XXX JORNADES CATALANES DE DRET SOCIAL

PROBLEMÁTICA DE LA UTILIZACIÓN DE LA PRUEBA DIGITAL EN EL ACTO DE JUICIO ORAL

Maria Dolores Pérez Martínez

Letrada de la Administración General de la Seguridad Social

INTRODUCCIÓN

En el procedimiento laboral es ya frecuente la aportación de pruebas o evidencias de origen digital o electrónico con el fin de acreditar hechos o incumplimientos laborales cometidos tanto por los trabajadores como por las propias empresas, denominándose por ello prueba digital. La mayoría de las prestaciones laborales se desarrolla en entornos digitales, ya sea a través de la generación, almacenamiento y tratamiento de la información digital (software, servidores informáticos, archivos digitales, *log*, etc.), ya sea a través del uso de sistemas de comunicación electrónica (correo electrónico, *sms*, aplicaciones de mensajería instantánea, como *Line*, *WhatsApp*, *Yahoo Messenger*, chats, etc.).

La duda es si este tipo de pruebas o evidencias digitales tienen suficiente amparo normativo en nuestro ordenamiento jurídico para considerarlas válidas y eficaces como medio de prueba en un juicio, y en caso de ser así, cuál será la forma correcta de aportar judicialmente estos documentos electrónicos, como acreditar su validez y que valor probatorio pueden adquirir en el procedo judicial.

NORMATIVA RELACIONADA CON LA PRUEBA DIGITAL

Con carácter previo a analizar el concepto de evidencia o prueba digital, debemos partir de la definición que nos ofrece de "***documento electrónico***" el **artículo 3 de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica**, por la cual, se considerará "*documento electrónico la información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado*".

Asimismo la nueva Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los derechos digitales, regula materias directamente

relacionadas con la prueba digital, al incidir en su artículo 6 en el consentimiento del afectado en la utilización de sus datos personales.

En el derecho a la intimidad en el uso de los dispositivos digitales en el ámbito laboral, al fijar en su artículo 87.2 que el empleador podrá acceder a los contenidos derivados del uso de medios digitales facilitados a los trabajadores a los solos efectos de controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la integridad de dichos dispositivos, debiendo establecer criterios de utilización de los dispositivos digitales respetando en todo caso los estándares mínimos de protección de su intimidad de acuerdo con los usos sociales y los derechos reconocidos constitucional y legalmente y en su elaboración deberán participar los representantes de los trabajadores. El acceso por el empleador al contenido de dispositivos digitales respecto de los que haya admitido su uso con fines privados requerirá que se especifiquen de modo preciso los usos autorizados y se establezcan garantías para preservar la intimidad de los trabajadores, tales como, en su caso, la determinación de los períodos en que los dispositivos podrán utilizarse para fines privados. A tales efectos os trabajadores deberán ser informados de los criterios de utilización a los que se refiere este apartado.

Derecho de los trabajadores y los empleados públicos a la desconexión digital a fin de garantizar, fuera del tiempo de trabajo legal o convencionalmente establecido, el respeto de su tiempo de descanso, permisos y vacaciones, así como de su intimidad personal y familiar. Las modalidades de ejercicio de este derecho se sujetarán a lo establecido en la negociación colectiva o, en su defecto, a lo acordado entre la empresa y los representantes de los trabajadores.(Art. 88 LO 3/2018).

Derecho a la intimidad frente a uso de dispositivos de videovigilancia y de grabaciones de sonido en el lugar de trabajo, que el empleador utilice en las funciones de control prevista en el artículo 20.3 del ET, siempre que se informe con carácter previo, y de forma expresa, clara y concisa, a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de esta medida. En ningún caso se admitirá la instalación de sistemas de grabación de sonidos ni de videovigilancia en lugares destinados al descanso o esparcimiento de los trabajadores o los empleados públicos, tales como vestuarios, aseos, comedores y análogos. Se admitirá únicamente cuando resulten relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo y siempre respetando el principio de proporcionalidad, el de intervención mínima y las garantías previstas legalmente.(Art. 89 LO 3/2018).

Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral, en el que con carácter previo, los empleadores habrán de informar de forma expresa, clara e inequívoca a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de la existencia y características de estos dispositivos. Igualmente deberán informarles acerca del posible ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión. (Art. 90 LO 3/2018).

Derechos a que en los convenios colectivos puedan establecer garantías adicionales de los derechos y libertades relacionados con el tratamiento de los datos personales

de los trabajadores y la salvaguarda de derechos digitales en el ámbito laboral. Art. 91 LO 3/2018).

PRUEBA DIGITAL COMO MEDIO DE PRUEBA EN LA JURISDICCIÓN SOCIAL

El art.90.1 de la Ley Reguladora de la Jurisdicción Social , regula la admisibilidad de los medios de prueba , disponiendo que las partes, previa justificación de la utilidad y pertinencia de las diligencias propuestas, podrán servirse de cuantos medios de prueba se encuentren regulados en la ley para acreditar los hechos controvertidos o necesitados de prueba, incluidos los procedimientos de reproducción de la palabra, de la imagen y del sonido o de archivo y reproducción de datos, que deberán ser aportados por medio de soporte adecuado y poniendo a disposición del órgano judicial los medios necesarios para su reproducción y posterior constancia de autos.

Debiendo aportar a la vista oral los soportes multimedia y medios de reproducción para hacer efectiva la prueba (art. 90 LRJS, art. 384.1 LEC) "medios, procedimientos o instrumentos que permitan archivar, conocer y reproducir la información digital" (arts. 299.2 y 384.3 LEC).

El art. 90.2 de la misma norma procesal añade que no se admitirán pruebas que tuvieran su origen o que se hubieran obtenido, directa o indirectamente, mediante procedimientos que supongan violación de derechos fundamentales o libertades públicas . Esta cuestión podrá ser suscitada por cualquiera de las partes o de oficio por el tribunal en el momento de la proposición de la prueba, salvo que se pusiese de manifiesto durante la práctica de la prueba una vez admitida. A tal efecto, se oirá a las partes y, en su caso, se practicarán las diligencias que se puedan practicar en el acto sobre este concreto extremo, recurriendo a diligencias finales solamente cuando sea estrictamente imprescindible y la cuestión aparezca suficientemente fundada. Añade el precepto que contra la resolución que se dicte sobre la pertinencia de la práctica de la prueba y en su caso de la unión a los autos de su resultado o del elemento material que incorpore la misma, sólo cabrá recurso de reposición , que se interpondrá, se dará traslado a las demás partes y se resolverá oralmente en el mismo acto del juicio o comparecencia **,** quedando a salvo el derecho de las partes a reproducir la impugnación de la prueba ilícita en el recurso que, en su caso, procediera contra la sentencia.

A su vez, completa esta regulación el art.90.4 de la Ley Reguladora de la Jurisdicción Social al establecer que cuando sea necesario a los fines del proceso el acceso a documentos o archivos, en cualquier tipo de soporte, que puedan afectar a la intimidad personal u otro derecho fundamental, el juez o tribunal, siempre que no existan medios de prueba alternativos, podrá autorizar dicha actuación, mediante auto, previa ponderación de los intereses afectados a través del juicio de proporcionalidad y con el mínimo sacrificio, determinando las condiciones de acceso, las garantías de

conservación y aportación al proceso, obtención y entrega de copias e intervención de las partes o de sus representantes y expertos, en su caso.

