protección del patrimonio cultural que se encuentra situado tanto en la plataforma continental de cualquier Estado parte como en la Zona, recogiendo expresamente, en este último caso, la declaración de intenciones contenida en el artículo 149 de Montego Bay, pero extendiendo la responsabilidad y los derechos del Estado ribereño a preservar y proteger el patrimonio cultural subacuático más allá del mar territorial y la zona contigua, abarcando también a la zona económica exclusiva y la plataforma continental. Así, se faculta al Estado ribereño para prohibir o autorizar cualquier actividad dirigida al patrimonio cultural subacuático que se halle en dichas aguas.

La protección, que parte del principio fundamental de no explotación comercial de los objetos hallados, se articula a través de la obligación de cualquier nacional de un Estado parte o buque que enarbole pabellón de un Estado parte de comunicar no sólo cualquier descubrimiento de patrimonio cultural subacuático que realicen en su plataforma continental o en la de terceros países o en la Zona, sino también de cualquier actividad que tengan intención de llevar a cabo y cuyo objeto primordial sea dicho patrimonio cultural subacuático, pudiendo, directa o indirectamente, alterarlo o causarle cualquier daño. A partir de esta notificación, la Convención exige la realización de una serie de notificaciones y consultas entre los Estados Parte que declaren su interés sobre los bienes hallados, así como la puesta en práctica de las medidas de protección y la expedición de las autorizaciones para la realización de actividades dirigidas cuyo objeto sea el patrimonio cultural subacuático que esos Estados hayan acordado conjuntamente.

La regulación de la Convención no reconoce a unos Estados parte frente a otros Estados derechos preferentes sobre el patrimonio cultural subacuático por razón del pabellón del buque, sino que pretende la más estrecha colaboración entre todos los Estados parte con el objetivo final de lograr una mejor protección y preservación del patrimonio cultural subacuático por el beneficio de toda la humanidad, y sobre el respeto al principio angular antes comentado de la no explotación comercial del patrimonio cultural subacuático. Por el bien de ese patrimonio esperemos que esta Convención reúna cuanto antes el mayor números de países signatarios que permitan su entrada en vigor

Conclusiones

Como se ha visto, la regulación actual de esta cuestión presenta numerosas lagunas que son aprovechadas por algunas compañías que se dedican profesionalmente, con fines exclusivamente lucrativos o comerciales, al hallazgo y extracción de estos bienes de indudable valor histórico y cultural, muchas veces actuando con total impunidad.

Atendidas las carencias de Montego Bay, la Convención de la UNESCO para la protección del patrimonio cultural subacuático intenta no sólo desterrar la posibilidad de actuación de estas compañías cazatesoros sino también involucrar a los Estados del pabellón de los pecios hundidos en su protección dondequiera que éstos se hallen.

No obstante, el bajo número de ratificaciones de la Convención[4] demuestra su falta de acogida entre los Estados y, por tanto, la necesidad de que los Estados sigan trabajando para lograr una eficaz protección del patrimonio cultural subacuático, ya sea por medio de acuerdos multilaterales distintos de la Convención de la UNESCO o por medio de acuerdos bilaterales con otros Estados.

Finalmente, y por lo que respecta a nuestras aguas, habremos de reflexionar sobre los riesgos que pueden generar la dispersión de competencias y la falta, en ocasiones, de la adecuada y deseable coordinación entre Administraciones o, incluso, entre Departamentos de una misma Administración, circunstancias de las que no dudemos se aprovechan algunas compañías.

Tomás Fernández-Quirós y
Victoria Andrés Cabrera (*)

EL PODER DE CONTROL EMPRESARIAL SOBRE LOS MEDIOS INFORMÁTICOS PUESTOS A DISPOSICIÓN DEL TRABAJADOR. SENTENCIA DEL TRIBUNAL SUPREMO DE 26 DE SEPTIEMBRE DE 2007

El control empresarial de la utilización por parte de los empleados de los medios informáticos puestos a su disposición había sido una cuestión analizada por un número significativo de resoluciones judiciales en distintas instancias, pero sin que se hubiera conseguido alcanzar una conclusión totalmente clara y segura acerca del contenido y límites de dicho control empresarial ni sobre la forma en que tal control debía llevarse a cabo desde un punto de vista práctico.

