expuesto se estaba decidiendo sobre un expediente sancionador cuya tramitación está informada por los derechos y garantías propios del derecho procesal penal. Además, el asunto tenía un claro componente fáctico ya que la sanción se impone a raíz de una inspección inicial de un camión frigorífico y un posterior examen de los animales transportados y de la documentación exhibida por el sancionado. En ese caso, resulta absolutamente necesario reconocer, respetar y favorecer el derecho a la prueba del administrado en vía jurisdiccional cuya función consiste en servir de cauce procesal para que los administrados puedan impugnar los actos y determinaciones de la Administración en el ejercicio legítimo de sus derechos. En ese punto, el Tribunal Constitucional considera suficientes las alegaciones del recurrente en amparo que acredita que mediante: «la que califica como "prueba pericial y testifical-pericial" de la veterinaria del matadero de…., hubiera podido demostrar, sustancialmente que no había comercializado piezas de bovino mayores de doce meses sin columna vertebral, con infracción de la legislación reguladora de la encefalopatía espongiforme bovina, con lo que según la demanda de amparo todos los hechos por los que ha sido sancionada caerían por su base, salvo la existencia de algunas irregularidades documentales». STC 80/2011 de 6 de junio.

Frente a esta alegación el Tribunal Superior de Justicia no fundamenta ni motiva las razones de su denegación de prueba limitándose a señalar que: «la prueba, en los términos en que ha sido interesada, no reviste la trascendencia que la parte promovente pretende otorgarle, al obrar en las actuaciones elementos de juicio bastantes para que la Sala pueda formar su convicción judicial». Decisión que en ningún momento se fundamenta debidamente con la debida explicación de las razones por las cuales el Tribunal no consideró trascendente el recibimiento del pleito a prueba para su resolución. Y señala el TC en este punto: «sin que puedan reputarse motivación suficiente en el presente caso las frases estereotipadas utilizadas por el órgano judicial en una y otra resolución, sin ninguna individualización para el asunto concreto enjuiciado. Debe tenerse presente a estos efectos que la existencia de una motivación adecuada y suficiente en función de las cuestiones que se susciten en cada caso concreto constituye una garantía esencial del justiciable, ya que la exteriorización de los rasgos más esenciales del razonamiento que han llevado a los órganos judiciales a adoptar una decisión dada permite apreciar su racionalidad, además de facilitar el control de la actividad jurisdiccional y, consecuentemente, de mejorar las posibilidades de defensa, por parte de los ciudadanos, de sus derechos (SSTC 209/1993, de 28 de junio, FJ 1.º, y 4/2005, de 17 de enero, FJ 5.º). Y desde luego esta deficiente motivación de la que adolece la decisión de denegar el recibimiento del pleito a prueba no resulta subsanada en este caso por la Sentencia dictada en el proceso (STC 42/2007, de 26 de febrero, FJ 5.º)». STC 80/2011 de 6 de junio.

La conclusión final que se debe obtener de este comentario es lo bien lejos que estamos de un sistema de justicia en el que los Tribunales de Justicia sean los primeros encargados de velar por la tutela judicial ordinaria de los derechos fundamentales de lo ciudadanos. Más al contrario resulta estremecedor que todavía, en el Siglo XXI, se puedan producir tan claras vulneraciones de los derechos fundamentales de los ciudadanos sin la menor explicación o fundamento. Decisiones arbitrarias e inmotivadas como las que motivaron el recurso de amparo del que conoce el Tribunal Constitucional en la comentada STC 8/2011 deberían estar proscritas de nuestro sistema de impartición de justicia. No resulta admisible que se deba tener que recurrir ante el Tribunal Constitucional para reclamar la plena garantía y reconocimiento de los derechos fundamentales de los ciudadanos. Desde mi punto de vista algo debe cambiar en el sistema porque no resulta lógico que los órganos jurisdiccionales dificulten o impidan el ejercicio legítimo de los ciudadanos en defensa de sus derechos e intereses legítimos. Especialmente en materia de proceso contencioso-administrativo. ■

NOTAS

(1) SENTIS MELENDO, S., La prueba, EJEA, Buenos Aires, págs. 292 y ss.

(2) TARUFFO, M., La prueba de los hechos, ed. Trotta, págs. 504.