La normativa citada no es sino desarrollo y determinación en el ámbito del proceso social de lo que establece el art. 11.1 de la LOPJ (RCL 1985, 1578, 2635) al disponer, tras indicar que en todo tipo de procedimiento se respetarán las reglas de la buena fe, que *"no surtirán efecto las pruebas obtenidas, directa o indirectamente, violentando los derechos o libertadas fundamentales"* . Como cabe observar en el ámbito del proceso laboral ya no es que se indique que no producen efecto las pruebas que hayan vulnerado derechos fundamentales, sino que incluso no deben admitirse esas pruebas**,** sin duda pensando el legislador que debe evitarse la contaminación del juez o magistrado que deba resolver el asunto si ha estado en contacto con un material probatorio que, en definitiva, vulnera los derechos fundamentales de los implicados en el proceso. Similar regulación se contiene en el art. 287 de la LEC (RCL 2000, 34, 962 y RCL 2001, 1892) .

La prueba digital además de estar sometida a las normas de pertinencia y utilidad prevista en los arts. 87.1 y 87.2 de la LRJS, art. 283 LEC, es decir referida a los hechos sobre los que no hubiere conformidad salvo en los casos en que la materia objeto del proceso esté fuera del poder de disposición de los litigantes, siempre que aquéllas sean útiles y directamente pertinentes a lo que sea el objeto del juicio y a las alegaciones o motivos de oposición previamente formulados por las partes en el trámite de ratificación o de contestación de la demanda, También deberá ajustarse al test de proporcionalidad, es decir, necesidad, proporcionalidad e idoneidad, desarrollado entre otras en la SSTCo 14/1984 i 201/2004-).

Sobre la admisión de la prueba digital es relevante hacer referencia a la sentencia del Tribunal Superior de Justicia de Galicia de 14 de diciembre de 2018 JUR 2019/35764 al establecer no procede inadmitir un medio de prueba por la ilicitud de un medio de prueba como el propuesto por vulneración de derechos fundamentales en el acto del juicio sin haber resuelto en la vista sobre la licitud o no del mismo con las garantías y trámites que prevé el citado art. 90.2 LRJS . Pues tal trámite del art. 90.2 LRJS para decidir sobre la licitud o no del medio de prueba permite a las partes formular alegaciones expresamente sobre tal particular, y, asimismo, la práctica de las diligencias que sean necesarias para resolver sobre tal extremo lo que, en su caso, podría incluso exigir el visionado en todo o parte tal grabación, pues en ocasiones puede resultar complicado determinar la licitud de un medio de prueba sin conocer su contenido; debiendo, por lo demás, de resolverse oralmente en la vista, cabiendo asimismo recurso de reposición también a resolver oralmente. La inadmisión del medio de prueba sin haber resuelto en la vista sobre la licitud daría lugar a retrotraer las actuaciones al señalamiento del acto de juicio, para su nueva celebración, sin perjuicio de que, en el mismo, en el caso de que así se alegue o lo estime necesario de oficio, proceda el magistrado de instancia, siguiendo los trámites del art. 90.2 LRJS , a resolver con libertad de criterio sobre la licitud o no del citado medio de prueba.

VALIDEZ PROBATORIA DE UNA EVIDENCIA DIGITAL

Los cuatro requisitos básicos para asegurar la validez probatoria de una evidencia digital son:

1.-La prueba electrónica se debe obtener de manera lícita.

2.-Se debe respetar el derecho a las comunicaciones, a la intimidad y a cualquier otro derecho fundamental.

3.-Hay que respetar la cadena de custodia de la prueba digital. Asegurar que las pruebas no han sido manipuladas durante el proceso de obtención, análisis y presentación.

4.-Cuando sea necesario probarse la autenticidad e integridad de la prueba electrónica por medio de un perito ingeniero en informática colegiado.

La autenticidad y la integridad del mensaje son dos conceptos distintos aunque íntimamente relacionados. El presupuesto de autenticidad del mensaje significa la concordancia del autor aparente con el autor real. Por su parte, la integridad del mensaje como presupuesto de admisibilidad se refiere a la concordancia de la copia, testimonio o certificación con el mensaje original.

No es necesaria la acreditación de la autenticidad ni de la integridad del mensaje cuando la prueba no ha sido impugnada por la parte contraria o cuando exista un acto de reconocimiento expreso de la conversación y de su contenido. Así se pronunció la Sentencia núm. 159/2014, de la Sección 3ª de la Audiencia Provincial de Córdoba de 2 de abril de 2014 (JUR 2014, 168647): "*es, además, llamativo que se impugne por la defensa dicha documental cuando el propio acusado ha llegado a reconocer en el acto del juicio (…) haber remitido uno de los mensajes de " WhatsApp*". En caso contrario, la carga de probarlo corresponderá a quien lo aporta. En tal situación, la jurisprudencia viene admitiendo diversos medios de prueba para acreditar la validez del mensaje.

La relevante Sentencia de la Audiencia Provincial de Córdoba de 2 de abril de 2014, admitió el Acta del Letrado de la Administración de Justicia sobre el contenido de los mensajes con su transcripción, y su correspondencia con el teléfono y con el número correspondiente.: "*el Secretario Judicial, según consta en la diligencia extendida por el mismo (…) procedió a la "transcripción xerográfica de los mensajes recibidos por doña Dolores en el terminal número NUM003 " Por tanto, (…) resulta que quien ostentaba la fe pública judicial, (…) dejó constancia de un hecho con trascendencia procesal. Nada hay que objetar a un acto consistente en reflejar, merced a una serie de fotocopias de las diversas pantallas del terminal presentado por la denunciante, determinados mensajes a través de "WhatsApp" asociados a un usuario con nombre "José Miguel", el del denunciado".*

La jurisprudencia también admite otros medios de prueba sobre la autenticidad como: (i) el acta notarial relativa al contenido de la conversación; (ii) la exhibición o cotejo con el otro terminal implicado (Sentencia núm. 143/2014 de la Sección Séptima de la Audiencia Provincial de Barcelona de 7 de mayo de 2014: "*dado que se trata de una*

conversación vía WhatsApp (…), la misma puede llegar a conocerse a través de ambos terminales. Y el Sr. Gustavo entregó el suyo voluntariamente y con carácter previo, incluso, a la solicitud de información a las compañías telefónicas"); y (iii) la práctica de una prueba pericial informática que acredite la autenticidad y el envío de los mensajes, la más adecuada para aquellos casos en que exista contradicción entre las partes en litigio (Sentencia núm. 51/2013 de la Sección 27ª de la Audiencia Provincial de Madrid de 23 de septiembre de 2013: "*no existiendo (…) prueba que avale su declaración, pues los mensajes (…) no han sido reconocidos por el acusado, ni se ha practicado sobre los mismos prueba pericial informática que acredite su autenticidad y su envío"*).

Lo expuesto anteriormente se refiere únicamente a la validez como medio de prueba y no a la trascendencia probatoria de su contenido. Así se pronunció la Sentencia núm. 486/2016, de la Sección 4ª de la Audiencia Provincial de Barcelona, de 6 septiembre de 2016: *"Este Tribunal considera que existen riesgos tales como el de la supresión de mensajes de WhatsApp de la secuencia de mensajes de una conversación, el de la incorporación de mensajes reenviados, etc. Y de ahí las cautelas en la incorporación al proceso como medio de prueba de este tipo de pruebas.*

Por lo tanto, una cosa es que las partes presenten la transcripción de unos presuntos mensajes y otra distinta es que la valoración del contenido de tales mensajes, para lo cual debe quedar acreditada, previamente, la realidad de la emisión y recepción de los mensajes por las partes, a cargo de la parte que presenta el medio de prueba. Además, de acuerdo con la Sentencia núm. 276/2017 de la Sección 4ª de la Audiencia Provincial de Valencia, de 25 abril de 2017: "*lo habitual será la valoración conjunta del material probatorio: no únicamente lo que resulte del contenido de los mensajes de WhatsApp, sino del resto de pruebas existentes y practicadas: declaraciones de las partes y testificales*".

