

ARÁNZAZU ROLDÁN MARTÍNEZ

Doctora en Derecho

Profesora de Derecho del Trabajo y de la Seguridad Social.

Universidad Europea de Madrid

(Comentario a la STSJ de la Región de Murcia de 19 de julio de 2005, rec. núm. 793/2005) *

I. RESUMEN DE LOS HECHOS Y CUESTIONES DE FONDO

La actora había venido prestando servicios con categoría de auxiliar administrativo, con funciones de cajera, para la empresa «FERROVIAL SERVICIOS, S.A.». Para la realización de su trabajo, tanto ella como su compañera tenían una pequeña caja de caudales cada una, donde se guardaba la recaudación de todas las operaciones de cobro realizadas por cada una, teniendo para ello una llave. Asimismo, todas las operaciones de caja que realizaban se registraban en un ordenador, con funciones de caja registradora, que operaba con una clave personal para cada una de ellas, desconociendo la actora cuál era la clave de su compañera, que sí conocía ambas claves. Al final del turno de trabajo, debían proceder al arqueado de la caja mediante el cuadro de su caja de caudales con el registro de operaciones correspondiente a su clave de operaciones, restando el saldo resultante al saldo inicial, y esa diferencia en metálico había de ser entregada a su superior. El día 1 de diciembre de 2004 al incorporarse a su trabajo la actora, no funcionaba el sistema informático y había bastantes personas esperando por ser día de renovación de matrícula, por lo cual tanto ella como su compañera comenzaron a operar manualmente. Al poco tiempo se solucionó el problema y comenzaron a realizar cobros ambas, cada una en su ordenador y con su número de clave. La compañera de la actora trabajaba habitualmente en turno de tarde si bien ese día acudió en turno de mañana de apoyo, iniciando su trabajo a las 9 horas. La actora estuvo operando en la Caja Registradora del centro de trabajo con su compañera, cada una de ellas con su ordenador y con su clave hasta las 11:00 horas, en que la otra trabajadora se subió al despacho de su superior regresando sobre las 12:30 aproximadamente, momento en que la actora se marchó a almorzar, cubriendo su turno su compañera, para lo cual se colocó en la pantalla de la actora, pero introduciendo su clave y los datos con su propia

* Véase el texto íntegro de esta Sentencia en la *Revista de Trabajo y Seguridad Social (Legislación, Jurisprudencia)*. CEF. Núm. 274, enero 2006.

clave de operaciones. A las 12:45 aproximadamente la actora se reincorporó a su puesto de trabajo, marchándose su compañera, quien cerró su caja de caudales, pero dejó el programa informático con su clave de operaciones abierta. A partir de las 12:45 horas no se registraron operaciones de caja con la clave de la actora, constando, sin embargo, según documentación aportada por la empresa y consistente en listado informatizado una serie de operaciones realizadas con la clave de su compañera entre las 12:45 y las 14:55 horas, sin constancia cierta de quién fuese la persona que las realizó. La compañera permaneció reunida hasta las 14:15 horas. Consta acreditado que con la clave de operaciones de la actora, y entre las 9 de la mañana y las 15:00 horas, se ingresaron 1.700,05 euros. Y con la clave de operaciones de su compañera, entre el momento en que ésta se marchó y las 14:55 horas, se ingresaron 1.425,32 euros, siendo que obviamente esta recaudación no la pudo efectuar su compañera puesto que no estaba.

Las cantidades anteriores constan de los registros de operaciones del programa informático de caja registradora, los cuales se acompañaron como anexo a la carta de despido. La empresa considera que la cantidad ingresada por la actora en ese día fue muy superior a la que entregó a su jefe y ello porque llega a la conclusión de que las cantidades registradas a partir de un momento con la clave de su compañera fueron realmente ingresadas por la actora. Como consecuencia del descuadre entre lo supuestamente ingresado y lo entregado, deduce la comisión de una falta muy grave de hurto y de transgresión de la buena fe contractual y abuso de confianza y procede a un despido disciplinario. La empresa infiere la culpabilidad de la trabajadora de las siguientes deducciones: del dato de que no era necesario el conocimiento de la clave pues ésta estaba abierta, del hecho de que en ese momento fuera la única que podía tener acceso a la caja registradora, y de que a partir de las 12:27 dejaron de registrarse operaciones con su clave.

Las pruebas aportadas al juicio consisten en declaraciones de testigos y fundamentalmente en el listado informatizado de las operaciones realizadas desde ambos ordenadores. La sentencia de instancia declara que el despido es improcedente, al estimar que no hay prueba suficiente de la culpabilidad de la trabajadora.

En el fondo de la sentencia late el tema relativo a la dificultad probatoria que presentan los documentos informáticos, dada su relativa facilidad de manipulación.

Los hechos analizados en la sentencia objeto de estudio ponen de manifiesto cómo las herramientas informáticas, que en la Sociedad de la Información, constituyen el instrumento ordinario de trabajo de los empleados, han facilitado enormemente la acreditación de incumplimientos contractuales de los trabajadores, aportándose como medio de prueba en juicio. Sin embargo, tienen el inconveniente de que su manipulación es mucho más sencilla, siendo también más dificultosa la prueba de la autoría y autenticidad de los documentos que incorporan ¹. Ambas objeciones son puestas de manifiesto por la parte trabajadora, en el caso objeto de la sentencia. En efecto, ésta basa su defensa en los siguientes argumentos:

¹ Sobre la mayor facilidad de manipulación de los documentos y comunicaciones electrónicas, *vid.*, SERRANO OLIVARES, R., «Comunicaciones a través de Internet y seguridad jurídica», *Relaciones Laborales*, núm. 8, abril 2005.

- 1.º No quedó acreditado que la única explicación para lo acontecido fuera la que defendía la empresa, pues nada impide que se modificasen o manipulasen los datos que figuran en el listado aportado, incluyendo importes, claves y horas de las operaciones, lo que realmente puede hacerse por alguien con un conocimiento básico de informática.
- 2.º Que la compañera de la trabajadora no realizase las operaciones, no implica que no pudiese haber sido hecho por otra tercera persona, pues ambas trabajadoras no eran las únicas que conocían las claves de operadora ni el procedimiento para operar, como queda demostrado en el acto del juicio.
- 3.º Nada impide pensar, como hipótesis posible, que la compañera de la trabajadora, en el tiempo en que estuvo realizando cobros, pudiera, intencionadamente o por error (el sistema informático había estado fallando ese día, y nada ha acreditado que se solucionasen todos los problemas) haber realizado operaciones en un horario distinto del que aparece en el listado.

Trataremos en este comentario de dar una idea clara de la naturaleza de los nuevos medios probatorios, de su admisión en juicio y de su capacidad para demostrar la autoría de los hechos imputados a los trabajadores.

II. CONFIGURACIÓN Y ENCUADRAMIENTO DE LA PRUEBA MEDIANTE SOPORTES INFORMÁTICOS EN LA LEY DE PROCEDIMIENTO LABORAL Y EN LA LEY DE ENJUICIAMIENTO CIVIL

El artículo 90.1 de la Ley de Procedimiento Laboral ² establece que *«las partes podrán valerse de cuantos medios de prueba se encuentren regulados en la Ley, admitiéndose como tales los medios mecánicos de reproducción de la palabra, de la imagen y del sonido, salvo que se hubieran obtenido, directa o indirectamente, mediante procedimientos que supongan violación de derechos fundamentales o libertades públicas»* ³.

El artículo 90.1 del Texto Refundido de la Ley de Procedimiento Laboral (TRLPL) debe completarse con el artículo 299.2 de la Ley de Enjuiciamiento Civil (LEC) ⁴ que admite como fuentes de prueba *«los instrumentos que permiten archivar, conocer o reproducir datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase»*. La forma de acceso al proce-

² RDLeg. 2/1995, de 7 de abril (BOE del día 11).

³ Encontramos un ejemplo de la utilización de este tipo de prueba en la STSJ Cantabria de 23 de febrero 2004 (Rec. 46/2004) una empresa especializada, en presencia del representante de la empresa, y a instancia de ésta, acompañado de representante de la empresa y sin ningún otro trabajador, procedió a la revisión del ordenador de la trabajadora, llevando a cabo una copia completa en espejo del disco del ordenador. El Tribunal califica como nula la prueba por no haberse realizado en presencia del trabajador y de un representante de los trabajadores.

⁴ Ley 1/2000, de 7 de enero (BOE del día 8).

so de dichos instrumentos se regula con mayor concreción en el artículo 384 de la LEC ⁵. En el momento actual, entre dichos instrumentos cabe considerar principalmente los soportes informáticos, entre otros, los disquetes flexibles y discos duros, discos compactos, Unidades ZIP, DVD, cintas magnéticas para copias de seguridad, ficheros informatizados, memorias flash, etc. Conviene recordar, además, que mediante estos instrumentos también se pueden archivar imágenes y sonidos en forma de datos digitales ⁶. La doctrina considera que el uso del correo electrónico está integrado en dichos medios de prueba ⁷.