(3) RODRÍGUEZ GARCÍA, N., Abstención, recusación y tacha de peritos. Análisis de su regulación en la Ley 1/2000, de Enjuiciamiento Civil en «Libro homenaje al Profesor Dr. D. Eduardo Font Serra», t. I, Ministerio de Justicia, Centro de Estudios Jurídicos, Madrid, 2004, págs. 988.

(4) En este sentido también FERNÁNDEZ URZAINQUI, F. J., Comentario al art. 309 LEC, en «Comentarios a la nueva Ley de Enjuiciamiento Civil», t. II, FERNÁNDEZ-BALLESTEROS; RIFÁ-SOLER; VALLS-GOMBAU; Ed. Atelier, Barcelona, 2001, págs. 1470.

Preguntas con respuesta

La prueba a consulta

LA LEY 17373/2011

Preguntas con respuesta: la prueba a consulta

Esta sección está destinada a consulta de los lectores, a cuyo efecto invitamos a nuestros lectores a formular aquellas consultas relacionadas con la probática o el derecho probatorio que estimen conveniente.

La primera cuestión planteada, centrada en el ámbito laboral, considera la obtención lícita de medios de prueba en los soportes digitales de los trabajadores por parte del empresario ponderando los derechos fundamentales del trabajador. Las facultades empresariales se encuentran limitadas aquí por los derechos fundamentales del trabajador, que son prevalentes y constituyen un «límite infranqueable» no solo a sus facultades sancionadoras, sino también a las facultades de organización y de gestión del empresario, causales y discrecionales.

La segunda cuestión, en torno a la prueba pericial informatica en general, describirá y evaluará una novedosa técnica desarrollada por INCIDE y basada en la heurística, que permite agilizar las investigaciones y asegurar con mayores garantías los derechos fundamentales de los usuarios de los medios digitales investigados.

I. ¿CÓMO AFECTA A LA INTIMIDAD Y AL SECRETO DE LAS COMUNICACIONES LA PRUEBA ELECTRÓNICA EN EL ÁMBITO LABORAL?

Jordi MUÑOZ-SABATÉ I CARRETERO
Abogado. Socio de DRET PRIVAT

Ya no son extrañas en el ámbito de las relaciones laborales las ocasiones en las que con motivo de un conflicto se somete a la consideración judicial hechos que de un modo u otro requieren la extracción de pruebas ubicadas en soportes digitales. El progreso tecnológico también ha hecho evolucionar los modelos de producción clásicos hacia un entorno digital estrechamente asociado al uso de dispositivos electrónicos y a nuevas herramientas de la información, a tal punto que es difícil encontrar alguna empresa o negocio que en la gestión de sus recursos y en su relación con el mercado no cuente con estas nuevas tecnologías. En este contexto, el trabajo como factor de producción ha experimentado con gran intensidad esta evolución con la puesta a disposición del trabajador de nuevos medios e instrumentos de trabajo cuya rentabilidad y eficacia nadie pone hoy en duda en términos de productividad y competitividad.

Este nuevo entorno digital a través del cual se mueven gran parte de las transacciones corporativas no es desde luego ajeno al derecho probatorio. En efecto, con las nuevas tecnologías de la información y la comunicación se han ampliado las fronteras de la prueba con la aparición de nuevos medios que, concebidos bajo la concepción generalizada de documento electrónico, almacenan «información de cualquier naturaleza en forma electrónica, archivada en soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferen-

ciado» (art. 3.5 Ley de Firma Electrónica). Y, al mismo tiempo, lo que podríamos designar como objeto de prueba, también ha manifestado un notable desarrollo con la aparición de «hechos electrónicos» que, como una consulta a una página web o el envío de un correo electrónico, están continuamente presentes en el devenir diario de una empresa. Con una progresión en constante crecimiento, cada día es más habitual constatar como en el proceso judicial se hace uso del documento electrónico, mediante la aportación de los e-mails del trabajador a fin de acreditar la sustracción de información, o de la pericial forense cuando se trata de demostrar el acceso a páginas de contenido ajeno al trabajo o a información confidencial de otros compañeros, o la existencia de intrusiones o robos de información clasificada, por poner unos ejemplos.