La cadena de custodia aplicada a una prueba es el procedimiento mediante el cual se conserva la integridad física y lógica de una prueba. Esta conservación se extiende desde la identificación y recolección de la prueba, pasando por su registro y almacenamiento, su posterior traslado y el análisis final de la misma, hasta su destrucción (si procede).

Para que una cadena de custodia sea considerada válida como tal, un fedatario público debe atestiguar, mediante documento elevado a público, el estado de la prueba antes de su análisis, para que, una vez se haya producido éste, sea posible determinar que la prueba no ha sido contaminada y que su estado es el mismo que el anterior al análisis. En España, las únicas figuras de fedatarios públicos existentes son el notario y el Letrado de la Administración de la Seguridad Social. El fedatario únicamente puede dar fe y atestiguar el estado de una prueba cuando ésta llega a sus manos, pero no puede garantizar el estado de la misma antes de que ésta haya llegado a él ni por tanto que la prueba no haya sufrido modificaciones previas.

Se pondrán algunos ejemplos gráficos un ordenador incautado por la policía a un criminal y encendido antes de ser enviado al fedatario público ya no es una prueba en la que se pueda considerar que se haya conservado la cadena de custodia, puesto que el sistema operativo ya ha modificado y accedido a determinados ficheros.

Asimismo, aunque el ordenador no haya sido encendido, tampoco se podría garantizar "estrictamente" la conservación de la cadena de custodia si el fedatario no estaba presente en el momento de la incautación, puesto que cualquier fichero informático es susceptible de ser modificado mediante software, así como también pueden ser alterados los diversos registros existentes en el sistema operativo para aparentar que no ha habido accesos, por lo que, en principio, un ordenador aparentemente no encendido o un disco no accedido, en realidad, puede que sí lo fueran. Se entrecomilla la palabra *estrictamente* debido a que, cuando la Policía o la Guardia Civil incautan material informático y lo almacenan, aunque aún no se haya dado fe pública del contenido de los discos, en teoría sí se conserva a nivel judicial la cadena de custodia, debido a que el almacenaje se presupone seguro, de tal forma que nadie podría acceder, dentro de las dependencias policiales, al material incautado; pero, a nivel técnico estricto, si alguien muy experto lograse acceder a dicho material y alterarlo sin dejar huella, sería virtualmente imposible demostrar, en este último ejemplo, que el ordenador sí fue encendido o el disco accedido, por lo que la duda sobre la invalidez de la cadena de custodia ya estaría sembrada, siempre y cuando se pudiese demostrar que la custodia de la prueba no fue ortodoxa.

En conclusión para que se mantenga la cadena de custodia de una prueba informática, es siempre necesario que esté presente el fedatario en la incautación o intervención del material informático a los criminales, para realizar clonados públicos de los discos. Así, el fedatario público podrá dar fe del estado de la prueba en ese preciso instante.

Según indican los peritos informáticos colegiados, muchas veces se confunde el término "cadena de custodia" y se le asocia un significado de "no modificación de la prueba". Esto que, en un principio, pudiera parecer lo mismo, realmente no lo es. La conservación de la cadena de custodia siempre implica una no modificación de la prueba, pero una no modificación de la prueba, no implica que se pueda garantizar ante un Tribunal que se ha conservado la cadena de custodia. Por ejemplo, si un cliente le entrega a un perito un disco duro o un dispositivo móvil, el perito pondrá todo su empeño en la conservación de la cadena de custodia y en la no modificación de la prueba pero, si no eleva ante notario el estado de la prueba en el momento preciso de su entrega por parte del cliente, no se podrá garantizar ante un Tribunal que la mencionada cadena de custodia se haya conservado y, aun así, sólo se podrá garantizar la cadena de custodia desde que el cliente le entregó la prueba al perito, no antes. Esto quiere decir que, el cliente, por su cuenta, podría haber modificado la prueba para "colocar" o "retirar" de la misma las evidencias que le interesen, con o sin la ayuda de expertos. Será labor, en este caso, del perito informático, determinar y plasmar en el informe pericial, tras el análisis de la prueba, qué posibilidades hay de que esto haya sido posible teniendo en cuenta la dificultad inherente a la eventual alteración de las pruebas. Por ejemplo, no es lo mismo encontrarse una fotografía o vídeo comprometidos dentro de un disco duro en el que no se ha conservado la cadena de custodia (algo relativamente sencillo de realizar para alguien con unos conocimientos informáticos mínimos, puesto que sólo tiene que colocar el archivo en el disco), que un correo electrónico comprometido, enviado o recibido, que se encuentre

borrado dentro de un fichero de carpetas personales (algo con una complejidad más elevada).

Para garantizar la cadena de custodia debería haber un protocolo informático, en el este: Estén presentes los representantes de los trabajadores, el trabajador afectado o notario, perito o testigo acreditado que lo ratifique. Extraer el disco duro de la terminal ante Notario, con precinto y depósito en la Notaría Pericial informática, copia del disco duro ante Notario y traslado de la copia al laboratorio informático para analizar los resultados (algoritmos y conclusiones periciales s/palabras clave ciegas) sin control de emisor/destinatario del e-mail.

Sobre la copia del disco duro original, que se precinta notarialmente y se le da un número sólo se debe permiten rescatar lo que interesa (STS 8.2.018, Social, u.d. 1121/2015).

MEDIOS DE PRUEBA DIGITAL

La evidencia digital se puede aportar al proceso, de acuerdo con las normas procesales de admisión de prueba **(**arts. 90 y ss. LRJS**),** como un documento privado o mediante un documento público, en función del origen e intervención en el propio documento; a través de la aportación de un informe pericial de expertos; o también mediante la constatación directa del propio Juzgado a través del denominado reconocimiento judicial, si bien, como veremos, no todas estas fórmulas tendrán el mismo valor probatorio quedando su valoración sometida a las reglas de la sana crítica del juez.

Por lo tanto, la evidencia digital, dentro del proceso judicial incluye cualquier información, documento, archivo o dato, almacenado en un soporte electrónico y susceptible de poder ser tratado e identificado digitalmente para su posterior aportación en un proceso judicial**.**

La prueba “electrónica” puede ser practicada mediante la aportación como un mero **documento privado**, como la impresión directa del equipo informático particular sin la intervención de un fedatario público, o la impresión de un correo electrónico o el pantallazo de un *WhatsApp*. Aunque, esta forma puede generar dudas sobre su autenticidad y en consecuencia disminuir su valor probatorio obligando al Juez a valorar esa prueba en conjunto con el resto del ramo probatorio presentado por las partes como puede ser el propio interrogatorio de la parte o declaraciones de otros testigos (STSJ Madrid, Sala de lo Social, 10-6-15, Rec. 817/2014), o incluso puede llevar a denegar su consideración como documento en sí mismo (STSJ Galicia, Sala de lo Social, 28-1-16, Rec. 4577/2015).

El documento electrónico es prueba documental en formato electrónico cuya firma acredita al autor, no el contenido según el reglamento UE 910/2014. por lo que la constatación de hechos digital debe acreditarse por prueba pericial, porque no cualquier "captura" de imagen o impresión de email o whatsapp es válida si se impugna de contrario (art. 90.1 lrjs, lec arts. 299.2 y 382 a 384, valoración sana crítica –art. 382.3 lec-)

En lo que respecta a la posibilidad de impugnación de los documentos privados presentados, una vez aportado el documento en la fase probatoria del juicio, y en el supuesto de que alguna de las partes dude sobre su autenticidad o integridad deberá impugnarlo y proponer prueba sobre su autenticidad a través del llamado *cotejo pericial de letras*. En la práctica es habitual manifestar la falta de reconocimiento del documento por la parte que no lo ha propuesto, ya que el reconocimiento expreso tiene el valor de plena prueba en el proceso, tanto del contenido como de la fecha e identidades que constasen en dicho documento reconocido por ambas partes. Igualmente si el documento no es impugnado expresamente la valoración judicial suele tender a presumir su autenticidad salvo prueba en contrario (*iuris tantum*).