Dichos instrumentos serán examinados por el Tribunal por los medios que la parte proponente aporte o el que aquél disponga utilizar y de modo que las demás partes del proceso puedan, con idéntico conocimiento que el Tribunal, alegar y proponer lo que a su derecho convenga. La práctica de la prueba exige que en el acto del juicio se tome conocimiento directo del contenido del disquete, el disco duro del ordenador o del CD-ROM ⁸.

Sería necesario acompañar junto con los soportes informáticos su transcripción escrita, de modo que resulte más cómoda la práctica de la prueba. Esta previsión existe para los instrumentos de filmación, grabación y semejantes (art. 382 LEC) ⁹ y no se entiende por qué no se ha establecido también para estos instrumentos. La conveniencia de extender este modo de presentación a los soportes informáticos ha sido ya señalada por la doctrina ¹⁰.

Pese a que algunos Tribunales hablan de «pericia», creemos que los informes elaborados por los informáticos, de la misma empresa o de otra contratada al efecto, sobre el contenido del ordenador del trabajador no serían sino una «transcripción escrita» ¹¹. Sirva a modo de ejemplo, la Sentencia

⁵ Aunque no se mencionara de forma expresa, la jurisprudencia había venido admitiendo la incorporación al proceso de la información contenida en medios audiovisuales e informáticos. *Vid.*, FERNANDO GARCÍA, F.M., «Los medios e instrumentos idóneos para reproducir imágenes o sonidos o archivar y conocer datos relevantes para el proceso», en, AA.VV. (RÍOS SALMERÓN, B., y SEMPERE NAVARRO, A.V., coords.), *Incidencia de la Ley de Enjuiciamiento Civil en el Procedimiento Laboral*, Aranzadi, Pamplona, 2001, pág. 304. En nota a pie de página 2, cita la siguiente jurisprudencia: STS de 5 y 17 de julio de 1984 (Ar. 4121 y 4149) y 4 de junio de 1990 (Ar. 5012) y SSTSJ Andalucía de 28 de noviembre de 1991 (Ar. 6998) y 22 de julio de 1992 (Ar. 654).

⁶ FERNANDO GARCÍA, F.M., «Los medios e instrumentos idóneos...», *op. cit.*, pág. 305. *Vid.*, también, SANCHÍS CRESPO, C., *La prueba por soportes informáticos*, Tirant lo Blanch, Valencia, 1999, págs. 162-164.

⁷ BONILLA BLASCO, J., «Los efectos jurídicos del correo electrónico en el ámbito laboral», *Relaciones Laborales*, núm. 13, 2001, pág. 111.

⁸ MONTERO AROCA, J.; GÓMEZ COLOMER, J.L.; MONTÓN REDONDO, A. y BARONA VILAR, S., *Derecho Jurisdiccional II. Proceso Civil*, Tirant lo Blanch, Valencia, 2004, pág. 335.

⁹ «Al proponer esta prueba, la parte podrá acompañar en su caso, transcripción escrita de las palabras contenidas en el soporte de que se trate y que resulten relevantes para el caso.»

¹⁰ SANCHÍS CRESPO, C., *La prueba por soportes...*, *op. cit.*, pág. 163.

¹¹ En la STSJ Castilla y León/Valladolid de 8 de noviembre de 2004 (Rec. 2006/2004) la prueba fundamental para demostrar el uso irregular de Internet que hacía el trabajador, es el documento en el que se refleja el resultado del registro realizado en el ordenador. Previamente se había encargado a una empresa informática que preparase la terminal de ordenador usada por el ahora demandante, con un programa llamado «espía», de venta común en las tiendas de informática, al objeto de registrar, copiando el disco duro, las entradas del trabajador en Internet y las páginas visitadas. La citada empresa aceptó el encargo y programó el llamado «espía» haciendo un seguimiento de la terminal usada por el actor desde 2 de marzo de 2004 a 31 de marzo de 2004.

del Tribunal Superior de Justicia (STSJ) Castilla y León/Valladolid de 19 de noviembre de 2004. La empresa, ante la sospecha de que el trabajador pasaba información a organizaciones de la competencia, encomendó a la empresa Agrocom Servicios Integrales, S.L. la instalación de una aplicación informática en el ordenador que utilizaba el trabajador, sacándose posteriormente la información, invitando al trabajador a que lo presenciara, ausentándose éste y haciéndose en presencia de otros dos trabajadores, con el informático. Dicho informe constituye prácticamente la única prueba para probar los hechos imputados al trabajador. El Tribunal habla de la «pericia» practicada.

La doctrina se encuentra dividida en torno a la consideración de dichos instrumentos como *medios* de prueba de carácter autónomo¹² o, simplemente, como *fuentes* de prueba, que, por tanto, han de incorporarse al proceso a través de documentos¹³. Aunque no se mantenga esta opinión, lo cierto es que lo más fácil o incluso lo único posible para una de las partes, el trabajador, es aportar un soporte en papel (por ejemplo, la correspondencia electrónica cruzada con el empresario), que, a todas luces, es un documento convencional, aunque materialice una operación o comunicación llevada a cabo por conexión electrónica¹⁴. En este sentido, por ejemplo, un correo electrónico impreso tendría la condición de documento privado, siendo su valor probatorio el que el Tribunal le atribuya conforme a las reglas de la sana crítica. Pero hará «prueba plena», lo mismo que los documentos públicos, si su autenticidad no es impugnada por la parte a quien perjudiquen.

La índole de estos medios de prueba explica que, con frecuencia, la parte que los proponga esté interesada en aportar con ellos dictámenes y medios de prueba instrumentales –prueba pericial, por ejemplo– para la interpretación y para la valoración (lo que permite el párrafo segundo del art. 384 LEC). También las otras partes pueden aportar dictámenes y otros medios de prueba cuando cuestionen la autenticidad y exactitud de lo reproducido¹⁵. De hecho, en el antecedente sexto de la STSJ Madrid de 13 de marzo de 2001 se hace referencia a la existencia de un acta notarial que acreditó que, dentro del listado de correos electrónicos del ordenador personal del directivo, aparecía el mensaje enviado por el actor, sobre materia «*Resignation*», que fue recibido en ordenador del destinatario con texto idéntico al reproducido¹⁶. También en la STSJ Galicia

¹² CAVAS MARTÍNEZ, F., «El recurso laboral de duplicación y la nueva Ley de Enjuiciamiento Civil», AA.VV. (RÍOS SALMERÓN, B. y SEMPERE NAVARRO, A.V., coords.), *Incidencia de la Ley de Enjuiciamiento Civil en el Procedimiento Laboral*, Aranzadi, Pamplona, 2001, pág. 419; ALONSO GARCÍA, R.M., *El proceso de trabajo y la nueva Ley de Enjuiciamiento Civil*, Civitas, 2001, pág. 419.

¹³ De esta opinión son MONTERO AROCA, J.; GÓMEZ COLOMER, J.L.; MONTÓN REDONDO, A. y BARONA VILAR, S., *Derecho Jurisdiccional...*, *op. cit.*, 2004, pág. 334; FERNANDO GARCÍA, F.M., «Los medios e instrumentos idóneos...», *op. cit.*, págs. 305-308; MONTOYA MELGAR, A.; GALLANA MORENO, J.M.; SEMPERE NAVARRO, A.V. y RÍOS SALMERÓN, B., *Curso de procedimiento laboral*, Tecnos, 2001, pág. 129.

¹⁴ *Vid.*, DE LA OLIVA SANTOS, A., *Derecho Procesal Civil: Proceso de Declaración*, Editorial Universitaria Ramón Areces, 7.ª edición, 2004, pág. 376. Aunque DE LA OLIVA hace esta reflexión cuando habla del soporte electrónico en el que consta el contrato celebrado por vía electrónica, creemos que también se puede hacer extensiva a los correos electrónicos. En la STSJ Comunidad Valenciana de 26 de junio de 2003 (Ar. 1111) el técnico informático descarga una serie de archivos, donde aparece material festivo y fotografías, todo lo que se hace constar en un legajo.

¹⁵ *Vid.*, sobre el medio de prueba consistente en la reproducción de la palabra, el sonido y la imagen e instrumentos de archivo, conocimiento y reproducción de palabras, datos, cifras y operaciones matemáticas, DE LA OLIVA SANTOS, A., *Derecho Procesal Civil*, *op. cit.*, págs. 389-390.