En este sentido, uno de los desafíos con los que se encuentra el derecho probatorio en esta nueva realidad digital es hacer frente a los problemas de legalidad que en orden a su obtención, validez y eficacia plantea el derecho del trabajo, problemática que aun siendo común a otros sectores de nuestro ordenamiento adquiere aquí una interesante dimensión por la incidencia tan relevante que tienen los derechos fundamentales sobre el aseguramiento de las pruebas y su posterior análisis forense. Piénsese que en situaciones por ejemplo de conflicto, como un despido o un expediente de empleo, puede resultar conveniente anticipar las estrategias de prueba contemplando el aseguramiento de los dispositivos electrónicos y de la información puesta a disposición de un trabajador así como el resguardo de su contenido (ordenadores, servidores corporativos, agendas electrónicas, teléfonos, etc.); precaución tanto mayor si tomamos en consideración que la arquitectura de los sistemas operativos de una gran parte de las empresas está en muchas ocasiones más abocada al rendimiento que a su propia seguridad, circunstancia que deja expuesto el contenido de sus archivos en manos del usuario haciéndolo muy volátil ante la mínima sospecha o evidencia. En otras ocasiones, la situación exigirá realizar un análisis forense inmediato con el que poder reconstruir la cadena de evidencias necesarias sobre un determinado hecho o acontecimiento (quién, cuándo y desde dónde se envió un determinado correo, o se manipuló un archivo de datos), sobre el que en su caso apoyar una determinada decisión.

Pues bien, en cualquiera de estas situaciones, ya sea el aseguramiento ya sea el análisis forense inmediato o posterior, la legitimidad de la prueba electrónica no resultará tampoco ajena aquí a ese «test de admisibilidad» que, siguiendo la sentencia del Tribunal Supremo de 30 de diciembre de 2009, supone constatar que el dispositivo y el contenido objeto de prueba es atribuible al sujeto en cuestión (autenticidad); que no ha sido alterado (integridad); y que en su obtención se han respetado los derechos y libertades fundamentales y, en su caso, las garantías establecidas por la normativa común o convencional (licitud). Pero es precisamente respecto de este último presupuesto, el de la licitud de la prueba, donde tal vez el derecho laboral cobra un especial protagonismo en el ámbito de la prueba, y ello básicamente motivado por esa particular confrontación de derechos que se produce cuando unos instrumentos de producción titularidad de la empresa son utilizados para fines particulares por el trabajador (para almacenar contenidos multimedia, o para comunicarse con amigos o familiares). La convicción social generalizada de una cierta tolerancia con este uso particular de los medios de la empresa (STS, Sala de lo Social, de 26 de septiembre de 2007), no es desde luego un obstáculo para que pueda ejercerse por parte de la misma un ordenado control que descubra un uso abusivo, desviado o fraudulento. Al fin y al cabo, no puede perderse de vista aquí que contrariamente a lo que acontece con las taquillas del empleado (art. 18 ET), los medios electrónicos que se le entregan para el desempeño de su trabajo no forman parte de su esfera privada ni están al margen de los poderes de control reconocidos por el art. 20.3 ET. Aun con ciertos titubeos, la jurisprudencia ha terminado por inclinarse por la inaplicabilidad del art. 18 ET en los casos de registros informáticos como medida de control empresarial negando su equiparación con los registros sobre la persona del trabajador, sus taquillas y efectos particulares (Sentencia del Tribunal Supremo de 26 de septiembre de 2007). Se parte para ello de la premisa de que los registros informáticos forman parte del poder directivo ordinario del empresario y que, en atención al art. 20.3 ET, éste ostenta la facultad de adoptar las medidas que considere oportunas para vigilar el cumplimiento de las obligaciones laborales de sus empleados.

De lo que se trata en estos próximos apartados es conocer de qué modo pues el derecho a la intimidad y al secreto de las comunicaciones condicionan a partir del art. 18 de la Constitución la intrusión en los procesos del aseguramiento y análisis forense y, por derivación de ello, la licitud de la prueba, todo ello tomando en su debida consideración que el poder de dirección del empresario se refleja a su vez en derechos reconocidos constitucionalmente (arts. 33 y 38 CE) en una convergencia de derechos cuyo equilibrio implica en resumen: a) por una parte, los derechos fundamentales del trabajador «deben adaptarse a los requerimientos de la organización productiva en que se integra» (SSTC 5/1981, 47/1985, 77/1985, 10671996, 199/1999), y b) por otra parte, que también «las facultades empresariales se encuentran limitadas por los derechos fundamentales del trabajador», que son prevalentes y constituyen un «límite infranqueable» no solo a sus facultades sancionadoras, sino también a las facultades de organización y de gestión del empresario, causales y discrecionales (SSTC 292/1993, 136/1996, 90/1997, 213/2002).