A diferencia de los documentos privados, los **documentos públicos** a priori no son susceptibles de impugnación salvo que se tenga la seguridad de que sea una falsificación, en cuyo caso se solicitará su cotejo con el original (matriz notarial si se trata de una escritura pública) o bien la ratificación del funcionario que intervino el documento.

Si se opta por incorporarlo a un documento público, dicha aportación se podrá efectuar mediante un acta notarial (**fe pública notarial**) en la cual se constatará por el Notario (fedatario público) la existencia de dichos mensajes, otorgando fe pública del acceso a la cuenta de correo o del dispositivo móvil donde esté instalada la aplicación de mensajería, y procediendo a imprimir los mensajes elegidos incorporándolos finalmente al acta notarial. En el acta de protocolización de los mensajes además se incluirá la dirección de correo electrónico o el número de teléfono desde los que se hayan enviado o recibido los mensajes, las fechas de los referidos mensajes, así como las identidades de los intervinientes que figuren en los textos protocolizados.

El mismo valor probatorio de documento público tendrán las diligencias de constancia realizadas en el propio Juzgado a petición de los interesados (**fe pública judicial**). En este caso, será el Letrado de la Administración de Justicia (anteriormente el Secretario Judicial) el que levante acta del contenido del concreto correo electrónico o mensaje de *WhatsApp*, identidades que figuren en dichos mensajes, así como del dispositivo móvil utilizado.

Adicionalmente a las anteriores fórmulas de aportación de pruebas electrónicas, y como un plus de garantía de autenticidad y no manipulación, se presenta la posibilidad de practicar una **prueba pericial informática** sobre el contenido de los mensajes electrónicos, y en general sobre cualquier otro contenido almacenado digitalmente, como pueden ser ordenadores, dispositivos móviles, páginas webs, redes sociales o similares.

En este caso el trabajo del perito informático consistirá principalmente en el desarrollo de procedimientos encaminados a “preservar” las evidencias digitales que se puedan derivar del contenido electrónico que se pretenda aportar en juicio. Esta preservación se obtiene a través de la realización de copias forenses “exactas” de la información digital almacenada dando lugar a un código alfanumérico de dicha información (código *hash*). Dicha copia se realiza por duplicado, depositando una de ellas ante Notario, y quedando la segunda copia en poder del perito para su posterior análisis técnico. Las técnicas utilizadas en este análisis suelen ser de carácter selectivo, es decir, sólo se

busca aquella información que resulte necesaria para la investigación, a través, por ejemplo, de búsquedas “ciegas”, evitando con ello posibles injerencias en datos o informaciones de carácter íntimo o privado del trabajador investigado.

Finalmente los resultados de la investigación se trasladarán a un informe pericial técnico que será el que se aporte en juicio. Es frecuente en la práctica que acuda el perito el día del juicio para ratificar el informe evitando con ello posibles impugnaciones de la parte contraria.

Para finalizar, me parece de utilidad exponer los criterios que actualmente están aplicando los tribunales para considerar válida la aportación judicial de la prueba de mensajería instantánea, en particular la referida a la prueba de mensajes de *WhatsApp*. Siguiendo las consideraciones efectuadas por el Tribunal Superior de Justicia de Galicia en su reciente sentencia de 28 de Enero de 2016, mencionada anteriormente, y en lo que respecta a los “pantallazos”, para “*considerar una conversación de WhatsApp como documento –a los fines del proceso laboral–, sería preciso que se hubiese aportado no sólo la copia en papel de la impresión de pantalla o, como se denomina usualmente, <<pantallazo>> –que es lo único que cumple el actor–, sino una transcripción de la conversación y la comprobación de que está se corresponde con el teléfono y con el número correspondientes. Esto podría haber conseguido a través de la aportación del propio móvil del Sr. Abel y solicitando que, dando fe pública, el LAJ* [actual Letrado de la Administración de Justicia] *levante acta de su contenido, con transcripción de los mensajes recibidos en el terminal y de que éste se corresponde con el teléfono y con el número correspondiente; o, incluso, mediante la aportación de un acta notarial sobre los mismo extremos*”.

En definitiva, como señala el Tribunal, para que se pueda aceptar como documento una conversación o mensaje de este tipo (algo diferente de su valor probatorio) se establecen cuatro supuestos: a) cuando la parte interlocutora de la conversación no impugna la conversación; b) cuando reconoce expresamente dicha conversación y su contenido; c) cuando se compruebe su realidad mediante el cotejo con el otro terminal implicado (exhibición); o, finalmente, d) cuando se practique prueba pericial que acredite la autenticidad y envío de la conversación, para un supuesto diferente de los anteriores.

En conclusión**,** la elección de la fórmula concreta de presentación o aportación de una prueba digital, por otro lado extremadamente usual en nuestros días, será capital la hora de acreditar con visos de seguridad y fiabilidad los hechos y/o la información que puedan estar almacenados en cualquier tipo de soporte digital, y cometer un error en esta fase de preparación de la prueba puede marcar definitivamente el éxito o fracaso en un proceso judicial.

En cuanto a la aportación como medio de prueba de los soportes digitales es relevante la sentencia del Tribunal Superior de Justicia de Asturias,núm. 2530/2017 de 14 noviembre que valora la eficacia probatoria a los correos electrónicos e incluye en la crítica los archivos digitales del ordenador a los que accedió la empresa con la ayuda del perito. Afirma que por sus características como archivos digitales o documentos electrónicos tienen el mismo valor en el proceso judicial que los documentos privados y la sentencia procedió a valorar los correos y archivos digitales como partes de un

conjunto más amplio de fuentes de convicción y esta actividad,, constituye una correcta manifestación de las amplias facultades reconocidas a la Juzgadora de instancia en la legislación procesal y no vulnera los límites de la función encomendada, que no le exigen una exposición exhaustiva sobre cada uno de los medios de prueba por separado. Además, aun los documentos privados no autenticados pueden constituir medios probatorios eficaces y en este sentido el Art. 326.2 párrafo segundo de la LEC establece que cuando no se pudiere deducir su autenticidad o no se hubiere propuesto prueba alguna al respecto, el tribunal valorará el documento privado conforme a las reglas de la sana crítica.

En cuanto a la valoración de los soportes digitales como un medio de prueba la sentencia de la Audiencia Provincial de Burgos núm. 169/2018 de 4 abril. JUR 2018\186525 también hace referencia a la valoración directa del juez al indicar que como recuerda la STS 7/2014, de 22 de enero (RJ 2014, 887) , "carece de sentido cuestionar la autenticidad de las voces y echar en falta una prueba pericial que asegure la autenticidad de lo grabado. Conviene tener presente -decían las SSTS 75/2012, 28 de septiembre , 412/2011, 11 de mayo (RJ 2011, 3749) y 593/2009, 8 de junio (RJ 2009, 4710) , entre otras- que la validez de las escuchas telefónicas no exige como presupuesto constitutivo el aval de un informe pericial que dictamine acerca de la coincidencia entre la voz registrada y la de aquella persona a la que esa voz se atribuye por la investigación. La posibilidad de alcanzar una convicción judicial sin necesidad de un dictamen pericial previo ha sido ya defendida por la jurisprudencia de esta Sala (cfr. STS 1286/2006, 30 de noviembre (RJ 2007, 446)), que también ha proclamado la no exigencia, con carácter general, de una comparecencia previa al juicio oral, con la correspondiente audición, con el fin de que los imputados pudieran reconocer o negar como propia la voz que había sido objeto de grabación (cfr. STS 537/2008, 12 de septiembre (RJ 2008, 6954)). Es cierto que el órgano de enjuiciamiento no puede albergar duda alguna respecto de la autenticidad y la atribuibilidad de las voces. Pero su convicción no tiene por qué obtenerse necesariamente mediante el formato de una pericial o una comparecencia previa de audición". La falta de iniciativa procesal a la hora de aportar cualquier elemento probatorio que pudiera respaldar su reproche, obligan a rechazar tal línea argumental. Más el TS en Auto de inadmisión del recurso de casación de 26 de marzo de 2016 afirma en correspondencia a lo aquí acontecido que "..a mayor abundamiento, en las sentencias de esta Sala con referencia 406/2010 y 210/2012 , hemos dicho que cuando el material de las grabaciones está a disposición de las partes, que bien pudieron en momento procesal oportuno solicitar dicha prueba y no lo hicieron, reconocieron implícitamente su autenticidad, sin olvidar, se reitera, que la identificación de la voz de los acusados puede ser apreciada por el Tribunal en virtud de su propia y personal percepción y por la evaluación ponderada de las circunstancias concurrentes.

