

A PROBA NO PROCESO LABORAL: ALGÚNS PUNTOS CRÍTICOS RECENTES *

IGNACIO GARCÍA-PERROTE ESCARTÍN
Maxistrado da Sala do social do Tribunal Supremo
Catedrático de Dereito do Traballo da UNED (s.e.)

RESUMO

O editorial trata 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 videovixilancia; e a xeolocalización.

Palabras chave: correo electrónico, proba ilícita, despedimento, dispositivos dixitais, videovixilancia, xeolocalización.

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

*Este editorial publicarase tamén no *Liber Amicorum* en memoria de Aurelio Dendentado Bonete que están a preparar Jesús R. Mercador Uguina e Ana de la Puebla Pinilla.

the workplace; and geolocalization in the context of employment relationships.

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

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.

SUMARIO

1. FONTES DE PROBA E MEDIOS DE PROBA. 2. MEDIOS DE PROBA. 3. NATUREZA DOS MEDIOS DE PROBA DO ARTIGO 299.2 LEC E DO ARTIGO 90.1 LRXS: ALGÚNS PRECEDENTES. 4. A IMPORTANCIA DA STS 706/2020, 23 XULLO 2020 (PLENO, REC. 239/2018): A NATUREZA DE PROBA DOCUMENTAL DO CORREO ELECTRÓNICO. 5. PROBA DE INFORME DE DETECTIVE: É TESTIFICAL DOCUMENTADA. 6. CARGA DA PROBA. 7. PROBA LESIVA DE DEREITOS FUNDAMENTAIS: A NOVIDADE DA STC 61/2021, 15 MARZO. 8. A LEI ORGÁNICA DE PROTECCIÓN DE DATOS PERSOAIS E GARANTÍA DOS DEREITOS DIXITAIS (LOPDGDD) E A JURISPRUDENCIA PREVIA DO TRIBUNAL EUROPEO DE DEREITOS HUMANOS (TEDH), TC E TRIBUNAL SUPREMO (TS): 8.1. DISPOSITIVOS DIXITAIS DOS TRABALLADORES E CONTROL EMPRESARIAL (ARTIGO 87 LOPDGDD); 8.2. VIDEOVIXILANCIA E GRAVACIÓN DE SONS NO LUGAR DE TRABALLO (ARTIGO 89 LOPDGDD); 8.3. SISTEMAS DE XEOLOCALIZACIÓN NO ÁMBITO LABORAL (ARTIGO 90 LOPDGDD)

1. FONTES DE PROBA E MEDIOS DE PROBA

Partindo da diferenciación entre fontes de proba e medios de proba, podería dicirse que as primeiras -as fontes- son *numerus apertus*, mentres que os segundos -os medios-, serían, máis ben, *numerus clausus*.

Como se sabe e lembrárase máis adiante, os apartados 1 e 2 do artigo 299 da Lei de axuízamento civil (LEC) establecen os medios de proba. O mesmo fan os artigos 90.1 (no seu segundo inciso, ao que igualmente farase referencia enseguida) e 91 e 95 da Lei reguladora da xurisdición social (LRXS).

Pero o artigo 299.3 LEC dispón que *"cando por calquera outro medio non expresamente previsto nos apartados anteriores deste artigo puidese obterse certeza sobre feitos relevantes, o tribunal, a instancia de parte, admitirao como proba, adoptando as medidas que en cada caso resulten necesarias."*

Parece, pois, que se admiten outros medios de proba, ademais dos enunciados nos apartados 1 e 2 do artigo 299 LEC. Con todo, o artigo 90.1 LRXS prevé que *"as partes, previa xustificación da utilidade e pertinencia das dilixencias propostas, poderán servirse de cantos medios de proba se atopen regulados na Lei para acreditar os feitos controvertidos ou necesitados de proba"*. Pártese, así, de que os medios de proba son unicamente os que están *«regulados na Lei.»*

2. MEDIOS DE PROBA

Sexa como for, os xa mencionados apartados 1 e 2 do artigo 299 LEC enuncian os medios de proba de que se poderá facer uso en xuízo.

O teor literal destes dous apartados do artigo 299 LEC é o seguinte:

"1. Os medios de proba de que se poderá facer uso en xuízo son:

- 1.º Interrogatorio das partes.*
- 2.º Documentos públicos.*
- 3.º Documentos privados.*
- 4.º Ditame de peritos.*
- 5.º Recoñecemento xudicial.*
- 6.º Interrogatorio de testemuñas.*

2. Tamén se admitirán, conforme o disposto nesta Lei, os medios de reprodución da palabra, o son e a imaxe, así como os instrumentos que permiten archivar e coñecer ou reproducir palabras, datos, cifras e operacións matemáticas levadas a cabo con fins contables ou doutra clase, relevantes para o proceso."

A destacar a referencia que o artigo 299.2 LEC fai aos:

- *"medios de reprodución da palabra, o son e a imaxe."*

E aos:

- *"instrumentos que permiten archivar e coñecer ou reproducir palabras, datos, cifras e operacións matemáticas levadas a cabo con fins contables ou doutra clase."*

Pola súa banda, e en sentido coincidente, o artigo 90.1 LRXS menciona os:

- *"procedementos de reprodución da palabra, da imaxe e do son."*

E o:

- *"arquivo e reprodución de datos."*

Precisando o artigo 90.1 LRXS que estes medios de proba *"deberán ser achegados por medio de soporte adecuado e poñendo á disposición do órgano xurisdiccional os medios necesarios para a súa reprodución e posterior constancia en autos"*, previsión esta última que seguramente non sexa xa tan necesaria ao dispoñer xeralmente os xulgados do social destes medios.