¹⁶ La sentencia admitió la validez del correo electrónico como medio para comunicar la dimisión del directivo.

de 30 de mayo de 2003¹⁷ a requerimiento de la empresa, se persona un notario para presenciar cómo el informático grababa un CD con el contenido del ordenador del trabajador. Insertado un segundo CD fueron recogidos ambos, así como la CPU del ordenador por el notario, quien los trasladó a la sede de la Notaría donde los precintó. Se mantuvieron precintados hasta la realización del informe pericial judicial¹⁸. Será incluso frecuente, aportar el informe del informático de la empresa, que no se limitará a exponer el contenido del ordenador sino que puede hacer valoraciones en torno a las operaciones realizadas por el trabajador despedido (por ejemplo, puede detectar el borrado de archivos).

Con relación a los documentos confeccionados, enviados y firmados por medios electrónicos, expresamente la Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico –LSSICE¹⁹– dispone en el artículo 24.2 que «*en todo caso, el soporte electrónico en que conste un contrato celebrado por vía electrónica será admisible en juicio como prueba documental*». Por su

¹⁷ Rec. 1759/2003.

¹⁸ También en la STSJ Cantabria de 24 de enero de 2005 (Ar. 13) el registro se realizó en presencia de notario quien levantó acta de notoriedad, que se incorpora a los autos. En el mismo sentido, STSJ Cantabria de 26 de agosto de 2004 (Ar. 2513) donde el notario asistió, además, acompañado de un informático. En la STSJ Cataluña de 1 de marzo de 2005 (8691/2004) se juzgaba el despido de una trabajadora a la que se imputaba el acceso desde su ordenador, y sin quebrantar ninguna clave especial o confidencial de la empresa, a información relativa a las posibles subidas salariales de sus compañeros, tras lo cual envió cartas a todos los compañeros de su departamento indicando el salario de cada uno de ellos más el de dos empleados de otro departamento. La empresa se hizo cargo del ordenador de la trabajadora el cual fue analizado por perito informático ante notario, realizando un peritaje que consistió en un análisis digital del ordenador y en el análisis del navegador por Internet. Por el perito se llegó a la conclusión de que dicho ordenador fue utilizado para recopilar información necesaria en la elaboración de las cartas. En la STSJ Canarias/Las Palmas de 15 de marzo de 2005 (Rec. 843/2004) se calificó como procedente el despido del trabajador, Presidente del Comité de Empresa, que con un disco duro extraíble externo al ordenador dedicó muchas horas de su trabajo a copiar archivos del ordenador de la empresa, teniendo terminantemente prohibido el uso de disquetes en la unidad así como el uso de dispositivos externos. El actor en fecha de 20 de noviembre de 2003 llevó a cabo una conexión con un dispositivo externo al ordenador de la recepción, esto es, un disco duro extraíble, sobre el que se puede trabajar conectándolo al ordenador. El archivo con el que estaba trabajando el actor era un listado de los trabajadores eventuales de la empresa. Ésta tuvo conocimiento de dicha conexión, pues habían percibido con anterioridad la conexión de dichos dispositivos, no sabiendo de dónde provenían, por lo que prepararon los ordenadores para detectar la conexión de aquéllos. Así la empresa automáticamente, al percatarse de la conexión procedió a llamar al jefe de seguridad del hotel, y a un miembro del Comité de Empresa, personándose conjuntamente al Director del Hotel, en donde se encontraba el actor, requisando dicho dispositivo con consentimiento de aquél, sellándolo en un sobre para ser posteriormente examinado. El dispositivo fue examinado ante el Secretario General de UGT, un abogado del Sindicato, el jefe de personal de la empresa demandada y ante un notario, levantando acta del contenido del dispositivo, examinado por un técnico experto, independiente a las dos partes. En la STSJ Murcia de 15 de junio de 1999 (Rec. 692/1999) con el fin de obtener pruebas de que el trabajador utilizaba el ordenador de la empresa para negocios particulares, el empresario hace personar a un notario, quien acompañado de una persona que dijo ser experto en informática, constató que en uno de los ordenadores allí presentes y que el responsable de Recursos Humanos identificó como el utilizado habitualmente por el demandante, había archivados una serie de documentos. En los hechos enjuiciados en la STSJ Castilla-La Mancha de 9 de septiembre de 1999 (692/1999) se acuerdan medidas de índole cautelar, para la obtención de copia del disco duro del ordenador que utilizaba, así como la suspensión cautelar de empleo del trabajador. El contenido de todo ello, se encuentra incorporado a un CD-ROM, obtenido a presencia del notario del Ilustre Colegio Notarial. Aceptados los cargos por el trabajador, únicamente solicita la declaración de improcedencia del despido por defectos formales en la comunicación del mismo.

¹⁹ La Ley 34/2002, de 11 de julio, de Servicios de la sociedad de la información y de comercio electrónico (BOE núm. 166, de 12 de julio de 2002).

parte, el artículo 3.º 8 de la Ley de Firma Electrónica –LFE²⁰– señala que «*el soporte en el que se hallen los datos firmados electrónicamente será admisible como prueba documental en juicio*». El artículo 24 de la LSSICE habla de documentos electrónicos en general sin necesidad de que vayan firmados electrónicamente, mientras que el artículo 3.º 8 de la LFE se aplica a todo tipo de documentos firmados electrónicamente con independencia de que sirvan o no de respaldo a una relación contractual²¹.

A diferencia del proceso civil, donde la prueba por soportes informáticos debe proponerse con la presentación de la demanda, en el laboral se realizan, de forma oral y en el momento del juicio, todas las actuaciones de petición de recibimiento a prueba, recibimiento del pleito a prueba y proposición de la prueba. Ello dificulta, sin duda alguna, la capacidad de reacción de la contraparte, quien no conocerá la estrategia del demandante hasta el momento del juicio, salvo que la parte que propone la demanda estime oportuno advertir la prueba y adjuntar la transcripción con la presentación de la demanda. Las carencias de la ley procesal podrían repararse mediante la solicitud por la parte afectada de la práctica anticipada de la prueba. Obsérvese cómo, siendo los soportes informáticos propiedad de la empresa, la parte perjudicada es, normalmente el trabajador²². Conforme al artículo 90.2 del TRLPL, deberá solicitarse el requerimiento al empresario con al menos tres días de antelación a la fecha del juicio. Admitida la práctica de la prueba, y salvo causa justificada, la parte que tiene en su poder los documentos o archivos requeridos (en este caso el empresario) deberá aportarlos so pena de que puedan estimarse probadas las alegaciones efectuadas por la parte contraria (el trabajador) en relación con la prueba acordada (art. 94.2 TRLPL).

III. VALORACIÓN DE LA PRUEBA

La LPL guarda silencio en materia de valoración de la prueba practicada mediante instrumentos que permiten archivar, conocer o reproducir datos relevantes para el proceso, razón por la cual debe acudir al artículo 384 párrafo tercero de la LEC conforme al cual las reproducciones referidas se valorarán por el Tribunal según las reglas de la sana crítica aplicables según la naturaleza de cada uno de los instrumentos. Rechaza, pues, el legislador de forma deliberada la valoración tasada, que deja para los documentos *stricto sensu*. FERNANDO GARCÍA considera que esta solución es opinable en lo que se refiere a los instrumentos (ej.: un texto informático) y medios que contengan palabras o voces. En tales casos y al igual que en la prueba documental, se puede plantear si el autor aparente es el autor real (autenticidad). Por ello, hubiera tenido justificación la aplicación de las reglas de valoración del documento privado no impugnado por inauténtico, de modo que si el autor aparente no impugnara su identificación o la reconociera, el Juez quedará vincula-

²⁰ Ley 59/2003, de 19 de diciembre (BOE del día 20).

²¹ GÁLLEGO HIGUERAS, G. F. «Comentarios a la reciente Ley 59/2003, de 19 de diciembre, de Firma Electrónica: algunas novedades al marco regulador existente», *Revista Aranzadi de Derecho y Nuevas Tecnologías*, año 2004-3, núm. 6, págs. 21-40, págs. 34-35.

²² FERNANDO GARCÍA, F. M., «Los medios e instrumentos idóneos...», *op. cit.*, págs. 309-310.

do por tal admisión o reconocimiento de la autenticidad (art. 326.1 LEC). Con todo, la opción legal a favor de la valoración conforme a las reglas de la sana crítica no admite dudas ²³. Considera la autora, sin embargo, que aunque se niegue la asimilación a un documento privado de esta fuente de prueba, será preciso concluir la autenticidad de las reconocidas por la parte perjudicada, ya que la admisión por una parte de hechos que le son enteramente perjudiciales constituye prueba tasada (art. 316 LEC) ²⁴.