PELIGROS DE LA MANIPULACIÓN DE LA PRUEBA DIGITAL

En Google “Play Store” tenemos a nuestro alcance y de forma gratuita aplicaciones como “WHATSFAKE” o “FAKE CHAT”. Estas App permiten sustituir o suplantar una conversación real de WhatsApp". Un pantallazo, es una imagen que cualquiera podría modificar con Photoshop o cualquier otro programa de edición de imágenes. Así que no parece que sea una prueba sólida la presentación de un pantallazo de una conversación de whatsapp como medio de prueba en juicio.

La autenticidad del contenido es complicada, pues hay aplicaciones para su modificación (WhatsApp Toolbox, Fake SMS Sender, etc.). La STS, Sala Penal, 19.5.2015 (rec. cas. 2387/2014) dice: «la impugnación de la autenticidad de cualquiera de esas conversaciones, cuando son aportadas a la causa mediante archivos de impresión, impresión, desplaza la carga de la prueba hacia quien pretende aprovechar su idoneidad probatoria» (pericial sobre el origen, destinatarios i contenido) "La posibilidad de una manipulación de los archivos digitales mediante los que se materializa ese intercambio de ideas, forma parte de la realidad de las cosas" STSJ Aragón de 23 junio 2014.

DESARROLLO JURISPRUDENCIAL DE LA PRUEBA DIGITAL

1.-DVD, CD, DISCO DURO, USB, tablet.

Es importante para la constitución como medios de prueba de estos soportes electrónico que los mismo tengan la firma electrónica con certificado de entidad reconocida (Ley 59/2003 y art. 326.3 LEC). No son documentos electrónicos los e-mails sin firma electrónica. Dado que el correo electrónico necesita de un soporte informático (ordenador, tablet, etc.), accederá al proceso normalmente por medio de copia impresa, pero nada impide el reconocimiento judicial del soporte en el acto de la vista, acompañando transcripción (art. 384 LEC). A fin de dar validez a los documentos con firma electrónica con certificado de la entidad la impugnación temeraria de la firma digital podrá llevar aparejada, a criterio del Juez, multa de 120 a 600 €.

En cuanto a la plasmación documental de esta prueba digital la sentencia núm. 2658/2017 de 21 noviembre. AS 2017\2186 del Tribunal Superior de Justicia de Asturias valora que un reportaje fotográfico plantea varios problemas. Las fotografías que contiene, en realidad fotocopias de imágenes impresas en papel obtenidas a partir de archivos digitales, no son documentos en sentido estricto, pues en éstos la escritura ha de ser la única o al menos la principal forma de representación, como se desprende de los arts. 265 y siguientes, 273 a 280, 299, 300, 317 a 323 y 333 de la Ley de Enjuiciamiento Civil (RCL 2000, 34) y 1216 a 1224 y 1225 a 1230, excepto el derogado 1266, del Código Civil (LEG 1889, 27) . Las fotografías presentadas son medios de reproducción de imágenes y por eso están comprendidos en el art. 299.2 de la Ley de Enjuiciamiento Civil , en apartado distinto a los documentos (art. 299.1 LEC). En el recurso de suplicación no son medios de prueba con aptitud para modificar las premisas fácticas de la sentencia [art. 193 b) y 196.3 LJS].

Los denominados documentos electrónicos y su regulación en la Ley 59/2003, de 19 de diciembre (RCL 2003, 2975) , de firma electrónica, justifican las dudas sobre si puede mantenerse el concepto estricto y clásico de documento antes indicado. Pero, en cualquier caso, para la toma en consideración de las fotografías no bastaría con la aportación de la imagen impresa en papel, sino que deberían figurar incorporados, y no lo están, los archivos digitales de los que se obtuvo la impresión en papel, sin los cuales falta el soporte imprescindible para su valoración como medio de prueba.

2.- En cuanto a las **PÀGINAS WEBS**, se ha admitido el correo electrónico impreso como prueba documental y, por ende, con valor para la revisión fáctica en suplicación, lo que constituye un acicate a su impresión, salvando así el obstáculo que para el acceso al recurso de suplicación presentan los medios de reproducción de sonido o imagen o la prueba de instrumentos de los arts. 382 a 384 LEC", STSJ de Aragón 822/2010, de 17 de noviembre [AS 2011\136]. "La página web puede ser una modalidad de prueba electrónica consistente en un documento informático al que se puede acceder por vía de internet previa identificación de un enlace". Base jurídica: art. 384 LEC (ejemplo, "capturas" o "pantallazos" reconocidos). En vía penal se consideran como documentos privados (Facebook, WhatsApp, Twitter o Skype), pero en vía laboral son prueba de instrumentos según parte de la doctrina judicial (90.4 LRJS i 384 LEC).

Los videos en Facebook colgados por una trabajadora, de forma accesible a terceros, como prueba lícita: STSJ Castilla-León 30.4.2014 (R. 491/2014). Una trabajadora colgó en su perfil de Facebook dos vídeos obtenidos de la cámara de seguridad de la tienda donde prestaba servicios como encargada, en los que se refleja la caída al suelo de dos cajeras, lo que provocó comentarios jocosos de otros usuarios. Fue despedida por tal conducta, medida que el Juzgado de lo Social calificó de procedente. En suplicación, suplicación, la trabajadora denuncia que la decisión judicial se basa en una prueba obtenida con vulneración de su derecho fundamental a la protección de los datos personales. La sentencia desestima el recurso, argumentando 1.º) que las imágenes no eran propiedad de la actora, sino de la empresa, y 2.º) que la demandante las difundió en una red social accesible, en el que no consta que exista un control de seguridad al efecto, posibilitando así que las viesen una pluralidad de personas, alguna de las cuales las hizo llegar a la empresa, y perjudicando el derecho al honor y a la intimidad de sus compañeras.

Los contenidos en twitter(impreso, es prueba documental): aceptado en casos de extinción por vía del artículo 50 ET por mobbing (STSJ de Galicia 26.9.2013, AS 2013\2948); indicio en procesos de vulneración de DF(STSJ de Cataluña 29.4.2013, AS 2013\2994); despidos (STSJ de Madrid 26.1.2015, JUR 2015\7398). "No se considera vulnerada la intimidad de la trabajadora al haber sido obtenidas las fotografías de páginas de Facebook sin necesidad de utilizar clave ni contraseña alguna" (STSJ de Asturias 14.6.2013, JUR 2013\245751).

No tiene la misma trascendencia una opinión vertida en un perfil de acceso libre o público que otra realizada en un perfil cerrado o de acceso restringido (STSJ Andalucía-Málaga 22.5.2014, Rº 509/2014, despido por insultos y amenazas vs. otra compañera vía facebook en perfil abierto –muro-); o por el número de «amigos» o «seguidores» que tenga el usuario, en la medida en que incide en el eventual comentario, suele ser objeto de valoración, cuando se trata de críticas sobre la empresa (STSJ Navarra 21.2.2014, Rº. 44/2014, improcedencia de un despido porque a pesar de que la cuenta tenía acceso libre, no se constata la repercusión de los comentarios, habida cuenta del (escaso) número de seguidores en twitter que tenía el autor, parecido criterio en STSJ Madrid 10.3.2015, Rº 919/2014).