3. NATUREZA DOS MEDIOS DE PROBA DO ARTIGO 299.2 LEC E DO ARTIGO 90.1 LRXS: ALGÚNS PRECEDENTES

Maior importancia práctica ten determinar se os medios e instrumentos a que fan referencia o artigo 299.2 LEC e o artigo 90.1 LRXS son medios autónomos de proba ou, pola contra, pódense inserir no concepto, se se quere amplo, de documento. Como se sabe ben, só se se acepta o segundo, tales medios e instrumentos poderán fundar a revisión de feitos probados en suplicación e casación [artigos 193 b) e 207 d) LRXS].

Con anterioridade á LEC do ano 2000, cabe citar, en primeiro lugar, a STS 17 xuño 1996 (rec. revisión 1611/1995), na que se examina sobre a posible autonomía que podería ter a

fotografía incluída nun informe de detective, respecto deste informe, que non deixa de ser unha proba testifical. O relator desta sentenza foi Aurelio Dendentado Bonete, a quen tanto se bota de menos, e nela dicíase de xeito pioneiro o seguinte: *"A doutrina non é pacífica sobre o tratamento que, como medio de proba, hai que atribuír a estas formas de reprodución da imaxe: para quen sostén que, na noción de documento, o fundamental é a existencia dun obxecto que incorpora unha representación con posible valor probatorio e que pode ser trasladado a presenza xudicial e incorporado ás actuacións, as fotografías serían un documento. Pero para a tese que considera que a noción de documento debe limitarse ás declaracións de vontade manifestadas por escrito, estaríamos ante unha forma especial de recoñecemento xudicial, na que a imaxe do obxecto que o xuíz examina independízase do obxecto e pode ser presentada no acto de xuízo, aínda que o representado, en canto acción pasada, desaparecese."*

En segundo lugar, a STS (1ª) 523/1999, 12 xuño 1999 (rec. 2930/1994), entendeu que unhas cintas magnetofónicas achegadas debían someterse ao réxime establecido para os documentos.

Con posterioridade á LEC, e con fundamento na diferenza entre os apartados 1 e 2 do artigo 299 LEC, as SSTS 16 xuño 2011 (rec. 3983/2010), 26 de novembro de 2012 (rec. 786/2012) e 31/2020, 15 xaneiro 2020 (rec. 166/2018, FD quinto, 3) inclináronse por atribuír natureza autónoma -distinta da proba documental-, aos medios de reprodución da palabra, o son e a imaxe, así como aos instrumentos de arquivo e reprodución de datos.

Con todo, as SSTS 12 febreiro 2013 (rec. 254/2011) e 29 xaneiro 2019 (rec. 12/2018) non cuestionaron a idoneidade duns correos electrónicos para sustentar unha pretensión revisora casacional, aínda que finalmente desestimaron a solicitude.

4. A IMPORTANCIA DA STS 706/2020, 23 XULLO 2020 (PLENO, REC. 239/2018): A NATUREZA DE PROBA DOCUMENTAL DO CORREO ELECTRÓNICO

A importante STS 706/2020, 23 xullo 2020 (rec. 239/2018), ditada polo Pleno, chega no seu fundamento de dereito cuarto á conclusión de que o correo electrónico ten natureza de proba documental.

Sintetízanse a continuación os principais razoamentos desta sentenza:

1) O concepto amplo de proba documental que manexa a LEC, por exemplo, nos seus artigos 326.3, 327, 333 e 812.1. 1º.

2) O artigo 299.2 LEC límitase a establecer as peculiaridades destas fontes de proba (os medios de reprodución da palabra, o son e a imaxe e os instrumentos de arquivo e reprodución de datos) porque, a diferenza dos documentos escritos, non basta con comunicar estas probas á parte contraria, senón que normalmente é preciso visionar o vídeo, escoitar o audio ou examinar o instrumento de arquivo.

3) O concepto amplo de documento, comprensivo dos electrónicos, é o que impera no resto do ordenamento xurídico: artigo 26 CP; art. 230 LOPX; artigo 24.2 da Lei 34/2002, de servizos da sociedade da información e de comercio electrónico; artigo 3 da Lei 59/2003, do 19 de decembro, de sinatura electrónica; artigo 17 bis da Lei do notariado do 28 de maio de 1862; artigo 49.1 da Lei 16/1985, do 25 de xuño, do patrimonio histórico español; artigo 76.3 *in fine* do Real decreto 828/1995, do 29 de maio, polo que se aproba o Regulamento do imposto sobre transmisións patrimoniais e actos xurídicos documentados; artigo 41.1 do Real decreto 1671/2009, do 6 de novembro; e artigo 3 do Real decreto 263/1996, do 16 de febreiro, polo que se regula a utilización de técnicas electrónicas, informáticas e telemáticas pola Administración Xeral do Estado.

4) O avance tecnolóxico fixo que moitos documentos se materialicen e presenten a xuízo a través dos novos soportes electrónicos, o que non debe excluír a súa natureza de proba documental, coas necesarias adaptacións (por exemplo, respecto da proba de autenticación).

5) Se non se postula un concepto amplo de proba documental, chegará un momento en que a revisión fáctica casacional quedará baleirada de contido se se limita aos documentos escritos, cuxo uso será exiguo.

6) En consecuencia, debemos atribuír a natureza de proba documental aos correos electrónicos (que están nas actuacións).

7) Iso non supón que todo correo electrónico acredite o erro fáctico de instancia, do mesmo xeito que sucede cos documentos privados.