Ha de recordarse finalmente que la LFE contiene reglas especiales para la valoración de la prueba (art. 3.º 8). En efecto, en orden al procedimiento de prueba de la firma distingue en atención a cada tipo de firma electrónica ²⁵:

Tratándose de firma electrónica *reconocida* cabe señalar:

- Que la ley presume su autenticidad si no es impugnada.
- Si se impugna su autenticidad, establece el procedimiento para comprobarla: la firma será auténtica si el prestador de servicios de certificación, que expide los certificados electrónicos, ha cumplido todos los requisitos establecidos en la ley en cuanto a la garantía de los servicios que presta en la comprobación de la eficacia de la firma electrónica, y en especial, las obligaciones de garantizar la confidencialidad del proceso así como la autenticidad, conservación e integridad de la información generada y la identidad de los firmantes.

Si se trata de una firma electrónica *avanzada*:

- También deberá presumirse su autenticidad si no es impugnada.
- Si se impugna su autenticidad se estará a lo establecido en el apartado 2 del artículo 326 de la LEC, donde se establecen los criterios a tomar en cuenta ante la impugnación de un documento privado y se regula la posibilidad de que se solicite un cotejo pericial de letras o cualquier otro medio de prueba pertinente. En el caso de la firma electrónica avanzada tal cotejo resulta irrelevante por obvias razones por lo que es lógico que deban presentarse otros medios adecuados ²⁶. En caso de impugnación de una firma electrónica avanza-

²³ FERNANDO GARCÍA, F.M., «Los medios e instrumentos idóneos...», *op. cit.*, pág. 316.

²⁴ FERNANDO GARCÍA, F.M., «Los medios e instrumentos idóneos...», *op. cit.*, págs. 316-317. En el mismo sentido; *vid.*, ORMAZÁBAL SÁNCHEZ, G., «La prueba documental y los medios e instrumentos idóneos para reproducir imágenes o sonidos o archivar y conocer datos», *La Ley*, Colección Ley de Enjuiciamiento Civil, 2000, Madrid, pág. 206.

²⁵ RODRÍGUEZ HERNÁNDEZ, J., «Firma electrónica. Sus efectos jurídicos», *Revista Aranzadi de Derecho y Nuevas Tecnologías*, año 2004-3, núm. 6, pág. 46.

²⁶ En según qué circunstancias, podría ser viable un cotejo de firmas electrónicas al objeto de comprobar si una firma atribuida sin duda al pretendido firmante fue creada con los mismos datos de creación de firma que la que es impugnada. *Vid.*, GÁLLEGO HIGUERAS, G.F., «Comentarios a la reciente Ley 59/2003...», *op. cit.*, pág. 33.

da, los extremos a probar se referirán principalmente a aquellos que le confieren a ésta la capacidad de garantizar la identificación del firmante –por ejemplo, la confidencialidad de los datos de creación de firma– y la integridad del documento firmado –por ejemplo, la capacidad del sistema o algoritmo utilizado para crear la firma, de detectar manipulaciones en el mismo–.

IV. VIABILIDAD DE LAS NUEVAS FUENTES DE PRUEBA PARA FUNDAMENTAR EL RECURSO DE SUPPLICACIÓN Y CASACIÓN

Respecto de la consideración de los nuevos instrumentos informáticos como medios de prueba hábiles para propugnar con éxito una revisión fáctica de la sentencia de instancia en un recurso de suplicación, debe recordarse que sólo gozan de esta condición con carácter general, las pruebas documentales y periciales practicadas en el juicio²⁷. Los documentos sobre los que el recurrente se apoye para justificar la pretendida revisión de hechos declarados probados deben tener una eficacia radicalmente excluyente, contundente e incuestionable, de tal forma que el error denunciado emane por sí mismo de los elementos probatorios invocados, de forma clara, directa y patente, y en todo caso sin necesidad de argumentos, deducciones, conjeturas o interpretaciones valorativas²⁸.

Existen dificultades interpretativas para incluir dentro del término «documento» los instrumentos informáticos que permiten archivar y conocer datos relevantes para el proceso del artículo 299.2 de la LEC. Como explica CAVAS MARTÍNEZ²⁹, puesto que la LEC del año 2000 ha marcado las distancias con la prueba documental, y estos nuevos medios de prueba se configuran legalmente como instrumentos de convicción autónomos, puede deducirse que bajo el concepto expreso de documento o prueba documental a que se refiere el artículo 191 b), no pueden hallar cobijo estos medios mecánicos o informáticos de reproducción y/o acumulación de datos, de modo que, para poder sustentar en ellos el alegato de error de hecho, sería necesaria una modificación *ad hoc* de la LPL.

No obstante, en la STSJ Madrid de 6 de julio de 2004³⁰ la Sala considera que aunque los artículos 299.2 y 382 de la LEC recogen de modo autónomo la prueba documental y los instrumentos de filmación y grabación de la palabra, el sonido y la imagen, debe primar, a los efectos del artículo 191 b) de la LPL un concepto amplio de «documento» identificándolo con cualesquiera «cosas

²⁷ Artículo 191 de la LPL: el recurso de suplicación tendrá por objeto: «b) Revisar los hechos declarados probados, a la vista de las pruebas documentales y periciales practicadas». La revisión fáctica ha de ser *trascendente* respecto del fallo. A través de este motivo puede combatirse tanto el error aditivo (dar como probado lo que no sucedió), cuanto el omisivo (silenciar lo verdaderamente acaecido). *Vid.*, MONTROYA MELGAR, A.; GALIANA MORENO, J.M.; SEMPERE NAVARRO, A.V. y RÍOS SALMERÓN, B., *Curso de procedimiento laboral...*, *op. cit.*, pág. 249.

²⁸ *Vid.*, MONTROYA MELGAR, A.; GALIANA MORENO, J.M.; SEMPERE NAVARRO, A.V. y RÍOS SALMERÓN, B., *Curso de procedimiento laboral...*, *op. cit.*, págs. 250 y 330.

²⁹ CAVAS MARTÍNEZ, F., «El recurso laboral de suplicación...», *op. cit.*, págs. 415-420.

³⁰ Rec. 315/2004.

muebles aptas para la incorporación de señales expresivas de un determinado significado» (STS de 5 de febrero de 1998) y no sólo con «representaciones escritas». De esta forma serían admisibles en calidad de prueba documental, a los efectos del recurso de revisión, la fotografía, el vídeo, las cintas magnetofónicas y los «disquetes de ordenador».

En otros pronunciamientos el Tribunal sin negar el carácter de documento de los correos electrónicos rechaza, sin embargo, por las circunstancias del caso, su eficacia revisoria³¹. Así, en la STSJ Canarias/Santa Cruz de Tenerife de 7 de abril de 2005³² la razón que lleva a negar eficacia revisoria de los hechos declarados probados a los correos electrónicos es su consideración como «cartas remitidas entre unas y otras personas, que se consideran en sí como meras declaraciones y que por consiguiente, dada la naturaleza de las mismas están vedadas para que surtan efecto en la revisión pretendida»³³. En la STSJ Madrid de 1 de febrero de 2005³⁴ se solicita la revisión de los hechos declarados probados citando en apoyo de dicha pretensión una comunicación escrita, «un correo electrónico», y el Informe de Auditoría. La revisión es rechazada por el Tribunal porque dichas pruebas «no evidencian la existencia de error alguno del juzgador de instancia al valorar de forma conjunta la prueba practicada», conforme al artículo 97.2 del TRLPL.

³¹ A título de ejemplo, diversos pronunciamientos de suplicación han concedido eficacia revisoria a documentos tales como la denuncia formulada ante la Comisaría de Policía, las actas notariales, certificaciones de la Tesorería General de la Seguridad Social, certificado del Instituto Nacional de la Salud, contrato de trabajo, documentos privados o públicos, expedientes de regulación de empleo, el libro de matrícula, nóminas y recibos, pactos colectivos, otras sentencias, etc. En otras ocasiones se han tenido por documentos ineficaces actas de la Inspección, actas del juicio, actas de comité de empresa, boletines de cotización, una carta de despido, epístolas privadas, certificaciones no adveradas, certificaciones de central sindical o comité de empresa, convenios colectivos, la demanda, documentos de parte, escritos privados no ratificados a presencia judicial, fotocopias no adveradas, un informe clínico, un informe de agencia de investigación o detectives privados, el informe de auditoría, el certificado de vida laboral, el libro de matrícula, recibos y nóminas, un pliego de cargos, el recibo de saldo y finiquito y recortes de prensa. Aunque exista un cúmulo de pronunciamientos en suplicación acerca del valor de diversas modalidades de documentos o pericias, hay que ser muy prudente al invocarlos pues con frecuencia esa valoración está en función del conjunto del material probatorio existente en el caso y las contradicciones sobre la literosuficiencia o virtualidad revisoria de un documento pueden ser más aparentes que reales. *Vid.*, MONTROYA MELGAR, A.; GALIANA MORENO, J.M.; SEMPERE NAVARRO, A.V. y RÍOS SALMERÓN, B., *Curso de procedimiento laboral, op. cit.*, págs. 249-250.