3.- WHATSAPP y CORREO ELECTRONICO: "Para que una conversación de Whatsapp tenga plena validez ante un juez, debe estar certificada y autentificada, por

lo que necesita ser aportada con prueba pericial que identifique el origen real de la conversación, la identidad de los interlocutores y la integridad del contenido

Un perito informático se encarga de 1) extraer conversaciones originales de Whatsapp (o cualquier otra aplicación), 2) certificar y 3) custodiar la cadena de custodia.

En este sentido debe traerse a colación la sentencia 2047/2015 de 19-5-15, que aunque es de la Sala de lo Penal del Tribunal Supremo es trasportable a la jurisdicción social. Según la mencionada sentencia: "una prueba de comunicación bidireccional mediante cualquiera de los múltiples sistemas de mensajerías instantánea debe ser abordada con todas las cautelas. La posibilidad de manipular los archivos digitales mediante los que se materializa ese intercambio de ideas, forma parte de la realidad de las cosas. El anonimato que autorizan tales sistemas y la libre creación de cuentas con una identidad fingida, hacen perfectamente posible aparentar una comunicación en la que un único usuario se relaciona consigo mismo. De ahí que la impugnación de la autenticidad de cualquiera de las conversaciones, cuando son aportadas a la causa mediante archivos de impresión, desplaza la carga de la prueba hacia quien pretende aprovechar su idoneidad probatoria. De modo que será indispensable la práctica de una prueba pericial que identifique el verdadero origen de esa comunicación, la identidad de los interlocutores y la integridad de su contenido".

Los mensajes WhatsApp pueden ser prueba en el procedimiento como muestra la siguientes sentencias: STSJ Cantabria de 18 junio 2014 que confirma la sentencia de instancia y declara procedente el despido de un conductor de autobús que enviaba mensajes de WhatsApp mientras conducía, STSJ Galicia de 25 abril 2014 en la que se indica que no vulnera el derecho al secreto de las comunicaciones de una empleada (despedida) la utilización por parte de la empresa de la transcripción de una conversación de WhatsApp, llevada a cabo entre la recurrente y una interlocutora que era compañera de trabajo, pues el mencionado secreto no rige entre los comunicantes, dado que fue la otra trabajadora la que informó a la empresa de su contenido, STSJ Cataluña de 15 julio 2014 que declara la nulidad de actuaciones por no haber sido admitida por el Juzgador de Instancia, la "prueba documental" consistente en la reproducción de varias conversaciones de WhatsApp, STSJ La Rioja 22.1.2016: la entrega de los Whatsapp a la empresa por un compañero de trabajo receptor de éstos, no vulnera el secreto de las comunicaciones (no hay secreto para aquel a quien se dirige la comunicación) “la difusión a terceros por parte de una de las partícipes en el chat de Whatsapp del contenido de los mensajes, no vulnera el derecho fundamental al secreto de las comunicaciones” (STSJ Andalucía 22.11.2017) STSJ Galicia 28.1.2016, rec. 4577/2015 (conversaciones apps y redes sociales): para considerar una conversación WhatsApp como documento —a los fines del proceso laboral—, sería preciso que se hubiese aportado no sólo la copia en papel de la impresión de pantalla o, como se denomina usualmente, “pantallazo”, sino una transcripción de la conversación y la comprobación de que ésta se corresponde con el teléfono y con el número correspondientes o cuando la parte interlocutora de la conversación no la impugna o cuando la reconoce expresamente o bien cuando se compruebe su realidad mediante el cotejo con el otro terminal implicado (a través de la exhibición) y la sana crítica o también cuando una pericial acredita la autenticidad y el envío de la conversación o por último aportar el terminal al letrado de la Administración

de Justicia o un notario para que levante acta de su contenido, los números de teléfono involucrados y la hora y la fecha de la conversación.

En relación a los correos electrónicos, como medios de prueba, es imprescindible hacer mención a la Sentencia de 5 septiembre 2017 del TEDH 2017\61 Caso Barbulescu contra Rumania, en aplicación del art. 8 del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, en la que se establece que para dar valor probatorio a estos correos es necesario comprobar concretamente, si el empleador ha notificado previamente al demandante la posibilidad de que sus comunicaciones en *Yahoo Messenger* van a ser controladas y, por otro, haberle informado de la naturaleza y alcance de la vigilancia a que a la que va a ser sometido, así como del grado de intrusión en su vida privada y en su correspondencia. Por otra parte fijar qué motivos concretos justifican la introducción de las medidas de control, en segundo lugar, si el acceso al contenido de las comunicaciones sería posible sin su conocimiento.

Tras dicha sentencia el Tribunal Supremo dicto sentencia núm. 119/2018 de 8 febrero. RJ 2018\666 en la que manifestaba su conformidad con la bases sentadas en la referida sentencia del TEDH, pero haciendo los siguientes matices: “Consideremos, finalmente, que «se examinó el contenido de ciertos correos electrónicos de la cuenta de correo corporativo del actor, pero no de modo genéricos e indiscriminado, sino tratando de encontrar elementos que permitieran seleccionar que correos examinar, utilizando para ello palabras clave que pudieran inferir en qué correos podría existir información relevante para la investigación, [y atendiendo a la] proximidad con la fecha de las transferencias bancarias» [así, en la fundamentación jurídica de la sentencia de instancia, pero con valor de HDP: recientes, SSTS 02/06/16 -rco 136/15 (RJ 2016, 4879) -; 22/06/16 -rco 250/15 (RJ 2016, 2946) -; y SG 26/10/16 (RJ 2016, 5448) -rcud 2913/14 -]; y sin que deje ser relevantes dos circunstancias: a) que el contenido extraído se limitó a los correos relativos a las transferencias bancarias que en favor del trabajador le había realizado -contrariando el Código de Conducta- un proveedor de la empresa; y b) que -además y según se indica en la misma resolución del J/S- el control fue ejercido sobre el «correo corporativo del demandante, mediante el acceso al servidor alojado en las propias instalaciones de la empresa; es decir, nunca se accedió a ningún aparato o dispositivo particular del demandante...; a lo que se accedió es al servidor de la empresa, en la que se encuentran alojados los correos remitidos y enviados desde las cuentas corporativas de todos y cada uno de los empleados».

Siendo ello así , no cabe duda: a).- Que el hallazgo «casual» de la referida prueba documental excluye la aplicación de la doctrina anglosajona del «fruto del árbol emponzoñado», en cuya virtud al juez se le veda valorar no sólo las pruebas obtenidas con violación de un derecho fundamental, sino también las que deriven de aquéllas (sobre ello, SSTC 98/2000, de 10/Abril (RTC 2000, 98) ; 186/2000, de 10/Julio (RTC 2000, 186) ; 29/2013, de 11/Febrero (RTC 2013, 29) ; y 39/2016, de 3/Marzo (RTC 2016, 39) . Y SSTS 05/12/03 (RJ 2004, 313) -rec. 52/03 -; 07/07/16 -rcud 3233/14 (RJ 2016, 4434) -; SG 31/01/17 (RJ 2017, 1429) -rcud 3331/15 -; y 20/06/17 (RJ 2017, 3195) -rcud 1654/15 -); b).- Que la clara y previa prohibición de utilizar el ordenador de la empresa para cuestiones estrictamente personales nos lleva a afirmar -como hicimos en uno de nuestros precedentes- que «si no hay derecho a

utilizar el ordenador para usos personales, no habrá tampoco derecho para hacerlo en unas condiciones que impongan un respeto a la intimidad o al secreto de las comunicaciones, porque, al no existir una situación de tolerancia del uso personal, tampoco existe ya una expectativa razonable de intimidad y porque, si el uso personal es ilícito, no puede exigirse al empresario que lo soporte y que además se abstenga de controlarlo» (STS SG 06/10/11 (RJ 2011, 7699) -rco 4053/10 -); c).- Que el ponderado examen del correo electrónico que se ha descrito en precedente apartado, utilizando el servidor de la empresa y parámetros de búsqueda informática orientados a limitar la invasión en la intimidad, evidencia que se han respetado escrupulosamente los requisitos exigidos por la jurisprudencia constitucional y se han superado los juicios de idoneidad, necesidad y proporcionalidad.”.