8) Para iso será necesario valorar se se impugnou a súa autenticidade pola parte a quen prexudique; se foi autenticado, no seu caso; e se goza de literosuficiencia.

Da STS 706/2020 derívase a importancia que para o correo electrónico poden ter probas, como a pericial e testifical, se se cuestiona a súa autenticidade, así como a reprodución a presenza xudicial dos medios de reprodución da palabra, da imaxe e do son e dos instrumentos de arquivo e reprodución de datos (artigo 90.1 LRXS e artigo 299.2 LEC).

5. PROBA DE INFORME DE DETECTIVE: É TESTIFICAL DOCUMENTADA

Como xa se anticipou, a proba de informe de detective ten natureza de proba testifical documentada, aínda que, como albiscou Aurelio Dendentado na STS 17 xuño de 1996 (rec. revisión 1611/1995), cabería dar autonomía ás fotografías ou vídeos que o informe puidese conter e atribuírlles, en caso, a natureza de proba documental.

De conformidade co artigo 265.1.5º LEC:

"1. A toda demanda ou contestación haberán de xuntarse:

...

5.º Os informes, elaborados por profesionais da investigación privada legalmente habilitados, sobre feitos relevantes en que aquelas apoién as súas pretensións. Sobre estes feitos, se non foren recoñecidos como certos, practicarase proba testifical"

Un suposto, relativamente recente, de informe de detective é o examinado pola STS 155/2020, 19 febreiro 2020 (rcud. 3943/2017).

No caso, declarouse a procedencia do despedimento con base nun informe de detective, no que é o detective quen forza unha entrevista de traballo cun avogado durante a súa xornada de traballo. A sentenza de suplicación admite a dita proba contra o criterio do xulgado, quen a considerou proba

ilícita sen efecto probatorio, e modificou un feito probado con base no informe escrito do detective, que considera proba documental.

A STS 155/2020 concluíu que a admisión da proba non foi axustada a dereito, ao tratarse dunha proba ilícita.

Pero o que interesa aquí subliñar é que a STS 155/2020 estableceu que non cabe modificar feitos probados con informes escritos de detectives, que non teñen a condición de probas documentais senón de proba testifical.

Como se anticipou, xa a citada STS 17 xuño 1996 (rec. revisión 1611/1995), da que foi relator Aurelio Dendentado, advertía que a posible natureza documental podería atribuírse, no seu caso, ás fotografías, pero non ao informe do detective *"que é só a expresión escrita da declaración da testemuña, é dicir, un testemuño documentado sen máis valor que o testifical segundo reiterada e coñecida doutrina"*.

6. CARGA DA PROBA

Os apartados 1 a 3 e 5 a 7 do artigo 217 LEC, sobre *"carga da proba"*, teñen o seguinte teor literal:

"1. Cando, ao tempo de ditar sentenza ou resolución semellante, o tribunal considerase dubidosos uns feitos relevantes para a decisión, desestimarás as pretensións do actor ou do reconveniente, ou as do demandado ou reconvido, segundo corresponda a uns ou outros a carga de probar os feitos que permanezan incertos e fundamenten as pretensións.

2. Corresponde ao actor e ao demandado reconveniente a carga de probar a certeza dos feitos dos que ordinariamente se desprenda, segundo as normas xurídicas a eles aplicables, o efecto xurídico correspondente ás pretensións da demanda e da reconvención.

3. Incumbe ao demandado e ao actor reconvido a carga de probar os feitos que, conforme as normas que lles sexan aplicables, impidan, extingan ou enerven a eficacia xurídica dos feitos a que se refire o apartado anterior.

4. ...

5. De acordo coas leis procesuais, naqueles procedementos nos que as alegacións da parte demandante se fundamenten en actuacións discriminatorias por razón do sexo,

corresponderá ao demandado probar a ausencia de discriminación nas medidas adoptadas e da súa proporcionalidade.

Para os efectos do disposto no parágrafo anterior, o órgano xudicial, a instancia de parte, poderá solicitar, se o estimase útil e pertinente, informe ou ditame dos organismos públicos competentes.

6. As normas contidas nos apartados precedentes aplicaranse sempre que unha disposición legal expresa non distribúa con criterios especiais a carga de probar os feitos relevantes.

7. Para a aplicación do disposto nos apartados anteriores deste artigo o tribunal deberá ter presente a dispoñibilidade e facilidade probatoria que corresponde a cada unha das partes do litixio."

Un exemplo recente da aplicación do criterio da dispoñibilidade e facilidade probatoria do apartado 7 do artigo 217 LEC pode atoparse na STS 1114/2020, 11 decembro 2020 (rcud. 1482/2018). De interese é, así mesmo, rexeitando a súa aplicación, a STS 874/2021, 8 setembro 2021 (rcud. 1866/2020).

Pola súa banda, as SSTS 874, 875 e 876/2021, 8 setembro 2021 (rcuds. 1866/2020, 2543/2020 e 2554/2020, respectivamente) e 876/2021, 9 setembro 2021 (rcud. 2143/2019) establecen que a carga da proba da transmisión dunha unidade produtiva, en tanto que constitutiva para a estimación da demanda e de conformidade co artigo 217.2 LEC, correspóndelle á parte demandante.

7. PROBA LESIVA DE DEREITOS FUNDAMENTAIS: A NOVIDADE DA STC 61/2021, 15 MARZO

Como é ben sabido, e de conformidade cos artigos 11.1 da Lei orgánica do Poder Xudicial, 287.1 LEC e 90.2 LRXS, e por citar este último precepto, non se admitirán probas que tivesen a súa orixe ou que se obtivesen, directa ou indirectamente, mediante procedementos que supoñan violación de dereitos fundamentais ou liberdades públicas.