³² Rec. 124/2005.

³³ STSJ Cataluña de 22 de enero de 2003 (Rollo 7852/2002): admite el correo electrónico como prueba documental. Rechaza la revisión de los hechos declarados probados por basar su pretensión el demandante exclusivamente en un correo electrónico. Recuerda la sentencia que el Tribunal Superior no está facultado para efectuar una nueva ponderación de la prueba practicada, sino que su labor procesal se restringe a realizar un control de la legalidad de la sentencia de instancia recurrida en la medida que le sea pedido, y sólo de excepcional manera puede hacer uso de esa facultad de revisar las conclusiones fácticas; facultad reservada para cuando se ponga de manifiesto, de manera patente, y evidente que el juzgador de instancia ha cometido un error en la valoración de la prueba o cuando los razonamientos que le han llevado a éste a su conclusión fáctica carezcan de la más elemental lógica, premisas jurídicas, que no acontecían en el presente supuesto al haber sido ejercitada la soberana facultad de valoración de la totalidad de la prueba practicada, «interrogatorio de las partes, testimonial y documental, valorada en su conjunto conforme a la sana crítica» y dentro de las pautas que el ordenamiento jurídico le exige para cumplir con la misión que tiene encomendada, lo que obliga a la Sala a rechazar este primer motivo, ya que a mayor abundamiento de la documental citada como fundamento de la solicitud revisoria no se deduce de manera clara, terminante y patente, sin necesidad de conjeturas, hipótesis o razonamientos más o menos lógicos el extremo que se trata de introducir en la narración histórica de la sentencia recurrida.

³⁴ Rec. 4751/2004.

V. LA PRUEBA DE LA AUTORÍA DE LAS FALTAS COMETIDAS POR EL TRABAJADOR

Debemos empezar recordando que la presunción de inocencia no tiene aplicación en el ámbito de la jurisdicción social, siendo doctrina constante del TS –entre otras, Ss. de 15 de junio de 1992 y 20 de junio de 1994–, y ello, en cuanto –SSTC 24/1983, de 23 de febrero; 36/1985, de 8 de marzo y 62/1984, de 2 de mayo– «la jurisdicción penal y laboral operan sobre culpas distintas y no manejan de idéntica forma el material probatorio para enjuiciar en ocasiones una misma conducta». Tampoco existe violación del principio de presunción de inocencia, dado que, como ha reiterado el Tribunal Constitucional (TC), rectificando su inicial jurisprudencia –entre otras, STC de 18 de marzo de 1992– la presunción de inocencia es de aplicación exclusiva en el ámbito del proceso penal, y ello porque «de un lado, el despido no es más que una resolución contractual, y por tanto no conlleva la aplicación del derecho penal y, de otro, en que la consideración por los Tribunales Laborales de que una conducta implica incumplimiento contractual, no incluye un juicio sobre la culpabilidad o inocencia del recurrente».

La afirmación anterior no significa, sin embargo, que el empresario no tenga la obligación de aportar las pruebas de la falta cometida por el trabajador y de la gravedad de las mismas y que, en caso de que dichas pruebas sean insuficientes, el despido sea declarado improcedente por el juez.

Los escasos pronunciamientos judiciales que han entrado a enjuiciar la autoría de un documento electrónico, ya sean archivos informáticos o correos electrónicos o de una navegación por Internet, guardan relación con despidos disciplinarios en los que el empresario aporta como prueba el resultado de una monitorización³⁵. En la imputación de utilización abusiva por los trabajadores

³⁵ Para lograr la acreditación de los hechos la metodología habitual y hasta ahora no excesivamente cuestionada y que para nada altera la existencia de un programa de control o monitorización, consiste en que, previo precinto del ordenador a monitorizar y su aislamiento de Internet, redes Intranet, red de área local (LAN) y de conexiones con cualquier otro medio electrónico, el empresario encarga a una empresa o profesional especializado en análisis de contenidos de ordenadores que desentrañe el del trabajador y, en su caso, del servidor proxy, todo ello en presencia de fedatario público (notario) que da fe, archiva y guarda en su protocolo los elementos electrónicos acreditativos. Ha de advertirse que un usuario que accede a Internet en el entorno de una red de área local (LAN) debe pasar por un servidor proxy que concede o rechaza tal acceso a Internet. Dicho servidor proxy guarda rastros de la actividad del usuario y del terminal desde el que accede en Internet. Además, cabe la posibilidad de que el sitio web mande *cookies* al terminal del usuario, aunque éstas también pasan por el proxy y, por tanto, también son susceptibles de registro en el servidor proxy, lo que no implica que estas *cookies* residan en el servidor proxy. Además, también queda registro del historial de acceso a Internet en el propio terminal del usuario. Si está instalado un programa de control o monitorización en la red (LAN), registra no sólo el paso (como el servidor proxy), sino que guarda un historial. El usuario tiene acceso al fichero de guarda de los rastros de acceso a Internet únicamente en el ámbito de su terminal (es decir, puede borrar el historial de acceso en su terminal, así como eliminar las *cookies* que residen en el mismo). En cualquier caso, las *cookies* tienen *per se* cierta fecha determinada de caducidad y, una vez pasada ésta, dicha *cookie* se borrará del terminal del usuario. Por lo tanto, el usuario no tiene acceso a los archivos de registro de su actividad en el ámbito del servidor proxy, salvo el caso de que dicho usuario sí tenga acceso por ciertos motivos al servidor proxy, exista o no un programa de control o monitorización de los terminales (por ejemplo, es el administrador de la red de área local en su empresa). Los datos sobre la forma de practicarse la monitorización se han tomado de TAPIA HERMIDA, A. «La monitorización. Comentario a la STSJ de Andalucía, sede en Granada, de 22-4-2003, rec. núm. 3311/2002», *Revista de Trabajo y Seguridad Social*, CEF, núm. 248, noviembre 2003, págs. 153-154.

de los medios electrónicos puestos a su disposición por el empresario, hay un problema de prueba que no soluciona ni mitiga el establecimiento de un sistema de control o monitorización. Se trata de la posibilidad de que otros trabajadores accedan al *password* del ordenador desde el que se realiza la falta.

Como recuerda BONILLA BLASCO³⁶ la empresa pone normalmente a disposición de sus empleados una dirección individual de correo electrónico (lo más común es la arquitectura nombre y apellido@nombre de la empresa.com). En principio podría pensarse que todos los correos electrónicos que se envíen desde esta dirección se corresponden con el empleado al que se le ha asignado tal dirección de correo. Y esto es lo que ocurre en la inmensa mayoría de los casos. También debe señalarse que en la mayoría de las empresas, los empleados necesitan de un nombre de usuario y de una contraseña para acceder a los equipos informáticos que la empresa pone a su disposición de forma que para enviar un mensaje desde la dirección individual proporcionada por la empresa se requiere teclear en el momento del encendido del ordenador el nombre del usuario y la contraseña, que sólo el empleado en cuestión conoce.

No obstante, el problema de la autoría no se resuelve en su totalidad con la introducción de un nombre de usuario y de una contraseña en el momento de proceder al encendido del ordenador. Resulta común en la práctica de las empresas dejar el ordenador encendido mientras el empleado no está en su puesto de trabajo³⁷. En ocasiones, por razones atinentes a la organización y buena marcha de la organización empresarial, el empresario, si es una persona física, el administrador o administradores en otro caso, y el personal directivo de la empresa, han de tener conocimiento del *password* asignado a cada trabajador, y no es infrecuente que otros trabajadores, so pena de graves ineficiencias (costes), también tengan tal conocimiento, en ocasiones porque el propio trabajador lo comunica (por ejemplo, porque está de baja por enfermedad) o incluso porque dicho *password* se encuentre a disposición de quien con mínimo esfuerzo quiera obtenerla en una pluralidad de dependencias de la empresa (departamentos de informática, recursos humanos, dirección, etc.). Todo lo cual hace que, en definitiva, resulte muy difícil determinar quién ha efectuado una precisa navegación o ha utilizado un correo electrónico³⁸.

En este sentido, es cierta la afirmación de BONILLA BLASCO de que la adopción de los sistemas e instrumentos que garanticen la autoría en la utilización de estas comunicaciones, tales como la firma electrónica, facilitará enormemente la solución a todas estas cuestiones. Sin embargo, hoy en día, la utilización de estos instrumentos no es, ni mucho menos, práctica generalizada en las empresas³⁹.