Entrando en el abordaje de esta cuestión, son varios los aspectos técnicos y jurídicos que desde este prisma constitucional repercuten en la licitud de la prueba:

1.—El conocimiento por parte del trabajador de las facultades de control de la empresa sobre los recursos electrónicos y de la existencia de mecanismos de control, como la simple monitorización del correo electrónico o la implantación de un programa de contabilización del tiempo empleado en internet, va desde luego mucho más allá de un simple recomendación. De hecho la propia jurisprudencia del Tribunal Supremo ha venido a establecer como una manifestación de las reglas de la buena fe, la existencia de un deber (y un correlativo derecho a favor del trabajador) de información por parte de las empresas en orden al establecimiento de reglas de uso de estos medios, con aplicación de prohibiciones absolutas o parciales, y de controles, de tal modo que las actuaciones inspectoras de la actividad laboral deben ir precedidas de la necesaria información. Sería por ejemplo contrario a la buena fe el establecimiento subrepticio de mecanismos de control ante una sospecha de actuación fraudulenta, abusiva o desviada, y ello independientemente de su amplitud o gravedad, como da cuenta la reciente sentencia de la Sala de lo Social del Tribunal Supremo de 8 de marzo de 2011 al desestimar la procedencia de un empleado que había accedido a 5.566 visitas de contenido multimedia, piratería informática, anuncios y otros en un supuesto en el que la prueba se obtuvo a partir de una auditoría interna pero sin información previa por parte de la empresa sobre la existencia de controles ni ninguna advertencia sobre las reglas de uso de los ordenadores.

Se trata en definitiva de conocer de antemano y a partir de lo que se conoce como Protocolos de Usos Aceptables, Códigos de Conducta o Códigos de Buenas Prácticas, unas limitaciones y unas facultades que no tan solo sirvan para disciplinar el uso de estos medios de trabajo, sino que a su vez reduzcan las expectativas razonables de intimidad del trabajador, en los términos de las sentencias del Tribunal Europeo de Derechos Humanos de 25 de junio de 1997 (caso *Halford)* y 3 de abril de 2007 (caso *Copland)*. De hecho no son pocos los Convenios Colectivos que han adoptado iniciativas en este sentido, y día a día se está estandarizando en los contratos de trabajo las condiciones de uso y sus responsabilidades disciplinarias.

Con todo conviene precisar que la ausencia previa de esta información sobre las facultades de control no tiene por qué invalidar la prueba cuando la misma se haya obtenido de forma accidental a semejanza de lo que en el ámbito penal ocurre con el llamado «hallazgo casual», lo que suele ocurrir en ocasiones con motivo de una simple intervención rutinaria por parte del técnico informático. Ahora bien, hay que diferenciar bien entre lo que no constituye más que una evidencia electrónica sobre la existencia de un uso ajeno al trabajo *(v.gr.* la existencia de un virus, un troyano, o una desmedida presencia de archivos temporales), de la prueba electrónica en sí, pues mientras ésta permite fijar un hecho (quién, cuándo y desde dónde), la evidencia es una manifestación muy simple del hecho que requerirá para alcanzar esa misma convicción de la concurrencia de otras elementos indiciarios. En estos casos, esto es, cuando de un modo accidental o fortuito se tenga noticia de un uso irregular de los medios puestos a disposición del trabajador, los mecanismos de investigación, registros y controles que se activen a partir de este momento para la consecución de esa convicción no presentarán ya ninguna excepcionalidad para que se hagan al margen de las debidas cautelas y con el mismo respeto a la dignidad del trabajador y a los principios de la buena fe antes apuntados.

En otro orden de consideraciones, entiendo que la simple prohibición, ya sea total o parcial, de utilización de los ordenadores y demás medios digitales para fines particulares, es suficiente para dejar habilitada esa facultad de control aún cuando no se hubiera informado previamente de la misma ni de los medios a aplicar para comprobar el correcto uso. Básicamente porque parece claro que la prohibición señalada lleva implícita la facultad de control, y si la empresa ha dispuesto que el ordenador debe constituir una mera herramienta de trabajo sin destinarse a usos particulares, no puede desconocerse que a ello va anudada lógicamente la posibilidad de ejercer el control correspondiente para comprobar el cumplimiento de esa norma.