É xusto mencionar a importancia que tivo a doutrina sentada na STC 114/1984, 29 novembro, e que levou aos preceptos mencionados.

Aínda que ten a súa orixe nun procedemento penal, é útil a sistematización que fai a STC 97/2019, 16 de xullo, sobre os "*principios xerais da doutrina constitucional sobre a proba ilícita*" (FJ 2) e os "*elementos do xuízo de ponderación. Evolución da doutrina constitucional*" (FJ 3).

Pero, dende a perspectiva xurídico laboral, unha relevante novidade áchase na STC 61/2021, 15 marzo, sobre a repercusión que ten unha proba ilícita (control do computador dunha traballadora que vulnerou o seu dereito á intimidade e ao secreto das comunicacións, proclamados nos artigos 18.1 e 18.3 da Constitución; CE) sobre a cualificación do despedimento.

En apertada síntese, a doutrina da STC 61/2021, 15 marzo, pode expresarse así:

-Dende a perspectiva do artigo 24.1 CE, a STC 61/2021 acepta como interpretación fundada en Dereito e non arbitraria da legalidade ordinaria a realizada pola Sala do social do Tribunal Superior de Xustiza de Madrid, que cualificou o despedimento como improcedente e non como nulo, aínda que o Tribunal Constitucional (TC) sinala que non é a única interpretación posible, sempre dende a perspectiva da interpretación da legalidade ordinaria, que non lle corresponde realizar ao TC.

-Previamente, a STC 61/2021 rexeita que dos artigos 18.1 e 18.3 CE emane de forma inexorable que a cualificación do despedimento nestes casos haxa de ser a nulidade.

8. A LEI ORGÁNICA DE PROTECCIÓN DE DATOS PERSOAIS E GARANTÍA DOS DEREITOS DIXITAIS (LOPDGDD) E A XURISPRUDENCIA PREVIA DO TRIBUNAL EUROPEO DE DEREITOS HUMANOS (TEDH), TC E TRIBUNAL SUPREMO (TS)

Termina este rápido repaso sobre algúns puntos críticos recentes da proba no proceso laboral coa breve exposición dos controis empresariais que permite a LOPDGDD e da reveladora xurisprudencia previa do TEDH, TC e TS.

8.1. DISPOSITIVOS DIXITAIS DOS TRABALLADORES E CONTROL EMPRESARIAL (ARTIGO 87 LOPDGDD)

De conformidade co artigo 87 LOPDGDD, *"os traballadores ... terán dereito á protección da súa intimidade no uso dos dispositivos dixitais postos á súa disposición polo seu empregador"*. O empregador poderá acceder aos contidos derivados do uso de medios dixitais facilitados aos traballadores *"co único fin de controlar o cumprimento das obrigas laborais ou estatutarias e de garantir a integridade dos devanditos dispositivos"*. Os empregadores deberán establecer *"criterios de utilización"* dos dispositivos dixitais respectando en todo caso os estándares mínimos de protección da súa intimidade de acordo cos usos sociais e os dereitos recoñecidos constitucional e legalmente. Na súa elaboración deberán participar os representantes dos traballadores. O acceso por parte do empregador ao contido de dispositivos dixitais respecto dos que admitise o seu uso con fins privados requirirá que se especifiquen de modo preciso os usos autorizados e se establezan garantías para preservar a intimidade dos traballadores, tales como, no seu caso, a determinación dos períodos en que os dispositivos poderán utilizarse para fins privados. Os traballadores deberán ser informados dos criterios de utilización aos que se fixo referencia.

Convén precisar, non obstante, de acordo coa xurisprudencia á que a continuación se fará referencia, que, aínda que o artigo 87.3, parágrafo último, LOPDGDD non o explicita, a obriga empresarial de información non é só dos criterios de utilización dos dispositivos dixitais, senón que se estende a que se teña que informar adicionalmente de que a empresa controlará (*"monitorizará"*) que os traballadores cumpran con aqueles criterios de utilización, mesmo nos supostos de prohibición de uso para fins privados.

Pode ser de interese lembrar a importante xurisprudencia do TEDH, do TC e do TS recaída con anterioridade á LOPDGDD. A ausencia de regulación legal, entre nós, dos dereitos dixitais fixo que a xurisprudencia tivese o protagonismo case exclusivo na configuración deses dereitos.

O primeiro que hai que lembrar é que, con anterioridade á LOPDGDD, xa a xurisprudencia esixía das empresas que tivesen unha política clara sobre o uso dos medios informáticos e do control do respecto a esa política e que a

dita política fose comunicada aos empregados. Trátase, principalmente, das SSTS 26 setembro 2007 (rcud. 966/2006), 8 marzo 2011 (rcud. 1826/2010), 6 outubro 2011 (Sala Xeral, rcud. 4053/2010, con voto particular) e 119/2018, 8 febreiro (rcud. 1121/2015). A verdade é que a STS 26 setembro 2007, da que foi relator Aurelio Dendentado, é -e segue sendo- unha sentenza clave que sentou unha doutrina que non só continúa plenamente vixente, senón que é a que substancialmente se levou aos textos legais.