A todo ello hay que añadir el problema de la autenticidad, que está en íntima conexión con la seguridad informática en el uso del correo electrónico. Para ello existen las herramientas de encriptación de mensaje, pero que en la mayoría de los casos requieren de un software que, según lo que

³⁶ BONILLA BLASCO, J., «Los efectos jurídicos del correo electrónico...», *op. cit.*, pág. 110.

³⁷ Véase nota anterior.

³⁸ TAPIA HERMIDA, A., «La monitorización...», *op. cit.*, pág.166.

³⁹ BONILLA BLASCO, J., «Los efectos jurídicos del correo electrónico...», *op. cit.*, pág. 111.

dispongan las normas sobre utilización de los sistemas informáticos vigentes en la empresa, no está permitido instalar en los equipos informáticos de las distintas empresas, puesto que, si la empresa no cuenta con las oportunas licencias, se podrían vulnerar los derechos de propiedad intelectual ⁴⁰.

BONILLA BLASCO ⁴¹ propone acudir a las reglas de las presunciones ⁴², de forma que se presume que, en aquellos supuestos en los que la empresa ha instalado unos sistemas de seguridad para utilizar la dirección individual de correo de cada empleado, deba presumirse que el mensaje enviado bajo la dirección individual correspondiente a un empleado ha sido enviado por dicho trabajador ⁴³. Si el empleado cuestionara la autoría, la autenticidad o la exactitud del mensaje, entonces debería invertirse la carga de la prueba, aportando los dictámenes y medios de prueba apropiados para aquello en el sentido expuesto en el párrafo segundo del artículo 382 de la LEC ⁴⁴. A todo ello hay que añadir que es responsabilidad del empleado dar cumplimiento a los deberes mínimos de seguridad a este respecto, por lo que, por ejemplo, cuando comunique la clave de acceso a terceras personas, la presunción de autoría y autenticidad deberá operar en toda su extensión.

Por ello, y en espera de los futuros desarrollos técnicos que deberán tender hacia la expansión de la firma electrónica, la doctrina ha resaltado la enorme importancia de la instalación de sistemas de seguridad en los ordenadores puestos a disposición de los empleados, como medio para presumir la autoría de los mensajes, así como de la realización de copias de seguridad (*back ups*) y la instalación de sistemas informáticos de *tracking* en los que consten todas las entradas en el sistema, como medio para garantizar la autenticidad de los mensajes, es decir, la adecuación entre el contenido del mensaje enviado y del mensaje recibido ⁴⁵.

⁴⁰ BONILLA BLASCO, J., «Los efectos jurídicos del correo electrónico...», *op. cit.*, pág. 111.

⁴¹ BONILLA BLASCO, J., «Los efectos jurídicos del correo electrónico...», *op. cit.*, pág. 112.

⁴² Pese a que las presunciones no son propiamente medio de prueba, sino método para fijar la certeza de ciertos hechos o mecanismo de dispensa de la prueba, resultan igualmente importantes en materia probatoria. En este sentido, la LEC distingue entre las establecidas por la ley (presunciones *legales*) y las establecidas por el orden jurisdiccional (presunciones *judiciales*). Estas últimas exigen que entre el hecho admitido o probado y el presunto exista un «enlace preciso y directo según las reglas del criterio humano» (art. 386.1 LEC), admitiendo siempre la prueba en contrario (art. 386.2 LEC). *Vid.*, MONTROYA MELGAR, A.; GALIANA MORENO, J.M.; SEMPERE NAVARRO, A.V. y RÍOS SALMERÓN, *Curso de procedimiento laboral*, Tecnos, 2001, pág. 122.

⁴³ Indudablemente esta presunción no actúa cuando el trabajador carece de clave personal. *Vid.*, en este sentido STSJ Navarra de 19 de diciembre de 2003 (Rec. 291/2003): la Sala enjuicia el despido disciplinario del encargado gestor de una empresa que al iniciar un proceso de Incapacidad Temporal, se lleva a su domicilio disquetes del ordenador que versaban sobre informes de trabajo, alegando que actuó de esa forma por desconfiar de la utilización y manipulación del ordenador por otras personas. Se califica el despido como improcedente al no poder acreditarse la autoría del borrado de determinados ficheros por parte del trabajador, ya que éste no era la única persona que poseía llaves de la oficina y tuviera acceso al sistema informático, pues el ordenador carecía de clave de acceso y de claves especiales para guardar documentos. Recuerda el Tribunal que «la manipulación del sistema informático, en sus diversas modalidades, copia de documentos, su alteración, borrado de los mismos, e incluso el "espionaje" de la información y su sustracción, no es función dificultosa pudiendo ser realizada por cualquiera de las personas que accedan a ese puesto informático».

⁴⁴ El artículo 384.2 de la LEC, relativo a los «instrumentos que permitan archivar, conocer o reproducir datos relevantes para el proceso» remite al artículo 382.2 –dedicado a instrumentos de filmación, grabación y semejantes– conforme al cual «la parte que proponga este medio de prueba podrá aportar los dictámenes y medios de prueba instrumentales que considere convenientes. También las otras partes podrán aportar dictámenes y medios de prueba cuando cuestionen la autenticidad y exactitud de lo reproducido».

⁴⁵ BONILLA BLASCO, J., «Los efectos jurídicos del correo electrónico...», *op. cit.*, pág. 112.

Consideramos que la prueba en contrario de la autoría puede tener lugar demostrando que en el momento en que se realizó la acción imputada, por ejemplo, envío de un correo, el presunto autor no se encontraba en su puesto de trabajo o bien aportando informe de perito informático ⁴⁶ que demuestre, en el ejemplo que hemos puesto, que el correo fue enviado desde otro ordenador o que había sido modificado.

Aplicar la regla de presunciones es lo que se hace en la STSJ de Castilla y León/Valladolid de 19 de noviembre de 2004 ⁴⁷. El trabajador trabajaba en jornada flexible siendo su horario habitual de 9 a 14 y de 16 a 19 horas, trabajando con equipos informáticos conectados en red. Ante la sospecha de que pasaba información a organizaciones de la competencia, la empresa encomendó a la empresa Agrocom Servicios Integrales, S.L. la instalación de una aplicación informática en el ordenador que utilizaba el trabajador, sacando la información, invitando al trabajador a que lo presenciara, ausentándose éste y haciéndose en presencia de otros dos trabajadores, con el informático. De la información extraída del ordenador se comprobó que había entrado, en las horas y días que en la carta de despido se hacían constar, en los ordenadores de sus compañeros, así como en páginas de Internet de contenido lúdico a partir de las 14 horas, éstas en cortos períodos de tiempo. Uno de los días, sobre las 10,33 horas, se introdujo en el ordenador del Coordinador General de su empresa, realizando una copia de uno de los documentos, titulado «a Don Rodrigo.Doc», documento que guardó protegiéndolo con contraseña. Frente a la sentencia de instancia que reconoce la procedencia del despido, el trabajador recurre en suplicación, solicitando, entre otras cosas, modificación de los hechos declarados probados para que se recogiera que no se había acreditado que fuera él quien manejó el ordenador los días y horas que se dice en la carta de despido, rectificación que rechaza el Tribunal porque, entre otras razones, «resulta evidente y lógica la afirmación de que el ordenador del actor lo manejara él mismo en horas de trabajo».

Los Tribunales han enjuiciado casos en los que se tenía constancia de que la contraseña del trabajador era conocida por otros compañeros.

Por ejemplo en la Sentencia del Juzgado de lo Social de Barcelona de 16 septiembre 2002 ⁴⁸ el juez no admite como prueba la monitorización realizada. Los compañeros de trabajo tenían acceso al *password* del ordenador del trabajador en la medida en que éste era público (el propio auditor informático, atendiendo a la ausencia del trabajador, accedió a los archivos de éste a través de la contraseña de la misma que le proporcionó otro asalariado) ⁴⁹. En dichas circunstancias, correspondía

⁴⁶ En España propiamente no existe la «profesión» de perito informático, entre otras razones porque en la mayoría de las Comunidades Autónomas no se han constituido Colegios Profesionales. Aquellos que sí se han constituido, así como Entidades Análogas, como la Asociación para la Prevención y el Estudio de Delitos, Abusos y Negligencias en Informática y Comunicaciones Avanzadas, envían anualmente al Consejo General del Poder Judicial, listas de expertos para que sean incluidos en las listas de peritos para los Juzgados de los cuatro órdenes jurisdiccionales: civil, penal, contencioso-administrativo y laboral. <http://www.cita.es/apedanica/>

⁴⁷ Rec. 2143/2004.

⁴⁸ *Actualidad Aranzadi*, Nuevas Tecnologías, núm. 554.