(*) Abogados del Área de Mercantil de Uría Menéndez (Barcelona).

Por ello, la sentencia de la Sala de lo Social del Tribunal Supremo de 26 de septiembre de 2007 (RJ 2007\7514) (en adelante, la *«Sentencia»*) es, sin lugar a dudas, una sentencia de gran importancia y trascendencia, por cuanto supone el primer pronunciamiento de la Sala de lo Social del Tribunal Supremo (*«TS»*) en el que se unifica y sienta doctrina sobre *«el alcance y la forma del control empresarial sobre el uso por el trabajador del ordenador que se ha facilitado por la empresa como instrumento de trabajo»*. En concreto, la Sentencia clarifica alguno de los aspectos más relevantes que se venían discutiendo judicial y doctrinalmente acerca de esta cuestión, aunque probablemente deja algunos puntos sin resolver, como más adelante se comentará brevemente. Como muestra de su relevancia e importancia, esta sentencia ha tenido una amplia repercusión en distintos medios de comunicación, llegando incluso a ser portada de uno de los diarios económicos más importantes a nivel nacional (véase Expansión de 24 de octubre de 2007).

Conviene señalar, porque la Sentencia insiste sobre este aspecto, que lo relevante de la doctrina que en ella se unifica no tiene por objeto la valoración de la conducta del trabajador a efectos disciplinarios (acceso a páginas pornográficas de Internet a través del ordenador de la empresa), sino *«los límites del control empresarial»* sobre el uso del ordenador facilitado por la empresa.

En concreto, dos son los aspectos o puntos claves sobre los que la sentencia sienta doctrina unificada, a saber: (i) el empresario puede controlar, en principio, el uso por el trabajador del ordenador, y dicho control no se regula por el artículo 18, sino por el artículo 20.3 del Estatuto de los Trabajadores *(«ET»);* y (ii) para que dicho control sea lícito o legítimo, el empresario ha de establecer, previamente, las reglas del uso del ordenador y ha de informar a los trabajadores de la existencia del control y de las medidas aplicables en caso de incumplimiento de esas reglas.

Posibilidad de control empresarial al amparo de lo establecido en el artículo 20.3 del Estatuto de los Trabajadores (y no en el artículo 18)

Uno de los debates tradicionales en relación con el poder de control empresarial de los medios informáticos ha sido la norma o normas en las que dicho poder de control tenía su amparo y, con ello, los límites y garantías que debían respetarse para que dicho control fuera considerado lícito o legítimo.

En numerosas ocasiones (como en la resolución recurrida en el caso analizado por la Sentencia), nuestros órganos jurisdiccionales han acudido al artículo 18 del ET para analizar la licitud o no del control empresarial llevado a cabo sobre el ordenador puesto a disposición del trabajador, precepto aquél que establece y regula los registros por parte del empresario *«en sus taquillas y efectos particulares»*. Conviene reproducir aquí el mencionado artículo 18 en su integridad: *«Sólo podrán realizarse registros sobre la persona del trabajador, en sus taquillas y efectos particulares, cuando sean necesarios para la protección del patrimonio empresarial y del de los demás trabajadores de la empresa, dentro del centro de trabajo y en horas de trabajo. En su realización se respetará al máximo la dignidad e intimidad del trabajador y se contará con la asistencia de un representante legal de los trabajadores o, en su ausencia del centro de trabajo, de otro trabajador de la empresa, siempre que ello fuera posible»*.

Se puede adelantar ya, en relación a este artículo, que la conclusión del TS al respecto es rotunda: no cabe la aplicación del artículo 18 del ET al control del uso del ordenador por los trabajadores, ni siquiera analógicamente. Por el contrario, la sentencia unifica doctrina situando el control empresarial en el ámbito del artículo 20.3 del ET, el cual establece que: *«El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana [...]»*.