2.—El empresario no está apoderado desde luego para, so pretexto de estas facultades, llevar a cabo controles de un modo totalmente arbitrario. En nuestro ordenamiento no existe una normativa específica al día de hoy que regule la instalación y utilización de estas medidas de control, de tal modo que son los órganos judiciales

quienes habrán de ponderar en qué circunstancias puede considerarse legítimo su uso por parte del empresario al amparo de ese poder de dirección que le otorga el art. 20.3 ET. La propia amplitud que en este sentido le concede este precepto al disponer que *podrá adoptar las medidas que estime más oportunas de vigilancia y control* aparece supeditada por la misma norma *a la debida consideración de la dignidad del trabajador,* lo que viene a suponer que entre el fin pretendido mediante los medios de control instaurados y la posible restricción de los derechos fundamentales asociados a la dignidad, exista un cierto equilibrio. Cual acontece al fin y al cabo con cualquier medida restrictiva de derechos fundamentales, este equilibrio pasa en definitiva por someter la medida en cuestión a un *test de proporcionalidad* cuya superación dependerá de la consecución de estas tres condiciones que habrán de ponderar los órganos judiciales: que el acceso al dispositivo o medio electrónico sea adecuado para alcanzar el objetivo perseguido *(juicio de idoneidad);* que sea necesario, en el sentido de que no existan otras medidas menos intrusivas *(juicio de necesidad),* y, por último, que sea ponderada por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto *(juicio de proporcionalidad en sentido estricto)*.

Un exponente y una referencia judicial constante en este apartado es la sentencia del Tribunal Constitucional 186/2000 de 10 de julio de 2000, FJ 6.º:

«el derecho a la intimidad es aplicable al ámbito de las relaciones laborales» (STC 98/2000, de 10 de abril); y que «el derecho a la intimidad no es absoluto, como no lo es ninguno de los derechos fundamentales, pudiendo ceder ante intereses constitucionalmente relevantes, siempre que el recorte que aquél haya de experimentar se revele como necesario para lograr el fin legítimo previsto, proporcionado para alcanzarlo y, en todo caso, sea respetuoso con el contenido esencial del derecho (SSTC 57/1994 y 143/1994)».

Tomando ejemplos muy presentes en la jurisprudencia de casación y la menor emanada de las Salas de lo Social de los Tribunales Superiores de Justicia, resultará con todo lo dicho legítimo acceder al ordenador de un empleado con el propósito de comprobar el tiempo invertido en navegar por páginas ajenas a su cometido laboral a condición de que se le hubiera informado previamente de la existencia de controles, o, igualmente y con propósito semejante, cuando se hubiera avisado de la instalación de un programa de monitorizacion para contabilizar el tiempo empleado en internet a través de la consulta de las direcciones visitadas.

3.—Ahora bien, en supuestos como éstos y todos aquellos otros que nos ofrece la casuística judicial en esta materia, no puede perderse de vista que la consecución de este necesario e inexcusable equilibrio de derechos en juego pasará siempre por la máxima preservación de la intimidad o, dicho desde otra perspectiva, de su mínima afectación, cuyo alcance encuentra su máximo exponente con la sentencia del Tribunal Europeo de Derechos Humanos de 3 de abril de 2007 al señalar que están incluidos en la protección del art. 8 del Convenio Europeo de derechos humanos «la información derivada del seguimiento del uso personal de Internet». Partiendo de esta premisa, salvo supuestos excepcionales donde se pueda justificar la inexistencia de medidas menos intrusivas, no podrá accederse a los archivos personales del trabajador para controlar un uso desviado del correo cuando para ello baste con una simple impresión de la relación de dichos correos (STSJ Andalucía, Sala de lo Social, Secc. 2.ª, de 8 de julio de 2010), como tampoco extraer rastros o huellas como los archivos temporales que incorporen información sobre aspectos de la vida privada (ideología, orientación sexual, aficiones personales, etc.), como ocurre con el simple dominio de las páginas web que en la mayoría de los casos son reveladoras de su contenido.