⁴⁹ *Vid.*, también STSJ Madrid de 17 de octubre de 2001.

a la empresa probar que el trabajador se encontraba en el horario de la navegación que se le imputa en su puesto de trabajo. En el mismo sentido, la STSJ Madrid de 23 de marzo de 2004⁵⁰ califica de improcedente el despido de trabajador al que se le imputaba la navegación por Internet para asuntos privados, por no considerar probado que aquél fuera el autor de los accesos, pues el hecho de que se utilizara su ordenador y su clave aunque en principio pudieran dar lugar a presumirle autor, no cabe tal presunción cuando se acreditó que el *password* de todos los usuarios era conocido por todos los trabajadores⁵¹, y que en situaciones de bajas, permisos, necesidades de trabajo y otras causas, los empleados utilizaban de forma indistinta los ordenadores.

En la STSJ Andalucía de 22 de abril de 2003⁵²: aunque el ordenador hubiera sido utilizado por otros compañeros (no existía clave personal para entrar al mismo), queda acreditado que quien se introdujo en las páginas fue el trabajador pues el acceso tuvo lugar durante el período en que se encontraba solo en la empresa (de 7 a 9 de la mañana).

En la STSJ Madrid de 21 de junio de 2005⁵³ se analiza un supuesto en que el empresario, voluntariamente, había puesto a disposición del Comité de empresa y de las secciones sindicales, los medios de comunicación con los empleados, mediante un sistema de envíos denominado «Todos», pero sometidos a unas reglas en su uso. Entre otras, y a raíz de un comunicado remitido por el Comité que contenía ofensas a un trabajador, se impuso la necesidad de obtener autorización para la publicación de la información y evitar la difusión de noticias ajenas al derecho de información. Negada, posteriormente, la autorización para publicar dos comunicados, éstos fueron enviados desde el correo del que era responsable uno de los miembros del Comité, a los correos individualizados de los trabajadores, siendo posteriormente despedido aquél por desobediencia grave y transgresión de la buena fe contractual. El trabajador recurre la sentencia de instancia, que declaró procedente el despido, por entender que en ésta se había obtenido la conducta del demandante de unas presunciones, al no existir dato que permitiera entender su intervención. La Sala recuerda que la sentencia recurrida estimó, que el demandante era responsable del correo electrónico desde el que se difundió el comunicado porque, al haber puesto la empresa a disposición de los sindicatos, los medios de comunicación y las reglas para su uso, el demandante asumió la responsabilidad en el uso de aquel correo electrónico, del *password* y contraseña. Probado que los correos se enviaron desde el correo del demandante, la Sala estima que a lo anterior no obsta el hecho de que el trabajador tuviera concedido el día de los hechos un permiso, ya que no implica necesariamente que ese día no acudiera a la empresa o autorizase a otra persona a realizar tal envío en ese mismo día.

⁵⁰ Rec. 5644/2003 (Aranzadi Social 2004/2220).

⁵¹ La empresa asignaba a cada trabajador una clave o *password*, idéntica a la del correspondiente correo electrónico, y que consistía en la inicial del nombre y el apellido. La empresa no había establecido la obligación de cambiar de clave o *password*. Algunos trabajadores que intentaron cambiarla no pudieron efectuarlo y al ponerlo en conocimiento del departamento de Redes y Comunicación, éste les indicaba un proceso con el que hubieran podido modificar su clave. La empresa, cuando el cambio de clave no produce problemas al trabajador, desconoce y no puede saber si un trabajador ha variado o no la clave de usuario de acceso a Internet.

⁵² Rec. 3311/2002.

⁵³ Ar. 1707.

En cualquier caso no es necesario que el trabajador, cuando es el demandado, demuestre que el autor no fue él, siendo suficiente con hacer nacer en el juez la duda de que no fue él, por ejemplo mediante un informe pericial que recoja la posibilidad alta de que desde otro ordenador alguien pueda enviar correos con su dirección como si fuera desde su ordenador, o de que alguien pueda entrar en éste sin necesidad de introducir la contraseña del trabajador sancionado. En el caso enjuiciado en la STSJ Cantabria de 26 de agosto de 2004 ⁵⁴ el registro del servidor de la empresa y del disco duro del ordenador de uno de los trabajadores de un centro de trabajo diferente, revela que fue él quien envió un correo amonestando a un compañero, bajo la identidad supuesta del jefe de personal. Los informes periciales prueban que el trabajador había accedido a identificadores de correos de otros usuarios, había iniciado sesión de correo con ellos instalando programas con tal finalidad espuria (programas que permiten la captura de pulsaciones de teclado, así como programas de borrado de archivos temporales e históricos), y, finalmente, había remitido correos con identidad supuesta.

Si el demandado consigue despertar esa duda en el juez, se aplicarían las reglas de la carga de la prueba recogidas en el artículo 217 de la LEC: «1. Cuando, al tiempo de dictar sentencia o resolución semejante, el tribunal considerase dudosos unos hechos relevantes para la decisión, desestimarán las pretensiones del actor o del reconvincente, 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 reconvincente 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 reconvenición. 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. 6. 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».

Sirva de ejemplo de lo que acabamos de decir la STSJ País Vasco de 14 de septiembre de 2004 ⁵⁵. Frente a la acusación realizada por la empresa de que el trabajador se dedicaba en horas de trabajo a navegar por Internet, el juzgador tiene en cuenta la posibilidad de que los archivos hubieran podido ser manipulados sin dejar huella, así como la posibilidad de que se hubiera utilizado por otras personas la contraseña del trabajador para acceder a la red como si de él se tratara ⁵⁶. Indica el

⁵⁴ Ar. 2513.

⁵⁵ Ar. 3984.

⁵⁶ Son hechos probados de la sentencia que para el desarrollo de su actividad, existían en el departamento del trabajador varios ordenadores, sin que ninguno se hallare expresamente asignado a cada trabajador, sino que se ocupaban los disponibles a medida que se fuera llegando a la oficina; el trabajador tenía su contraseña, que también era conocida por su responsable y por la Directora del Departamento; el acceso a Internet a través de los ordenadores de la empresa quedaba registrado en un proxy corporativo, con el historial de la navegación de los distintos ordenadores, pudiendo accederse a ello sin conocer la contraseña de cada empleado. El actor no había usado ningún sistema para evidenciar que no deseaba que el registro de páginas de su navegación fuera visto; el registro que quedaba en el proxy podía ser manipulado para dejar constancia ficticia de las visitas a las páginas que se quisiera.

TSJ que «se trata de posibilidades que hay que barajar y que han permitido que el juzgador *a quo* no haya podido tener por probadas las imputaciones hechas por la empresa al actor para causar su despido, a pesar del más que pormenorizado análisis que del conjunto de la prueba practicada –y en su detalle–, ha hecho en la sentencia ahora recurrida». De igual manera, la imputación al trabajador de un determinado número de visitas a determinadas páginas web basándose en que sólo han podido ser visitadas por el trabajador al llevar asociados *cookies*, se ha rechazado por la doctrina bajo la consideración de que se trata de una imputación imprecisa, dado que los *cookies* son «ficheros que almacenan información de forma automática para facilitar los accesos, eliminando pasos intermedios para lograr una última conexión, pero esos contenidos son registros del ordenador desde el que se opera, y por ello indican que desde un ordenador se han utilizado los accesos»⁵⁷. Algunas sentencias han considerado que no resultan probados los hechos imputados al trabajador, cuando se prueba tan sólo que se ha conectado a un gran número de páginas, permaneciendo en muchas ocasiones abiertas simultáneamente varias de ellas, pero no se prueba que el trabajador haya dedicado un tiempo considerable a navegar por Internet para usos particulares⁵⁸. En todo caso, si las tareas del trabajador le obligan a conexiones o transferencias con páginas web, la imputación de un uso abusivo de Internet para fines privados requiere que se concreten las páginas que se consideran ajenas a sus funciones laborales⁵⁹.

En la STSJ Islas Baleares de 11 de octubre de 2004⁶⁰ se imputaba a la trabajadora, entre otras faltas, la navegación en horario de trabajo por páginas de Internet de contenido pornográfico. La empresa pretendía modificar un hecho declarado probado en la sentencia de instancia con la finalidad de que de la existencia de correos electrónicos recibidos en la dirección de correo electrónico que la trabajadora tenía en el ordenador de la empresa, remitidos desde servidores de páginas de Internet de contenido pornográfico, el Tribunal dedujera que la trabajadora se había suscrito en las citadas páginas para recibir dichos correos electrónicos, pues, teniendo la posibilidad de solicitar que se dejaran de enviar este tipo de correos electrónicos a su dirección de e-mail, no lo hizo; si bien cada correo electrónico de este tipo preveía la posibilidad de restringir el envío de los mismos. El Tribunal admite parcialmente tal modificación, «salvo los juicios de valor que se contienen en el mismo como que fue la actora quien suscribió las páginas de Internet de contenido pornográfico, al no expresarse en qué fecha se practicó dicha suscripción, dándose a entender dicha autoría de la posibilidad de que la misma lo podría haber restringido, lo que es una mera hipótesis, dado que no consta acreditado tal hecho, ni los conocimientos de informática de la actora sobre ello».