4.-VIDEOVIGILANCIA

En materia de video vigilancia, debido a la escasa regulación legal se ha producido jurisprudencia vacilante.

La STCo 39/2016, 3-3, donde se indica que es suficiente con “distintivos” de zona video vigilada en los centros de trabajo (Instrucción AEPD 1/2006) para que los mismos sean admitidos o la STCo 29/2013 y SSTS 31 . 1 .2017, u . d . 3331/2015 i 2.2.2017, u.d. 554/2016 más exigentes en la que se requiere de información previa de uso “laboral” de las imágenes, proporcionalidad, necesidad, idoneidad.

La STSJ MADRID 25.1.2019 (rec. 971/2018 exige que la instalación de cámaras de seguridad es una medida justificada por razones de seguridad (control de hechos ilícitos imputables a empleados, empleados, clientes y terceros), terceros), apta para el logro de ese fin y necesaria y proporcionada al fin perseguido, razón por la que estaba justificada la limitación de los derechos fundamentales en juego, máxime cuando tal y como consta acreditado la representación legal de los trabajadores tiene pleno conocimiento de la instalación del sistema de vigilancia, así como que se informa a toda la plantilla en el sistema de información de la empresa y se expuso en los tablones de anuncios de los centros de trabajo.

La STEDH 28.11.2017 – asunto NEVENKA ANTOVIC y JOVAN MIRKOVIC vs. UNIVERSIDAD DE MONTENEGRO (School of Mathematics) sobre monitorización de clases (“anfiteatros anfiteatros”) con cámaras de video vigilancia (camera surveillance) no justificada ni proporcionada en las que se vulnera vida privada e intimidad de los dos profesores (art. 8 CEDH).

SI una empresa quiere instalar cámaras de video vigilancia, debe informar a sus trabajadores de ello (si la cámara se instala de modo permanente y/o prolongado) SSTSJ Cataluña 19.2.2018, rec. 6637/2017 y 16.3.2018, rec. 154/2018, STSJ Granada 10.10.2018, rec. 2260/2017, STSJ Madrid 28.9.2018, rec. 275/2018—) y de la existencia de un fichero con datos de carácter personal (la imagen lo es), así como de que las grabaciones podrán ser utilizadas para justificar un incumplimiento (transparencia informativa); Si la cámara sólo se instala durante pocos días (los necesarios para confirmar la sospecha previa) y sólo graba alrededor del puesto de trabajo (sin grabar a nadie más ni en lugares controvertidos), puede defenderse la proporcionalidad, idoneidad y necesidad de la medida.

STSJ Galicia 24.7.2018 (rec. 993/2018) declara la ilicitud de la prueba video gráfica obtenida porque, aunque un conductor de autobús despedido (siendo calificado de nulo el despido) conociera la implantación de cámaras de seguridad, no se le había informado las características y alcance del tratamiento de los datos obtenidos, es decir, cuándo podían ser examinadas las grabaciones, durante cuánto tiempo y con qué propósitos, sin explicación concreta del posible uso sancionador disciplinario de incumplimientos laborales.

La STSJ Asturias 22.1.2019 (rec. 2361/2018), indica que “la instalación de una sistema de grabación de esa naturaleza no queda a la conveniencia de la empresa ni puede justificarse sólo por la circunstancia de tener atribuida la facultad de dirección y control del cumplimiento del contrato de trabajo, pues en la medida que supone una injerencia en el ámbito de derechos fundamentales de la trabajadora, debe cumplir rigurosamente los requisitos que habilitan para afectar esa esfera protegida de la trabajadora”, añade que “la grabación y visionado de las imágenes de la de demandante e n el puesto de trabajo es una prueba inadmisible, que no puede surtir efectos – art. 11.1 LOPJ y 90.2 LRJS-”, pero al ser la única prueba en que la empresa basó el despido acordado, indica que el mismo debe calificarse como improcedente “sobre la base de la ineficacia de la grabación como prueba de cargo y la inexistencia de otras pruebas acreditativas de los incumplimientos laborales imputados en la carta de despido ”.

La grabación de sonidos en el lugar de trabajo, se admitirá únicamente cuando resulten relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo y siempre respetando el principio de proporcionalidad, el de intervención mínima y las garantías legales. Los datos serán suprimidos en el plazo máximo de un mes desde su captación, salvo cuando hubieran de ser conservados para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones, en cuyo caso las imágenes deberán ser puestas a disposición de la autoridad competente en un plazo máximo de setenta y dos horas desde que se tuviera conocimiento de la existencia de la grabación. SJS 3 Pamplona 18.2.2019 (SJS 3 Pamplona 18.2.2019 (Roj: SJSO 281/2019, JUR 2019\80406) .

Para intentar resumir la doctrina del TS, TCo y TEDH sobre video vigilancia, me remito a la valoración conjunta que realiza el Juzgado de lo Social núm. 3 de Pamplona (Comunidad Foral de Navarra)Sentencia núm. 52/2019 de 18 febrero. AS 2019\1014, al analizar la evolución de la jurisprudencia en esta materia "Fijando los hitos más característicos , y la incidencia del Reglamento 2016/679 (LCEur 2016, 605) del Parlamento Europeo y del Consejo, del 27 de abril de 2016 y de la regulación de la video vigilancia en la Ley Orgánica 3/2018, de 5 de diciembre (RCL 2018, 1629) , de Protección de Datos Personales y Garantía de los Derechos Digitales"

Fijando como elementos más importantes : "a) La doctrina constitucional hasta las SSTC 29/2013 y 39/2016; b) Vigilancia y protección de datos: el deber informativo en la doctrina de las SSTC 29/2013 y 39/2016; c) La prohibición de la video vigilancia encubierta en la doctrina de la STEDH de 9-01-2018 (caso "López Ribalda y otras v. España"); d) El deber informativo como requisito imprescindible para la validez de las grabaciones audiovisuales y de los otros medios tecnológicos de control empresarial y

la incidencia del Reglamento 2016/679, del Parlamento Europeo y del Consejo, del 27 de abril de 2016 y e) El deber informativo en la LO 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales.".

En los casos citados, el TC resolvió el conflicto entre el derecho a la intimidad personal (Art. 18.1 CE) y las facultades de control empresarial de la actividad laboral con la aplicación estricta del principio de proporcionalidad. Pero la doctrina va a ser corregida en la STC 29/2013, de 11 de febrero , que establece condiciones adicionales para la validez de la utilización de las cámaras de vigilancia en los centros de trabajo, exigiendo con rigor el cumplimiento del deber de información previo a los trabajadores para admitir las grabaciones como prueba

Sin embargo, esta doctrina del TC va a ser modificada en la STC 39/2016, de 3 de marzo (RTC 2016, 39) delimitando el alcance del deber informativo a los trabajadores, que considera cumplido cuando la empresa coloca los distintivos informativos en las condiciones que establece la Instrucción 1/2006, de 8 de noviembre , de la AEPD. Parece evidente que el Pleno del TC ha cambiado la doctrina de la STC 29/2013.