A maneira de «romper» ou modular a «*expectativa de privacidad*», á que fai referencia, por exemplo, a aínda importante STEDH, 3 de abril de 2007 (Copland), é precisamente a existencia desa clara e comunicada política que pode incluír a prohibición do uso privado dos dispositivos ou permitir un uso moderado e que, como se sinalou, ha de advertir que a empresa fiscalizará que se cumpre a política establecida. O criterio de que a prohibición de uso privado leva implícita a facultade de control empresarial ha de entenderse matizada pola STEDH, 5 de setembro de 2017 (Barbulescu II).

Como é sabido, a xurisprudencia constitucional sentou dende o primeiro momento o criterio de que os traballadores poden exercer os seus dereitos fundamentais na empresa, aínda que coas modulacións ou adaptacións que sexan imprescindibles ou indispensables (principio de proporcionalidade) para preservar os dereitos empresariais.

A xurisprudencia considerou que o artigo 20.3 ET, en conexión cos artigos 33 e 38 CE, ampara o control empresarial no que están en xogo os dereitos dos traballadores recoñecidos nos apartados 1, 2, 3 e 4 do artigo 18 CE.

Esta doutrina foise construíndo nas SSTC 241/2012, 17 decembro, e 170/2013, 7 outubro, STEDH 5 de setembro de 2017 (Barbulescu II) e nas xa citadas SSTS, aínda que convén reiterar a cita da STS 119/2018, 8 febreiro, porque xa ten en conta a STEDH Barbulescu II.

A STC 241/2012, 17 decembro (con voto particular), axuízou un suposto no que existía unha prohibición para uso privado, polo que o TC aprecia que non había expectativa ningunha de

privacidade. As demandantes de amparo instalaron un programa no que facían comentarios despectivos de empregados e superiores, nun computador que era accesible a calquera, polo que declara o TC que non podía estar en xogo o secreto das comunicacións. Ás traballadoras impúxoselles unha sanción moi liviá.

Pola súa banda, a STC 170/2013, 7 outubro, declarou que o acceso do empregador a determinados correos electrónicos do traballador, que revelaban que transmitía indebidamente información reservada empresarial, non vulnerou os dereitos á intimidade e ao secreto das comunicacións do traballador (artigo 18.1 e 3 CE). Para a STC 170/2013, o traballador non podía ter unha razoable expectativa de confidencialidade nin de privacidade (o convenio colectivo prohibía o uso privado) e o control empresarial respectou a proporcionalidade constitucionalmente esixida. En efecto, para o TC o control empresarial foi xustificado, debido a que existían sospeitas dun comportamento irregular do traballador; a medida era idónea para a finalidade pretendida pola empresa (se o traballador revelaba a terceiros datos empresariais de reserva obrigada); e, en fin, a medida era necesaria, dado que o contido ou texto dos correos electrónicos serviría de proba da citada irregularidade ante a eventual impugnación xudicial da sanción empresarial, sen que fose suficiente o mero acceso a outros elementos da comunicación como a identificación do remitente ou destinatario, que por si sós non permitían acreditar o ilícito indicado. Finalmente –conclúe o TC–, a medida podía entenderse como ponderada e equilibrada; á marxe das garantías con que se realizou o control empresarial a través da intervención de perito informático e notario, o TC parte de que a controversia para dirimir cinguíase aos correos electrónicos achegados pola empresa como proba no proceso de despedimento.

A importante STEDH, Gran Sala, 5 de setembro de 2017 (Barbulescu II), que revoga a previa STEDH 12 de xaneiro de 2016 (Barbulescu I) –citada pola STC 39/2016, do 3 marzo, e que coincidía coa doutrina das SSTC 241/2012 e 170/2013– conclúe que aos tribunais romaneses faltoulles determinar, en particular, se o Sr. Barbulescu fora previamente advertido polo seu empregador das posibilidades de que as súas

comunicacións en Yahoo Messenger poderían ser controladas (o que debe facerse antes de que se inicien as actividades de control) e, doutro lado, que non fora informado da natureza e extensión do control ou do grao de intrusión na súa vida privada e correspondencia. Adicionalmente, a STEDH, 5 de setembro de 2017, entendeu que os tribunais romaneses fallaron á hora de determinar, en primeiro lugar, as concretas razóns que xustificaban a introdución das medidas de control; e, en segundo lugar, se o empregador puido usar medidas menos intrusivas. A STEDH, 5 de setembro de 2017, fai unha provisión da regulación supranacional, internacional e comparada, das obrigas positivas que emanan para os Estados do artigo 8 do CEDH e, aínda que recoñece, dun lado, que *"o empregador ten un lexítimo interese en asegurar o bo funcionamento da empresa e que iso pode facerse establecendo mecanismos para verificar que os empregados realizan as súas tarefas profesionais adecuada e diligentemente e, doutro, que os tribunais romaneses identificaron correctamente os intereses en presenza e os principios legais aplicables (necesidade, finalidade, transparencia, lexitimidade, proporcionalidade e seguridade)"*, reprocha aos tribunais romaneses o que se dixo. O TEDH rexeita as indemnizacións por danos materiais e morais pedidas polo Sr. Barbulescu.

Posteriormente, a STEDH, 22 de febreiro de 2018, (Libert c. Francia) (nº 588/13) considerou que non houbo ningunha violación da vida privada dun empregado dos ferrocarrís franceses (SNCF, empresa pública, fronte ao que ocorría no caso Barbulescu, o que pode ser relevante dende a óptica das obrigas negativas e positivas dos Estados) que foi despedido da empresa despois de que a consulta do seu computador profesional revelase o almacenamento de arquivos pornográficos e falsos certificados levados a cabo en beneficio de terceiros. O recorrente queixábase de que o seu empregador abriña sen a súa presenza ficheiros do disco ríxido do seu computador, o que sería unha vulneración do artigo 8 do CEDH. Os órganos xudiciais franceses consideraron procedente o seu despedimento, razoando que, salvo que os identifique expresamente como persoais (opción privado en Outlook) (neste caso, requírese en dereito francés

a presenza do empregado), cabe presumir que os correos son profesionais. E, se o son, o empresario pode velos; este é o dereito francés. O TEDH concedeu moita importancia ao feito de que o demandante non identificara ese ficheiro como privado ou persoal en Outlook.