En la STSJ Galicia de 30 de mayo de 2003⁶¹ el trabajador, al que se le imputaba navegación en horas de trabajo por páginas porno de Internet, alegaba como circunstancias para desvirtuar el hecho probado en sentencia de instancia de su autoría, el hecho de que su despacho no permanecía

⁵⁷ RUANO ALBERTOS, S., «Facultades de control por medios informáticos», *Tribuna Social*, num. 162, junio 2004, pág. 36. Cita la autora la STSJ Cataluña de 11 de junio de 2003 (Ar. 2516).

⁵⁸ RUANO ALBERTOS, S., «Facultades de control...», *op. cit.*, pág. 36. Cita la autora la STSJ Madrid de 23 de julio de 2003.

⁵⁹ RUANO ALBERTOS, S., «Facultades de control...», *op. cit.*, pág. 36.

⁶⁰ Rec. 292/2004.

⁶¹ Rec. 1759/2003.

cerrado, los ordenadores de la empresa trabajaban en red –salvo uno– y el ordenador que estaba en el despacho del trabajador no tenía clave de acceso. El Tribunal admite la adición de estos hechos pero entiende que no desvirtúan el hecho probado de la autoría por la especial ubicación del trabajador en su despacho –parece ser un despacho individual– y puesto que la pericia realizada demostró que los numerosos accesos se habían realizado desde su despacho.

El informe pericial propuesto por el trabajador o el perito judicial puede demostrar que el ordenador no fue manipulado. Así en la misma STSJ Galicia de 30 de mayo de 2003 consta acreditado que «a requerimiento de la demandada, el Notario Sr. P... se personó a las 18:30 horas del día 16 de agosto de 2002 en las oficinas de la F... G... de P..., hace saber su condición de Notario y el objeto de su presencia a Don I..., que dijo ser informático, quien procedió a extraer datos de un ordenador que se encontraba en el despacho en cuya puerta figuraba la palabra..., trasladando dichos datos a un CD. Insertando un segundo CD, fueron recogidos ambos, así como la CPU del ordenador trasladando todo al despacho donde los precintó. En el informe del perito judicial se hace constar que a las 16,50 horas del 16 de agosto de 2002, el ordenador deja de registrar actividad» y por lo tanto, desde esa fecha no mostraba cambio de estado alguno. El perito judicial había sido designado por insaculación por el juez entre ingenieros informáticos. En este sentido, resulta de gran importancia que el registro del ordenador se realice de la forma más inmediata posible a la actuación que se imputa. Por ejemplo, en la de Cantabria de 26 de agosto de 2004 ⁶² frente a la alegación del trabajador de que cualquier persona pudo conocer las claves precisas y validarse en la red como si fuera el usuario concreto, el Tribunal tiene en cuenta la «inmediación temporal entre la situación del actor, aparentemente trabajando entre las 16 y las 16:27 horas del día 6 de abril de 2004, abriendo determinados archivos de otros usuarios, (...) de 16:20 a 16:21, de naturaleza confidencial, durante la sesión, y el posterior e inmediato registro o intervención del ordenador que aprecia tal intromisión ilegítima».

Es evidente que en el campo en el que nos estamos moviendo será en muchos casos imprescindible el concurso de peritos informáticos ⁶³, para que a través de sus conocimientos se pueda proceder a la práctica de la prueba de determinados soportes informáticos por sus especiales características ⁶⁴.

⁶² Ar. 2513.

⁶³ Los peritos deberán ser traídos por la parte interesada o, en su caso, solicitados por el órgano judicial. En estos casos de designación judicial del perito, y salvo que las partes se muestren conformes a que el dictamen sea emitido por una determinada persona o entidad, habrá de seguirse el procedimiento previsto en el artículo 341 de la LEC, esto es, designando por orden a uno o varios de los incluidos en una lista que anualmente debe confeccionarse con los profesionales señalados por los respectivos Colegios o entidades análogas, academias e instituciones culturales y científicas, como dispuestos a actuar como peritos. Igualmente, previa solicitud a sindicatos, asociaciones y entidades apropiadas debe establecerse otra lista en la que se incluirán las personas que, sin título oficial, sean prácticos o entendidos en determinadas materias.

⁶⁴ *Vid.*, sobre el peritaje informático, LÓPEZ-SILVES, A., «Evidencias electrónicas», *Revista Digital Bit@cora*, núm. 2, marzo 2005, págs. 3-5, *Revista del Colegio Oficial de Ingenieros en Informática de la Comunidad Valenciana*, <https://mak-tub.eps.ua.es/servicios/ultimasnoticias/files/cas/00404/noticia.pdf>

VI. EXAMEN DE LA SENTENCIA DEL TRIBUNAL SUPERIOR DE JUSTICIA DE MURCIA DE 19 DE JULIO DE 2005

El TSJ de Murcia comparte el criterio de la sentencia de instancia y ratifica la calificación del despido improcedente, por considerar insuficientes las pruebas practicadas para llegar a la conclusión de que la actora se había apoderado del dinero de la empresa.

Frente a los casos analizados anteriormente, donde los archivos o los correos habían sido encontrados en el ordenador del trabajador, previa inclusión de la clave de éste, en el caso objeto de la sentencia la empresa imputa una serie de hechos a la propietaria de un ordenador, a la que se acusa de haber estado trabajando con la clave de una compañera. Ante tales circunstancias, el juez no puede aplicar la presunción de que la autora de los hechos es la propietaria del ordenador, pero tampoco puede presumirse que fue la titular de la clave, pues resulta suficientemente demostrado que durante el período de tiempo en el que ocurrieron los hechos, permaneció reunida con sus superiores. Correspondía a la empresa demostrar que pese a las especiales circunstancias del caso, la actora era la autora.

En primer lugar, respecto de la prueba testifical, la sentencia recuerda que ningún testigo manifestó haber visto a la actora operando o manejando la Caja en la franja horaria indicada en la carta de despido, sin que el hecho de que su compañera se encontrase realizando otros trabajos en el despacho de su superior, implicase que necesariamente había de ser la actora la que hubiese realizado esas operaciones, pues la misma lo negó en todo momento, no sólo en demanda sino también en el expediente informativo abierto y en el que ya se le imputaban una serie de cargos.

La actora sostuvo que a partir de esa hora dejó de operar con su clave, y que tampoco operó en ese tiempo con la clave de la compañera, ni siquiera por error, pues indicó que se había dedicado a atender al público en otros asuntos, y había estado por las taquillas y en otras dependencias durante ese tiempo, sin realizar cobros ni operar en Caja.

Por otro lado, la Sala estima que de la documentación aportada por la empresa y consistente en listado informatizado de supuestas operaciones realizadas con ambas claves de las dos trabajadoras, tampoco cabe extraer la exactitud y realidad de las operaciones a que se refieren y ello **por carecer de virtualidad probatoria en sí mismos dichos documentos, al ser documentos de parte, y no ir acompañados de otra prueba pericial, bien contable, bien practicada por perito experto en informática** que reflejase la fiabilidad de los citados documentos en cuanto a la exactitud y certeza de los datos que reflejan, no sólo en cuanto a la fecha y hora en que se realizaron las operaciones, sino en cuanto a la cuantía de las mismas, siendo evidente que cualquiera con ciertos conocimientos en informática puede manipular las fechas y horas y cualesquiera otros datos. Y prueba evidente de ello es el listado aportado con el número 6 de documentos, correspondiente a Informe de movimientos de caja por medios de pago del operador 003, en el que las horas de las supuestas operaciones aparecen reflejadas no en forma correlativa sino en desorden.

El Tribunal parece aplicar a la prueba consistente en el listado informático, el artículo 384 de la LEC, considerando que para acreditar la autenticidad y la ausencia de manipulaciones era necesario que la parte proponente hubiera aportado «dictámenes y medios de prueba» adicionales.

Pero es que además, ese día hubo un fallo en el sistema informático que impidió a primera hora el que se pudiesen realizar operaciones de Caja en el ordenador, lo que obligó a su realización manual, por lo que el resultado de los datos, y a falta de otra prueba en contrario, también pudiera ser debido a ese fallo en el sistema informático.

Termina la sentencia recordando que, si bien es cierto que la presunción de inocencia opera en el ámbito del Derecho público sancionador, ello no significa que pueda declararse como procedente un despido, cuando no consta probada la conducta que lo causa. Una cosa es ser presumido inocente frente a ser o no presumido inocente, y otra que se pruebe la conducta de referencia.