Pero las nuevas regulaciones, distinguiendo forma destacada, la reciente LO 13/2015, de 5 de octubre (RCL 2015, 1523, 1895) , que modifica la Ley de Enjuiciamiento Criminal (LEG 1882, 16) para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, exigiendo en la adopción de las mismas el respeto de los principios de idoneidad, excepcionalidad, necesidad y proporcionalidad y la aprobación de la LO 3/2018, de 5 de diciembre , que regula la video vigilancia en el ámbito de las relaciones laborales, adecuan los requisitos de la video vigilancia la exigencia informativa en esta materia conforme resulta de la doctrina del Tribunal Europeo de Derechos Humanos (TEDH sentencia de 9 de enero de 2018, caso López Ribalda), que consagra con carácter general la prohibición de los sistemas de video vigilancia ocultos o encubiertos. El deber informativo como requisito imprescindible para la validez de las grabaciones audiovisuales y de los otros medios tecnológicos de control empresarial. Incidencia del Reglamento 2016/679, del Parlamento Europeo y del Consejo, del 27 de abril de 2016, que no excepciona el deber informativo en supuestos de video vigilancia. Ante la posible disyuntiva entre la ultima doctrina del TC y el TEDH, parece que sería necesario que el juez plantee una cuestión de inconstitucionalidad ante el TC ni una cuestión prejudicial ante el TJUE. Podrá simplemente inaplicar la norma nacional que no respeta el derecho originario de la Unión Europea (Carta) y el derecho derivado dotado de eficacia directa y primacía en las relaciones verticales y en las horizontales (RGPD).

5.-GEOLOCALIZACIÓN–La LO 3/2018 en su articulo 90, ya establece como requisitos necesarios para la geolocalización que los empleadores habrán de informar de forma expresa, previa , clara e inequívoca, a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de la existencia y características de estos dispositivos e igualmente deberán informarles acerca del posible ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión de datos obtenidos (TCo STCO 241/2012, de 17 de diciembre). El secreto de las comunicaciones y a la intimidad no se ve afectado en un caso en que la empresa accede a los ficheros informáticos en que quedaban registradas las conversaciones

mantenidas entre dos trabajadoras a través de un programa de mensajería, instalado por ellas mismas en un ordenador de uso común y sin clave de acceso; conversaciones de carácter íntimo descubiertas por casualidad por un trabajador que dio cuenta a la empresa (TCo STCO 170/2013, de 7 de octubre). Basta que un Convenio colectivo sancione el uso de herramientas informáticas y correo electrónico para usos diversos al profesional para considerar que la empresa puede controlar los correos electrónicos de los empleados, empleados, sin aviso previo a estos y sin que ello vulnere su derecho al secreto de las comunicaciones y el derecho a la intimidad.

La carga de la prueba de la intromisión ilícita corresponde a quien sostiene la ilicitud (art. 217 LEC); sin perjuicio de la modulación de tal carga por el principio de disponibilidad probatoria SALA 2ª TS e SALA 2ª TS e-mail STS, Sala Penal, de 16.6.2014 (rec. 2229/2013)

En todo caso no existe ninguna posibilidad ni por la titularidad empresarial de la herramienta comunicativa (ordenador, teléfono, etc. propiedad de tercero ajeno al comunicante), ni del carácter del tiempo en el que se utiliza (jornada laboral) ni, tan siquiera, siquiera, de la naturaleza del cauce empleado (“correo (“correo corporativo”), para excepcionar la necesaria e imprescindible reserva jurisdiccional en la autorización de la injerencia. Tampoco una supuesta “tácita renuncia” al derecho por parte del trabajador.

El uso de dispositivos digitales facilitados por el empleador a los trabajadores (art. 87 LO 3/2018, de 5 de diciembre), supone la obligación empresarial de información previa sobre el uso privado permitidos de los mismos (tiempo (tiempo y forma de utilización), pudiendo ser legítimo el control de los mismos (arts. 22, 24 y 89) a los solos efectos de controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la integridad de dichos dispositivo s (art. 87.2). Ente los dispositivos digitales se incluye ordenador, móvil y tablets STS, Social, 8.2.2018 (u.d. 1121/2015).

CONCLUSIONES

Analizando toda la normativa, jurisprudencia de aplicación y doctrina sobre los soportes digitales como prueba en el procedimiento laboral, me permito concluir, que la aportación en juicio de este tipo de pruebas es una realidad que debemos aceptar pero que debe afrontarse con la intención clara de que la misma sea veraz e idónea.

La especialización de los conocimientos en informática que requiere la valoración de estos soportes electrónicos, muy dispares a su vez de la disciplina jurídica, obliga por parte de los juristas a ser conscientes de la necesidad de formarnos en las técnicas de creación, extracción y cadena de custodia de estos medios.

Entiendo que debemos ser muy cautelosos ante los posibles riesgos que genera la manipulación informática teniendo en cuenta el inicial desconocimiento y la realidad del tráfico informático. La facilidad de los operadores informáticos para transformar la realidad es uno de los peligros acreditados por los peritos informáticos. Existe en la actualidad un mercado subred, llamado “internet profunda” con protocolos de

encriptación y navegadores anónimos, difíciles de identificar, que se encargan de extraer y traficar con correos ajenos, desde los que se pueden manipular contenidos de correo electrónico. También se producen suplantaciones de páginas webs, que pueden arrojar informaciones que no se corresponden con la realidad del emisor. En el ámbito de los WhatsApp, cuentas falses, cuentas alquiladas, manipulaciones sobre terminales ajenos de fácil acceso.

Es relevante el enfoque limitante del uso de estos medios en el proceso laboral a la que tiende la jurisprudencia actual, en especial las sentencias del TEDH, que incluso ha hecho una llamada de atención en relación a la doctrina del Tribunal Constitucional y del Tribunal Supremo sobre el limitado alcance del deber informativo en materia de video vigilancia , imponiendo, por el contrario, el carácter absoluto del deber informativo vinculado a las garantías propias del derecho a la protección de datos en los términos que establecía el Art. 5 de la Ley 15/1999, y actualmente el artículo 11 de la LO 3/2018, de 5 de diciembre, sobre Protección de Datos Personales y garantía de los derechos digitales y en los artículos 12 , 13 y 14 del Reglamento 2016/679 del Parlamento Europeo y del Consejo, del 27 de abril de 2016, sobre tratamiento de datos personales y su libre circulación (RGPD).

La necesidad de la aportación de la prueba digital, como nueva realidad laboral, comporta mecanismos de consolidación de su autenticidad que deben crearse por nuestro sistema judicial y normativa legal. Por ello entiendo que los juristas deberíamos formarnos específicamente en la materia, a los juzgados debería proveerse de periciales informáticas adscritas al propio juzgado, por su especialidad e imparcialidad y debería reforzarse las medidas coercitivas ante las prácticas ilícitas en la obtención de este tipo de pruebas.

REFERENCIAS

-Raúl Rojas Rosco: "La prueba electrónica, validez y eficacia procesal". Colección: Desafíos Legales #RetoJCF Juristas con Futuro.

-Concepción Morales Vállez: "La prueba electrónica en el proceso laboral y en el control de los medios tecnológicos por el empresario". Ed.Sepin.

-Alemán Páez, Francisco (2017): “El derecho a la desconexión digital”.Revista de Trabajo y Derecho, 30

-Barrios Baudor, Guillermo Leandro (2019): “El derecho a la desconexión digital en el ámbito laboral español: primeras aproximaciones”, Aranzadi Doctrinal, 1.

-Miñarro Yanini, Margarita (2018): “La «Carta de derechos digitales» para los trabajadores del Grupo Socialista en el Congreso: un análisis crítico ante su renovado interés”. RTSS- CEF

-Xavier García Pañeda y David Melendi Palacio: "La Peritación Informática un enfoque práctico.".