En concreto, la sentencia analiza el siguiente supuesto de hecho: el trabajador, director general de la empresa demandada, prestaba sus servicios en un despacho, sin llave, en el que disponía de un ordenador carente de clave de acceso y conectado a la red de la empresa. Un técnico informático, ante el surgimiento de determinados problemas relacionados con el funcionamiento del ordenador, detectó la existencia de un virus informático como consecuencia de la navegación por páginas poco seguras de Internet, que resultaron ser de contenido pornográfico. Dicha navegación fue posteriormente comprobada en presencia del administrador de la empresa, procediéndose a almacenar en un dispositivo USB los archivos temporales de Internet, que recogían las páginas visitadas. Finalmente, dicho dispositivo USB fue entregado a un notario y la empresa procedió al despido disciplinario del trabajador.

Ante este supuesto de hecho, la sentencia del Tribunal Superior de Justicia de Galicia, que es la recurrida ante el TS, declaró el despido improcedente, confirmando la sentencia dictada previamente por el Juzgado de lo Social, por considerar que la prueba de la empresa había sido obtenida mediante un registro que no cumplía con las exigencias y requisitos del artículo 18 del ET. Por el contrario, en el supuesto resuelto por la sentencia de contraste, dictada por el Tribunal Superior de Justicia de Madrid, en el que también se esgrimía la descarga y visualización de ficheros de contenido pornográfico, el despido fue declarado procedente, excluyendo la mencionada sentencia de contraste la aplicación de las garantías del artículo 18 ET, al entender que el ordenador no es un efecto personal del trabajador, sino una herramienta de trabajo propiedad de la empresa.

Como se adelantaba anteriormente, la Sentencia confirma este segundo criterio y rechaza el aplicado por la sentencia recurrida. En concreto, el TS establece que el supuesto de hecho del artículo 18 del ET es «*completamente distinto del que se produce con el control* (empresarial) *de los medios informáticos en el trabajo*». Por ello, el TS considera que no cabe en ese control la aplicación directa del artículo 18 ET, pero tampoco su aplicación analógica, porque no hay «*ni semejanza de los supuestos, ni identidad de razón en las regulaciones*». El TS considera que los efectos personales del trabajador, así como su taquilla «*forma*(n) *parte de la esfera privada de aquél y quedan fuera del ámbito de ejecución del contrato de trabajo al que se extienden los poderes del artículo 20* (del ET)». Sin embargo, si de lo que se trata —como es el caso— es del control de un medio de producción, el artículo 20 del ET deviene completamente aplicable a todos los efectos.

Por ello, el TS concluye que el control del uso del ordenador facilitado al trabajador por el empresario no se regula por el artículo 18 del ET, por lo que no le son aplicables las garantías y límites del citado artículo 18 del ET, tal y como a continuación se expone.

Así, en primer lugar, el TS declara que el control empresarial del uso por el trabajador del ordenador no tiene que justificarse por la protección del patrimonio empresarial y de los demás trabajadores de la empresa (como requiere el artículo 18 del ET), ya que, en el caso del control del ordenador, la legitimidad de dicho control deriva del «*carácter de instrumento de producción del objeto sobre el que recae*», es decir, el propio ordenador.

Más detenidamente, el TS, razona, a este respecto, lo siguiente:

(i) El empresario tiene la facultad de controlar el uso del ordenador, «*porque en él se cumple la prestación laboral y, por tanto, ha de comprobarse si su uso se ajusta a las finalidades que lo justifican, ya que en otro caso estaría retribuyendo como tiempo de trabajo el dedicado a actividades extralaborales*».

(ii) Igualmente, el empresario tiene la facultad de «*controlar también los contenidos y resultados de dicha prestación*», citando, a este respecto, su anterior sentencia de 5 diciembre de 2003, sobre telemarketing telefónico (RJ 2004/313).