De igual modo deberá eludirse cualquier método de revisión exhaustiva que implique el acceso a todos los activos de información del medio analizado, mediante una apertura indiscriminada de todos los correos y archivos. Disponemos hoy en día de herramientas informáticas de análisis forense poco a poco reconocidas por nuestros tribunales que a través de lo se ha venido a designar «búsqueda ciega» evitan este tipo de invasiones mediante una técnicas heurísticas de búsqueda y filtrado semántico (1), que vienen a funcionar a modo de rastreo. Una vez reconocido y fijado el hecho objeto de investigación (por ejemplo, la desviación de información confidencial a la competencia o navegación por páginas pornográficas), se definen una serie de palabras claves o expresiones asociadas al hecho (nombre de empresas competidoras, números de teléfonos, direcciones de correos electrónicos, expresiones como adulto, sexo, etc.) a partir de las cuales se efectúa un rastreo que permite localizar los archivos o documentos vinculados a esas palabras sobre los que seguidamente focalizar la investigación, con discriminación de aquellos otros totalmente ajenos a su propósito o causa que pudieran contener información relacionada con la esfera personal del trabajador totalmente ajena a la investigación. Este método de localización de indicios a través de la búsqueda ciega de palabras claves ha obtenido ya su respaldo judicial en sentencias como la del Juzgado de lo Mercantil núm. 2 de Barcelona, de 9 de mayo de 2008, o el AP Barcelona, Secc. 15, de 2 de febrero de 2006.

4.—El respeto a la dignidad del trabajador no implica, por último, que deba estar presente en el control ni tampoco la presencia de un representante de los trabajadores, a modo y semejanza de lo que impone el art. 18 ET para el registro de las taquillas. Tomando en consideración lo ya comentado anteriormente a propósito de las facultades de control, la presencia del empleado, de un representante legal o, en su ausencia del centro de trabajo, de otro trabajador, adquiere su significado si se presta atención a que en los casos del art. 18 ET la empresa está ejercitando de forma excepcional una función de policía que la norma vincula a la protección de su patrimonio y el de los demás trabajadores, lo que nada tiene que ver el control de un medio de trabajo. Pero conviene aclarar que el hecho de que el trabajador no esté presente en el control no es en sí mismo un elemento que pueda considerarse contrario a su dignidad ni menos una exigencia legal que condicione la licitud de una prueba.

Ahora bien, como sucede con lo previsto por el art. 569 Ley de Enjuiciamiento Criminal para intervenciones similares, la presencia de uno u otros podrá si acaso constituir una garantía de objetividad y eficacia de la prueba, pero es ajeno a este juicio de proporcionalidad.

Al hilo de todas las anteriores consideraciones y como resumen, la prueba electrónica deberá ajustarse necesariamente y bajo condición de nulidad (art. 11.1 LOPJ), a toda esta serie de cautelas que, de un lado, justifiquen su obtención y aseguramiento y, de otro, preserven en ese justo equilibrio de derechos, la intimidad del trabajador, evitando intrusiones indiscriminadas y desproporcionadamente invasivas. Todo ello sin olvidar la existencia de aquellas otras garantías que afectan propiamente al ámbito de la admisión, eficacia y valoración, y que tienen un especial juego en la prueba electrónica en todo aquello que atañe a la cadena de custodia, sobre los que trataré en otra ocasión.

II. ¿CÓMO SE PUEDEN SALVAGUARDAR LOS DERECHOS FUNDAMENTALES AL REALIZAR INVESTIGACIONES INFORMÁTICAS?

Abraham PASAMAR NAVARRO
Director General INCIDE (Investigación Digital, S.L.)
Sergi MENÉNDEZ FRAGUA
Perito informático INCIDE (Investigación Digital, S.L.)

En el marco del desarrollo de muchas periciales informáticas, y en especial aunque no limitado, a aquellas que versan sobre la comisión de algún tipo de fraude (competencia desleal, extracción de información, fraude *on-line,* uso no autorizado de recursos, etc.), el perito debe efectuar un trabajo de localización de documentación relevante y revisión de la misma para valorar si es pertinente para el caso que se investiga o no.

En esta fase del trabajo se debe decidir la mejor forma de escoger, entre todo el universo de datos que puede contener un ordenador, aquellos documentos que tienen relevancia para la investigación y por tanto susceptibles de ser candidatos a incluir en el informe pericial y de los cuales se derivarán las conclusiones del mismo.

En estos casos, el reto al que se enfrenta el perito tiene dos vertientes diferenciadas. La primera de ellas, de carácter más técnico, consiste en determinar la mejor forma (más rápida y óptima) de llegar a la información de interés. La segunda de ellas, de carácter legal y mucho más sutil, tiene que ver con la metodología utilizada para escoger los documentos relevantes y su compatibilidad con la preservación de los derechos fundamentales del usuario del dispositivo digital que se analiza, sea éste un teléfono, un ordenador de empresa o un buzón de correo, por ejemplo.