No caso, establecíase o uso estritamente profesional, aínda que se toleraba unha utilización privada puntual; o recorrente contrariou «*masivamente*» estas instrucións e non pode pretender –dise, con amparo nalgunha sentenza francesa– que todo o disco ríxido é persoal. O control estaba previsto pola lei (afírmase), e o TEDH examina a finalidade lexítima (protección dos dereitos doutro ou dos demais; neste caso os do empregador; remítese a *Barbulescu*, 127: interese lexítimo do empresario en asegurar o bo funcionamento da empresa o que lle permite controlar os seus empregados) e a necesidade nunha sociedade democrática (imperiosa e proporcionada). Ao demandante, polas súas funcións (encargado da supervisión xeral), élle esixible un comportamento exemplar. O TEDH conclúe que as autoridades internas non excederon a marxe de apreciación que lles corresponde.

É imprescindible mencionar, finalmente, a STS 119/2018, 8 de febreiro, na que o TS ten xa en conta a STEDH, 5 de setembro de 2017 (*Barbulescu II*). Nun suposto de despedimento (declarado procedente polo TSX) no que a empresa utilizou como proba (aínda que non única) determinados correos electrónicos do traballador (que revelaban que recibira diñeiro dun provedor), o TS, corrixindo neste extremo ao TSX, declara que o acceso a eses correos non vulnerou ningún dereito fundamental do empregado recoñecido no artigo 18 da CE. O TS ten especialmente en consideración o feito de que a empresa dispoñía dunha política de utilización de medios informáticos na que se limitaba o uso de tales medios, incluído especialmente o correo electrónico, para fins exclusivamente profesionais. Así mesmo, as normas internas informaban con total claridade da posibilidade de que a empresa supervisase ou controlase a utilización de tales medios polos empregados. O traballador coñecía estas normas e aceptábaas diariamente ao acceder ao computador que tiña asignado.

Adicionalmente, a revisión do correo electrónico non se levou a efecto de modo xenérico ou indiscriminado, senón tratando de atopar elementos que permitisen seleccionar os correos a examinar, utilizando para iso palabras chave que permitisen inferir en que correos podería existir información relevante para a investigación. Desta forma, o exame limitouse aos correos pertinentes para a investigación, dispoñibles no correo corporativo do empregado, mediante o acceso ao servidor aloxado nas propias instalacións da empresa. Como consecuencia de todo iso, o TS entende que a investigación levouse a cabo en estrita conformidade cos canons constitucionais de idoneidade, necesidade e proporcionalidade.

O TS afirma que as pautas sentadas polo TEDH son substancialmente coincidentes coas emanadas do TC e do propio TS na súa doutrina anterior á STEDH Barbulescu II. Todo iso leva ao TS a concluír que a conduta empresarial supera folgadamente o filtro do TEDH e que a revisión do correo electrónico efectuada foi un medio idóneo e necesario para completar a investigación dos feitos que foron imputados na carta de despedimento do traballador. O TS entende que a STC 170/2013, 7 de outubro, é unha válida sentenza de contraste e cita tamén as SSTC 98/2000, 10 de abril, 186/2000, 10 de xullo e 241/2012, 17 de decembro, ademais de xurisprudencia do TC sobre o dereito á intimidade.

Son de gran interese, finalmente, as SSTS (2ª, Penal) 489/2018, 23 outubro, e 328/2021, 22 abril 2021 (rec. 715/2020).

8.2. VIDEOVIXILANCIA E GRAVACIÓN DE SONS NO LUGAR DE TRABAJO (ARTIGO 89 LOPDGDD)

De conformidade co artigo 89 LOPDGDD, os empregadores poderán tratar as imaxes obtidas a través de sistemas de cámaras ou videocámaras para o exercicio das funcións de control dos traballadores previstas no artigo 20.3 ET, sempre que estas funcións se exerzan dentro do seu marco legal e cos límites inherentes a este. Os empregadores haberán de informar con carácter previo, e de forma expresa, clara e

concisa, aos traballadores e, no seu caso, aos seus representantes, acerca desta medida.

No caso de que se captase a comisión flagrante dun acto ilícito polos traballadores entenderase cumprido o deber de informar cando existise polo menos o dispositivo ao que se refire o artigo 22.4 LOPDGDD. De momento, trátase do distintivo da Instrución 1/2006, 8 novembro, da Axencia Española de Protección de Datos. Recóllese aquí a doutrina da STC (Pleno) 39/2016, 3 marzo (con votos particulares), á que enseguida se fará referencia.

En ningún caso -precisa o artigo 89 LOPDGDD- admitirase a instalación de sistemas de gravación de sons nin de videovixilancia en lugares destinados ao descanso ou á provacidade dos traballadores tales como vestiarios, aseos, comedores e análogos.