(iii) Asimismo, el TS considera que el control de los medios informáticos puestos a disposición del trabajador «*se justifica también por la necesidad de coordinar y garantizar la continuidad de la actividad laboral en los supuestos de ausencias de los trabajadores (pedidos, relaciones con clientes...), por la protección del sistema informático de la empresa, que puede ser afectado negativamente por determinados usos, y por la prevención de responsabilidades que para la empresa pudieran derivar también algunas formas ilícitas de uso frente a terceros*».

(iv) En virtud de todo lo anterior, el TS concluye que «*el control empresarial de un medio de trabajo* (el ordenador) *no necesita, a diferencia de lo que sucede con los supuestos del artículo 18 del Estatuto de los Trabajadores, una justificación específica caso por caso. Por el contrario, su legitimidad deriva directamente del artículo 20.3 del Estatuto de los Trabajadores*».

En segundo lugar, por lo que se refiere a la exigencia establecida en el artículo 18 del ET de respetar en el control «*la dignidad*» del trabajador, la Sentencia hace notar que «*no es requisito específico de los registros del artículo 18, pues esta exigencia es general a todas las formas de control empresarial, como se advierte a partir de la propia redacción del artículo 20.3*». El propio artículo 20.3 establece que cualquier medida de control sobre el trabajador deberá llevarse a cabo «*guardando en su adopción y aplicación la consideración debida a su dignidad humana ...*».

En todo caso, y para despejar cualquier duda que pudiera existir a este respecto, el TS establece y aclara que el hecho de que el trabajador no esté presente mientras se lleva a cabo el control «*no es en sí mismo un elemento que pueda considerarse contrario a su dignidad*».

En tercer lugar, respecto a la exigencia de que el registro se practique en el centro de trabajo y en las horas de trabajo, el TS afirma que tiene sentido en el marco del artículo 18 del ET, que se refiere a facultades empresariales que, por su carácter excepcional, no pueden ejercitarse fuera del ámbito de la empresa, pero que no es aplicable al control de una herramienta de trabajo titularidad del propio empresario. En concreto, el TS afirma en este sentido que *«es claro que el empresario no puede registrar al trabajador o sus efectos personales fuera del centro de trabajo y del tiempo de trabajo, pues en ese caso sus facultades de policía privada o de autotutela tendrían un alcance completamente desproporcionado... Esto no sucede en el caso del control de un instrumento de trabajo del que es titular el propio empresario»*.

Por último, en lo relativo al requisito consistente en la presencia de un representante de los trabajadores o de un trabajador de la empresa a la hora de llevar a cabo el control empresarial, el TS concluye que *«tampoco se relaciona con la protección de la intimidad del trabajador registrado»;* es más bien —afirma el TS—, *«una garantía de la objetividad y de la eficacia de la prueba»*. Por ello, esta exigencia no puede ser aplicada al control por parte del empresario de los medios de producción, con independencia de que para lograr que la prueba que se obtenga del control sea eficaz *«tenga que recurrirse a la prueba testifical o pericial sobre el control mismo»*.

Necesidad del establecimiento previo de reglas relativas al uso del ordenador

Una vez establecido que el control del uso del ordenador no se regula por el artículo 18 del ET, el TS afirma que debe estarse a lo establecido en el artículo 20.3 del ET, si bien introduce ciertas matizaciones en cuanto a sus límites y su contenido.

La Sentencia recuerda, como antes se ha mencionado, que el propio artículo 20.3 del ET obliga a que el control guarde la consideración debida a la dignidad del trabajador, lo que, tal y como afirma el TS, *«también remite al respeto a la intimidad»* del propio trabajador. Por ello, el control empresarial del uso del ordenador es un problema más amplio que el de su inclusión o no en el ámbito del artículo 18 del ET, dado que es necesario también determinar su compatibilidad con la intimidad personal del trabajador (artículo 18.1 de la Constitución Española) *«o incluso con el secreto de las comunicaciones, si se tratara del control del correo electrónico»*. El TS menciona a este respecto el artículo 8 del Convenio Europeo para la protección de los Derechos Humanos y la jurisprudencia de nuestro Tribunal Constitucional sobre el derecho a la intimidad, derecho también aplicable en el marco de las relaciones laborales, tal y como recuerda la Sentencia, con cita de la sentencias del Tribunal Constitucional 142/1993, 98/2000 y 186/2000.

