril, y 186/2000, 10 julio, y, especialmente, la ya citada STC (Pleno) 39/2016, 3 marzo, que rectifica la STC 29/2013, 11 febrero, y la STEDH (Gran Sala) 17 octubre 2019 (López Ribalda II), que revoca la STEDH 9 enero 2018 (López Ribalda I).

La STC 186/2000 consideró compatible con la CE el establecimiento de un circuito cerrado de captación de imágenes únicamente en el puesto de trabajo (la caja) en el que se sospechaba que se estaban cometiendo irregularidades. La STC 186/2000 declaró que la medida era justificada, idónea, necesaria y equilibrada.

Por el contrario, la STC 98/2000 consideró incompatible con la CE un sistema de grabación de sonido que permitía, en un casino, en el que ya se grababan las imágenes, escuchar, además, las conversaciones de los trabajadores.

La STC (Pleno) 39/2016, de 3 marzo (con votos particulares), rectificando la STC 29/2013, de 11 febrero (también con voto particular), rechazó que se hubieran vulnerado los derechos a la intimidad y a la protección de datos de carácter personal (artículo 18.1 y 4 de la CE) por la utilización de imágenes captadas por las cámaras de videovigilancia instaladas en la empresa con la finalidad de supervisión laboral (había sospechas de que algún trabajador se estaba apropiando de dinero de la caja), entendiéndose cumplido el deber de información previa (que forma parte del contenido esencial del derecho a la protección de datos) a través del distintivo exigido por la Instrucción 1/2006, 8 noviembre, de la AEPD, colocado en el escaparate de la tienda, sin que haya que especificar la «*finalidad exacta*» que se le ha asignado a ese control y, respecto del derecho a la intimidad, el TC declara

que se observó estrictamente el principio de proporcionalidad. La STC 39/2016 tiene muy en cuenta la existencia de sospechas para justificar la instalación de un sistema de videovigilancia. Este es un elemento relevante pues una cosa es un sistema de videovigilancia instalado con carácter permanente (y no ante la existencia de concretas sospechas) y otra un sistema de videovigilancia instalado *ad hoc* ante la existencia de sospechas, sistema que será en principio temporal y no permanente. Especialmente tras la LOPDGDD, en el primer caso habrá que proporcionar la información previa, expresa, clara y concisa que exige el párrafo primero del artículo 89.1 LOPDGDD, mientras que en el segundo valdrá el dispositivo al que se refiere el párrafo segundo del artículo 89.1 LOPDGDD y al que se refería la STC 39/2016. Al cabo, y desde este punto de vista, las SSTC 29/2013 y 39/2016 podrían ser hasta compatibles.

Las SSTS, 7 julio de 2016 (rcud. 3233/2014), 31 enero 2017 (Pleno, rcud. 3331/2015),1 febrero 2017 (Pleno, rcud. 3262/2015) y 2 febrero 2017 (rcud. 554/2016) aplican ya el criterio de la STC 39/2016. La STS 2 febrero 2017 es interesante porque fueron otros trabajadores quienes se quejaron y denunciaron al trabajador despedido.

Por su parte, las SSTS 21/2019, 15 enero 2019 (rcud. 341/2017) y 212/2020, 5 de marzo de 2020 (rcud. 256/2017), aprecian falta de contradicción, porque las sentencias recurridas no contradicen la STC 39/2016, 3 de marzo de 2016, que era precisamente la sentencia referencial (en la STS 212/2020, 5 de marzo de 2020, se esgrimía adicionalmente como sentencia referencial para el segundo motivo la STS 630/2016, 7 de julio de 2016, rcud. 3233/2014). La STS 21/2019, 15 enero 2019 hace referencia a que la STEDH 9 enero 2018 (López Ribalda I), se encontraba pendiente de otro pronunciamiento por la Gran Sala del TEDH. La STS 212/2020, 5 marzo 2020 (rcud. 256/2017), tiene ya en cuenta la STEDH 17 octubre 2019 (López Ribalda II).

La muy relevante y ya mencionada STEDH (Gran Sala) 17 octubre 2019 (López Ribalda II), enjuicia un supuesto de vídeo vigilancia secreta de cajeras en un supermercado español entendiendo que, frente a lo que habría considerado

inicialmente el propio TEDH en López Ribalda I (STEDH 9 enero 2018 que ahora se revoca), no se vulneró su derecho a la vida privada (artículo 8 CEDH), y no solo su derecho a un juicio justo (artículo 6 CEDH), que ya López Ribalda I había rechazado que se hubiera infringido. La video vigilancia oculta tuvo por finalidad comprobar las sospechas de hurto. Las cuatro demandantes fueron despedidas, fundamental (aunque no únicamente), en base a las grabaciones de vídeo. Los tribunales laborales españoles admitieron como prueba las grabaciones y declararon la procedencia de los despidos; por su parte, el TC inadmitió los recursos de amparo. Ante las sospechas de hurto, el empresario instaló cámaras visibles y cámaras ocultas. La empresa informó a los trabajadores de la instalación de las cámaras visibles, pero no de las cámaras ocultas. Todos los trabajadores sospechosos de hurto fueron convocados a entrevistas individuales en las que se les mostraron los videos. Las cámaras habían filmado a las trabajadoras mientras ayudaban a los clientes y a las compañeras a sustraer artículos y a sustraerlos ellas mismas.