A utilización de sistemas similares aos referidos nos apartados anteriores do artigo 89 LOPDGDD para a gravación de sons no lugar de traballo admitirase unicamente cando resulten relevantes os riscos para a seguridade das instalacións, bens e persoas derivados da actividade que se desenvolva no centro de traballo e sempre respectando o principio de proporcionalidade, o de intervención mínima e as garantías establecidas nas previsións anteriores. Pecha a súa regulación o artigo 89 LOPDGDD, establecendo que a supresión dos sons conservados por estes sistemas de gravación realizárase atendendo ao disposto no artigo 22.3 LOPDGDD.

Tamén en videovixilancia é de interese recoller a importante xurisprudencia do TEDH, do TC e do TS anterior á LOPDGDD. As sentenzas relevantes son as SSTC 98/2000, 10 abril, e 186/2000, 10 xullo, e, especialmente, a xa citada STC (Pleno) 39/2016, 3 marzo, que rectifica a STC 29/2013, 11 febreiro, e a STEDH (Gran Sala) 17 outubro 2019 (López Ribalda II), que revoga a STEDH 9 xaneiro 2018 (López Ribalda I).

A STC 186/2000 considerou compatible coa CE o establecemento dun circuíto pechado de captación de imaxes unicamente no posto de traballo (a caixa) no que se sospeitaba que se estaban cometendo irregularidades. A STC

186/2000 declarou que a medida era xustificada, idónea, necesaria e equilibrada.

Pola contra, a STC 98/2000 considerou incompatible coa CE un sistema de gravación de son que permitía, nun casino, no que xa se gravaban as imaxes, escoitar, ademais, as conversacións dos traballadores.

A STC (Pleno) 39/2016, do 3 marzo (con votos particulares), rectificando a STC 29/2013, do 11 febreiro (tamén con voto particular), rexeitou que se vulneraran os dereitos á intimidade e á protección de datos de carácter persoal (artigo 18.1 e 4 da CE) pola utilización de imaxes captadas polas cámaras de videovixilancia instaladas na empresa coa finalidade de supervisión laboral (había sospeitas de que algún traballador estaba a apropiarse de diñeiro da caixa), entendéndose cumprido o deber de información previa (que forma parte do contido esencial do dereito á protección de datos) a través do distintivo esixido pola Instrución 1/2006, 8 novembro, da AEPD, colocado no escaparate da tenda, sen que haxa que especificar a «*finalidade exacta*» que se lle asignou a ese control e, respecto do dereito á intimidade, o TC declara que se observou estritamente o principio de proporcionalidade. A STC 39/2016 ten moi en conta a existencia de sospeitas para xustificar a instalación dun sistema de videovixilancia. Este é un elemento relevante pois unha cousa é un sistema de videovixilancia instalado con carácter permanente (e non ante a existencia de concretas sospeitas) e outra un sistema de videovixilancia instalado *ad hoc* ante a existencia de sospeitas, sistema que será en principio temporal e non permanente. Especialmente tras a LOPDGDD, no primeiro caso haberá que proporcionar a información previa, expresa, clara e concisa que esixe o parágrafo primeiro do artigo 89.1 LOPDGDD, mentres que no segundo valerá o dispositivo ao que se refire o parágrafo segundo do artigo 89.1 LOPDGDD e ao que se refería a STC 39/2016. Ao cabo, e dende este punto de vista, as SSTC 29/2013 e 39/2016 poderían ser ata compatibles.

As SSTS, 7 xullo de 2016 (rcud. 3233/2014), 31 xaneiro 2017 (Pleno, rcud. 3331/2015), 1 febreiro 2017 (Pleno, rcud. 3262/2015) e 2 febreiro 2017 (rcud. 554/2016) aplican xa o criterio da STC 39/2016. A STS 2 febreiro 2017 é interesante

porque foron outros traballadores os que se queixaron e denunciaron ao traballador despedido.

Pola súa banda, as SSTS 21/2019, 15 xaneiro 2019 (rcud. 341/2017) e 212/2020, 5 de marzo de 2020 (rcud. 256/2017), aprecian falta de contradición, porque as sentenzas recorridas non contradín a STC 39/2016, 3 de marzo de 2016, que era precisamente a sentenza referencial (na STS 212/2020, 5 de marzo de 2020, esgrimíase adicionalmente como sentenza referencial para o segundo motivo a STS 630/2016, 7 de xullo de 2016, rcud 3233/2014). A STS 21/2019, 15 xaneiro 2019 fai referencia a que a STEDH 9 xaneiro 2018 (López Ribalda I) atopábase pendente doutro pronunciamento pola Gran Sala do TEDH. A STS 212/2020, 5 marzo 2020 (rcud. 256/2017), ten xa en conta a STEDH 17 outubro 2019 (López Ribalda II).

A moi relevante e xa mencionada STEDH (Gran Sala) 17 outubro 2019 (López Ribalda II), axuíza un suposto de vídeovixilancia secreta de caixeiros nun supermercado español entendendo que, fronte ao que consideraría inicialmente o propio TEDH en López Ribalda I (STEDH 9 xaneiro 2018 que agora se revoga), non se vulnerou o seu dereito á vida privada (artigo 8 CEDH), e non só o seu dereito a un xuízo xusto (artigo 6 CEDH), que xa López Ribalda I rexeitara que se infrinxise. A vídeo vixilancia oculta tivo por finalidade comprobar as sospeitas de furto. As catro demandantes foron despedidas, fundamental (aínda que non unicamente), con base nas gravacións de vídeo. Os tribunais laborais españois admitiron como proba as gravacións e declararon a procedencia dos despedimentos; pola súa banda, o TC inadmitiu os recursos de amparo. Ante as sospeitas de furto, o empresario instalou cámaras visibles e cámaras ocultas. A empresa informou os traballadores da instalación das cámaras visibles, pero non das cámaras ocultas. Todos os traballadores sospeitosos de furto foron convocados a entrevistas individuais nas que se lles mostraron os vídeos. As cámaras filmaran as traballadoras mentres axudaban os clientes e as compañeiras a subtraer artigos e a subtraelos elas mesmas.