En la actualidad, no existe ninguna legislación al respecto de como realizar o presentar periciales informáticas. Básicamente, el trabajo de los peritos se puede enmarcar en los arts. 335 y 336 LEC.

Además de lo que dicta la LEC, el otro gran precepto al que pueden apelar los peritos en el desarrollo de su actividad profesional es lo relativo a la Constitución Española. Del análisis de la misma, transpira que para que la pericial informática pueda ser admitida en un procedimiento legal, no debe haberse vulnerado ninguno de los derechos fundamentales del usuario del dispositivo analizado.

En última instancia, aplica la doctrina jurisprudencial del Tribunal Constitucional, en su sentencia de 10 de julio de 2000 donde se considera que los medios de prueba, como requisitos para ser admitidos en un procedimiento, han de seguir los principios de proporcionalidad, idoneidad, necesidad y equilibrio.

Esto ha hecho que, como si de un proceso de ensayo y error se tratara, las diferentes formas de atacar este problema se han puesto a prueba en los Tribunales. En este sentido, los expertos reconocen que hay un antes y un después de la sentencia del 26 de septiembre de 2007 del Tribunal Supremo, que regula en qué forma se debe realizar el registro de un ordenador de un empleado, sentando las bases para la realización de futuras periciales informáticas en entornos laborales, pero extensibles a otras jurisdicciones.

Las técnicas heurísticas

La función heurística es un cálculo que nos permite, en cualquier estado intermedio en el camino hacia la solución óptima del problema, obtener un valor que nos indique si estamos cerca o lejos de dicha solución.

La búsqueda ciega y automatizada de palabras clave es la principal técnica utilizada en el sector de la informática forense para detectar los documentos electrónicos presentes en un dispositivo digital que contiene información relevante para una investigación, respetando la intimidad de las personas implicadas.

El método heurístico consiste en la realización de una segunda criba sobre los resultados obtenidos de la búsqueda ciega con el objetivo de detectar los documentos electrónicos que, además de información relevante para el caso, contienen información de carácter personal o íntima. Este análisis persigue, por un lado, poder acceder a los contenidos de los documentos electrónicos con la seguridad de que no contienen información personal, y, por otro lado, reducir aún más el número de documentos a analizar manualmente, que repercute directamente en la complejidad de la investigación.

Para esta detección de información personal se utilizan diversas variantes de lo que se llama análisis heurístico, que consiste en asignar, de manera ciega y automatizada, una puntuación a cada documento electrónico, basándose en ciertos criterios que pueden variar en cada caso, descartando aquellos sospechosos de contener información personal en base a esta puntuación. La implementación exacta de esta técnica puede variar dependiendo de los criterios utilizados por cada perito para la puntuación.

El método es simple. Consiste en la elaboración de tres listados de palabras: 1) un listado de palabras corporativas, formado por palabras propias del sector profesional en el que se enmarca la pericial; 2) un listado de palabras clave, formado por aquellas palabras relacionadas con la investigación, entendiendo que un documento que contiene este tipo de palabras, seguramente será un documento relevante, y 3) un listado de palabras personales, entendiendo que un documento que contenga estas palabras tendrá más probabilidad de contener información de tipo personal o no relacionada con la pericial.

La decisión de si un documento pertenece al ámbito personal, se responde en base a la diferencia entre el número de apariciones de palabras corporativas y clave de la investigación y el número de palabras personales que contiene un documento. Si esta suma da como resultado un número mayor que cero se considera que ese documento se encuentra lo suficientemente fuera del ámbito personal, y por tanto susceptible de ser integrado en la revisión manual.

La metodología heurística goza de todas las ventajas de la búsqueda ciega, es decir, permite optimizar los recursos que el perito dispone para la realización de la investigación dado que se reduce el volumen de información a revisar y establece un listón para la salvaguarda de los derechos fundamentales del usuario del dispositivo peritado.

Respecto a los derechos fundamentales, la técnica de búsqueda ciega, aunque establece una primera barrera de protección, no permite asegurar en todos los casos su fiabilidad al respecto, dado que un documento puede contener una palabra clave y al mismo tiempo ser de contenido íntimo o personal.