La STEDH López Ribalda II parte de que los tribunales españoles identificaron y ponderaron adecuadamente los derechos de las trabajadoras (el respeto a su vida privada *ex* artículo 8 CEDH) y los de la empresa (la protección de su propiedad y la buena marcha de su empresa), examinando la justificación de las medidas de videovigilancia. Respecto del argumento de que las trabajadoras no habían sido advertidas de la vigilancia, a pesar de que así lo establecía la legislación española vigente en ese momento, el TEDH declara que la medida estaba justificada por la existencia de sospechas legítimas de graves irregularidades y pérdidas, por la que la medida fue proporcionada y legítima. La STEDH López Ribalda II señala que los principios sentados en el caso Barbelescu II son aplicables a la videovigilancia en el lugar de trabajo. Los tribunales internos tuvieron en cuenta la sospecha de robo, que las cámaras enfocaban exclusivamente a las cajas y que las empleadas trabajaban en un área abierta al público. La STEDH López Ribalda II hace una distinción entre el grado de intimidad que un empleado puede esperar dependiendo de dónde trabaje: la expectativa

puede ser muy alta en lugares como baños o vestuarios, donde se puede justificar una prohibición total de la videovigilancia; puede ser alta en espacios de trabajo cerrados, como oficinas; y es, sin embargo, reducida en lugares visibles o accesibles para compañeros o para una amplia audiencia. También tiene en cuenta el TEDH que la vigilancia duró solo diez días, que las grabaciones fueron vistas por un número reducido de personas, que no se utilizaron para ningún otro fin que para determinar quiénes eran los responsables de las sustracciones y, especialmente, que ninguna otra medida hubiera permitido alcanzar dicho objetivo legítimo.

En cuanto a la falta de advertencia o notificación previa de la vídeo vigilancia, la STEDH López Ribalda II afirma que existe un amplio consenso internacional sobre la obligación de esa información previa, de manera que sólo una imperativa protección de los intereses públicos o privados importantes podría justificar la falta de información previa, lo que tiene como consecuencia que, si bien no cabe aceptar que la más mínima sospecha de que las irregularidades han sido perpetradas por los empleados pueden justificar una videovigilancia secreta por parte del empleador, la sospecha razonable de que se habían cometido graves irregularidades y el alcance de las mismas producidas en este caso pueden considerarse justificaciones serias, especialmente si, como ocurría en el caso, se sospechaba de la acción concertada de varios empleados. Por lo demás, las trabajadoras tenían a su alcance otros medios (que no utilizaron) para solicitar la reparación de la presunta violación de sus derechos en virtud de la legislación nacional de protección de datos.

La STEDH López Ribalda II descarta, finalmente, que la videovigilancia haya vulnerado el derecho a un juicio justo (artículo 6 CEDH), toda vez tuvieron la oportunidad de oponerse a la utilización de pruebas y los tribunales nacionales argumentaron ampliamente sus resoluciones. El TEDH tiene en cuenta que las grabaciones no eran los únicos elementos de juicio (se tuvieron en cuenta otras pruebas), y que las trabajadoras no refutaron su autenticidad y exactitud.

La reciente STS 817/2021, 21 julio 2021 (rcud. 4877/2018) puede ser de interés. La sentencia recurrida tenía en cuenta

la jurisprudencia anterior en un supuesto en el que, por aplicación de la STEDH 9 enero 2018 (López Ribalda I), se inadmitió la prueba de videovigilancia aportada por la empresa para justificar el despido del trabajador. La STS 817/2021 llega a la conclusión de que la prueba debió admitirse, conforme a la doctrina de las citadas STEDH (Gran Sala) 17 octubre 2019 (López Ribalda II), de la STC 39/2016, 3 marzo 2016 y de la sentencia de contraste, la STS 77/2017, 31 de enero de 2017 (Pleno, rcud. 3331/2015), reiterada por otras posteriores. Remito asimismo a la STS 1003/2021, 13 octubre 2021 (rcud. 3715/2018).

8.3. SISTEMAS DE GEOLOCALIZACIÓN EN EL ÁMBITO LABORAL (ARTÍCULO 90 LOPDGDD)

De conformidad con el artículo 90 LOPDGDD, los empleadores podrán tratar los datos obtenidos a través de sistemas de geolocalización para el ejercicio de las funciones de control de los trabajadores previstas en el artículo 20.3 ET, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo.

Con carácter previo, los empleadores habrán de informar de forma expresa, clara e inequívoca a los trabajadores y, en su caso, a sus representantes, acerca de la existencia y características de estos dispositivos. Igualmente deberán informarles acerca del posible ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión.

De interés son las SSTS 766/2020, 15 septiembre 2020 (rcud. 528/2018) y 163/2021, 8 febrero 2021 (rec. 84/2019). La primera sentencia confirma la procedencia del despido disciplinario, con base en datos del instrumento de geolocalización del vehículo de empresa que constatan su utilización fuera de la jornada laboral, pese a las instrucciones expresas al respecto; la trabajadora conocía la existencia del control por GPS por parte de la empresa.

Por su parte, la STS 163/2021 confirma la nulidad de un proyecto empresarial de geolocalización mediante app que los trabajadores repartidores debían instalar en sus móviles personales.