A STEDH López Ribalda II parte de que os tribunais españois identificaron e ponderaron adecuadamente os dereitos das

traballadoras (o respecto á súa vida privada ex artigo 8 CEDH) e os da empresa (a protección da súa propiedade e a boa marcha da súa empresa), examinando a xustificación das medidas de videovixilancia. Respecto do argumento de que as traballadoras non foran advertidas da vixilancia, a pesar de que así o establecía a lexislación española vixente nese momento, o TEDH declara que a medida estaba xustificada pola existencia de sospeitas lexítimas de graves irregularidades e perdas, pola que a medida foi proporcionada e lexítima. A STEDH López Ribalda II sinala que os principios sentados no caso Barbelescu II son aplicables á videovixilancia no lugar de traballo. Os tribunais internos tiveron en conta a sospeita de roubo, que as cámaras enfocaban exclusivamente ás caixas e que as empregadas traballaban nunha área aberta ao público. A STEDH López Ribalda II fai unha distinción entre o grao de intimidade que un empregado pode esperar dependendo de onde traballe: a expectativa pode ser moi alta en lugares como baños ou vestiarios, onde se pode xustificar unha prohibición total da videovixilancia; pode ser alta en espazos de traballo pechados, como oficinas; e é, con todo, reducida en lugares visibles ou accesibles para compañeiros ou para unha ampla audiencia. Tamén ten en conta o TEDH que a vixilancia durou só dez días, que as gravacións foron vistas por un número reducido de persoas, que non se utilizaron para ningún outro fin que para determinar os responsables das subtraccións e, especialmente, que ningunha outra medida permitiría alcanzar ese obxectivo lexítimo.

En canto á falta de advertencia ou notificación previa da videovixilancia, a STEDH López Ribalda II afirma que existe un amplo consenso internacional sobre a obriga desa información previa, de maneira que só unha imperativa protección dos intereses públicos ou privados importantes podería xustificar a falta de información previa, o que ten como consecuencia que, aínda que non cabe aceptar que a máis mínima sospeita de que as irregularidades foron perpetradas polos empregados poden xustificar unha videovixilancia secreta por parte do empregador, a sospeita razoable de que se cometeran graves irregularidades e o alcance das producidas neste caso poden considerarse

xustificacións serias, especialmente se, como ocorría no caso, se sospeitaba da acción concertada de varios empregados. Polo demais, as traballadoras tiñan ao seu alcance outros medios (que non utilizaron) para solicitar a reparación da presunta violación dos seus dereitos en virtude da lexislación nacional de protección de datos.

A STEDH López Ribalda II descarta, finalmente, que a videovixilancia vulnerase o dereito a un xuízo xusto (artigo 6 CEDH), xa que tiveron a oportunidade de opoñerse á utilización de probas e os tribunais nacionais argumentaron amplamente as súas resolucións. O TEDH ten en conta que as gravacións non eran os únicos elementos de xuízo (tivéronse en conta outras probas), e que as traballadoras non refutaron a súa autenticidade e exactitude.

A recente STS 817/2021, 21 xullo 2021 (rcud 4877/2018) pode ser de interese. A sentenza recorrida tiña en conta a xurisprudencia anterior nun suposto no que, por aplicación da STEDH 9 xaneiro 2018 (López Ribalda I), inadmitiuse a proba de videovixilancia achegada pola empresa para xustificar o despedimento do traballador. A STS 817/2021 chega á conclusión de que a proba debeu admitirse, conforme a doutrina das citadas STEDH (Gran Sala) 17 outubro 2019 (López Ribalda II), da STC 39/2016, 3 marzo 2016 e da sentenza de contraste, a STS 77/2017, 31 de xaneiro de 2017 (Pleno, rcud. 3331/2015), reiterada por outras posteriores. Remito así mesmo á STS 1003/2021, 13 outubro 2021 (rcud. 3715/2018).

8.3. SISTEMAS DE XEOLOCALIZACIÓN NO ÁMBITO LABORAL (ARTIGO 90 LOPDGDD)

De conformidade co artigo 90 LOPDGDD, os empregadores poderán tratar os datos obtidos a través de sistemas de xeolocalización para o exercicio das funcións de control dos traballadores previstas no artigo 20.3 ET, sempre que estas funcións se exerzan dentro do seu marco legal e cos límites inherentes a este.

Con carácter previo, os empregadores haberán de informar de forma expresa, clara e inequívoca aos traballadores e, no seu caso, aos seus representantes, acerca da existencia e características destes dispositivos. Igualmente deberán

informalos do posible exercicio dos dereitos de acceso, rectificación, limitación do tratamento e supresión.

De interese son as SSTS 766/2020, 15 setembro 2020 (rcud. 528/2018) e 163/2021, 8 febreiro 2021 (rec. 84/2019).

A primeira sentenza confirma a procedencia do despedimento disciplinario, con base en datos do instrumento de xeolocalización do vehículo de empresa que constatan a súa utilización fóra da xornada laboral, a pesar das instrucións expresas respecto diso; a traballadora coñecía a existencia do control por GPS por parte da empresa.

Pola súa banda, a STS 163/2021 confirma a nulidade dun proxecto empresarial de xeolocalización mediante *app* que os traballadores repartidores debían instalar nos seus móbiles persoais.