La introducción no solo de diccionarios de ámbito personal o íntimo, sino también de parámetros y pesos que nos permitan regular su importancia según la investigación en curso pretenden contrarrestar este inconveniente. A favor de la técnica heurística, cabe decir que la mayoría de implementaciones de la búsqueda ciega permiten al perito visualizar solamente el contexto que rodea la palabra clave dentro de un documento que la contiene, evitando de este modo la apertura completa del mismo de forma precipitada. Es decir, visualizando las palabras que rodean la expresión clave, el analista realiza un juicio de valor sobre la necesidad de proceder a la apertura del mismo. Sin embargo, puede ocurrir que este juicio de valor se haya realizado correctamente y sin embargo el documento contenga fragmentos de contenido íntimo cuya existencia no se podía prever de antemano. El uso de la técnica heurística habría permitido al perito eliminar de la revisión este documento basándose simplemente en el resultado o puntuación que la función heurística habría arrojado.

Así, esta técnica nos permitiría descartar de la investigación con un paso automático (y sin intervención humana) todos aquellos documentos susceptibles de contener información relacionada con la esfera personal del usuario del medio digital peritado, y por tanto que la pericial desde el punto de vista legal, goce de las máximas garantías de admisibilidad. La consideramos, pues, como una mejora considerable respecto a la metodología de búsqueda ciega de palabras clave.

A pesar de que la aplicación de técnicas heurísticas supone haber conseguido una mejora razonable sobre las técnicas existentes para la localización y revisión de documentación en el ámbito de las periciales informáticas, hay algunas consideraciones que deben tenerse en cuenta en su aplicación.

La más patente de todas es que no podemos olvidar que estamos utilizando funciones heurísticas y por tanto sujetas a errores. A pesar de que hemos hecho un esfuerzo por darle el máximo rigor matemático a la descripción formal de esta técnica, su propia definición se basa en conocimiento intangible y en la aplicación de la lógica humana o la experiencia previa en otras investigaciones por parte del perito.

La segunda consideración que es preciso tener en cuenta es que para que la heurística funcione como es debido, tanto los parámetros asociados a la misma como los diccionarios que utiliza deben estar bien definidos. Resaltamos esta palabra porque no es posible definir con rigor científico qué significa la expresión «bien definidos» en este contexto, dado que los resultados que proporciona suelen valorarse con criterios subjetivos, sobretodo en entornos judiciales en el que intervienen múltiples factores. A pesar de ello, un perito con experiencia debería saber valorar la bondad de los resultados obtenidos mediante la aplicación de esta metodología.

Especialmente en un momento en el que la jurisprudencia está dejando claro que existe una expectativa clara de intimidad en el uso del ordenador corporativo, y a pesar de que la misma proporciona al empresario una mayor capacidad de control, es importante ser muy prudente en el tipo de revisión que se ejerza. De lo contrario, se entraría en una corriente de revisiones indiscriminadas de información, donde se violentarían los derechos fundamentales, generalmente sin suficientes pretextos o justificaciones. Afortunadamente, la tecnología actual permite llevar a cabo técnicas de revisión muy efectivas a la par que garantes con el derecho a la intimidad y al secreto de las comunicaciones. En esta línea, y desde hace ya varios años, se viene utilizando la técnica de las búsquedas ciegas, que aun no siendo perfecta es mucho más proporcional que la técnica de revisión exhaustiva.

Para tratar de paliar las limitaciones comentadas, INCIDE propone formalmente una metodología basada en funciones heurísticas que consideramos supone una mejora sustancial a la técnica actual y cuya aplicación a las periciales informáticas permite obtener resultados más certeros, y en los que la salvaguarda de los derechos fundamentales de los usuarios de los medios peritados sea tratada con el máximo de objetividad y rigurosidad.

Por ello, consideramos que esta nueva técnica se convertirá en una herramienta que permitirá al perito ser más eficiente y preciso en su desempeño como experto en situaciones de litigio, ofreciendo además una medida de protección para el profesional dado que lo aleja de los riesgos derivados de una posible situación de vulneración de derechos fundamentales.

Finalmente, es preciso mencionar, que a pesar de que este artículo expone una idea novedosa y tiene gran parte de carácter teórico, no se trata de un mero ejercicio de investigación. La técnica heurística descrita en este documento ya se está utilizando en periciales informáticas con gran éxito y que están siendo admitidas en procedimientos judiciales. ■

NOTAS

(1) En este mismo número y apartado de Cuadernos de Probática de LA LEY se abordan estas técnicas heurísticas por parte de los peritos informaticos de INCIDE.