En concreto, el TS razona a este respecto que *«determinadas formas de control de la prestación de trabajo pueden resultar incompatibles con ese derecho* (a la intimidad)*, porque aunque no se trata de un derecho absoluto y puede ceder, por tanto, ante «intereses constitucionalmente relevantes», para ello es preciso que las limitaciones impuestas sean necesarias para lograr un fin legítimo y sean también proporcionadas para alcanzarlo y respetuosas con el contenido esencial del derecho. En el caso del uso por el trabajador de los medios informáticos facilitados por la empresa pueden producirse conflictos que afectan a la intimidad de los trabajadores, tanto en el correo electrónico, en el que la implicación se extiende también, como ya se ha dicho, al secreto de las comunicaciones, como en la denominada «navegación» por Internet y en el acceso a determinados archivos personales del ordenador»*.

En este punto, el TS realiza una importante reflexión acerca de *«la existencia de un hábito social generalizado de tolerancia con ciertos usos personales moderados de los medios informáticos y de comunicación facilitados por la empresa a los trabajadores»*, Como consecuencia de esa tolerancia, se crea para el trabajador *«una expectativa también general de confidencialidad en esos usos»;* expectativa que —razona el TS—, si bien *«no puede ser desconocida»* a la hora de llevar a cabo el control empresarial, tampoco puede convertirse en *«un impedimento permanente del control empresarial, porque, aunque el trabajador tiene derecho al respeto a su intimidad, no puede imponer ese respeto cuando utiliza un medio proporcionado por la empresa en contra de las instrucciones establecidas por ésta para su uso y al margen de los controles previstos para esa utilización y para garantizar la permanencia del servicio»*.

De este último inciso extrae el TS la segunda conclusión relevante de la Sentencia, al afirmar que *«lo que debe hacer la empresa de acuerdo con las exigencias de buena fe es establecer previamente las reglas de uso de esos medios —con aplicación de prohibiciones absolutas o parciales— e informar a los trabajadores de que va existir control y de los medios que han de aplicarse en orden a comprobar la corrección de los usos, así como de las medidas que han de adoptarse en su caso para garantizar la efectiva utilización laboral del medio cuando sea preciso, sin perjuicio de la posible aplicación*

de otras medidas de carácter preventivo, como la exclusión de determinadas conexiones». El TS termina su razonamiento afirmando que *«de esta manera, si el medio se utiliza para usos privados en contra de estas prohibiciones y con conocimiento de los controles y medidas aplicables, no podrá entenderse que, al realizarse el control, se ha vulnerado «una expectativa razonable de intimidad»*.

La exigencia de que los trabajadores deben estar previamente advertidos por el empresario de las reglas aplicables sobre el uso y control del ordenador constituye, sin duda, la segunda novedad importante introducida por el TS en su sentencia. Es por esta razón por lo que no debe sorprender que, a pesar de discrepar con la doctrina establecida por la sentencia recurrida del Tribunal Superior de Justicia de Galicia, que aplicó el artículo 18 del ET, el TS confirme dicha sentencia, ya que el recurso se da contra el fallo (que consideró improcedente el despido por obtener de forma ilegítima la prueba) y no contra sus fundamentos o razonamientos jurídicos. Es decir, dado que la empresa no había realizado esa previa advertencia, el TS considera que la prueba fue obtenida ilícitamente y, por ello, que el despido debía ser declarado improcedente, como también fue calificado por el Tribunal Superior de Justicia de Galicia, aunque —determina ahora el TS— con fundamento y razonamientos incorrectos.

La sentencia hace una segunda precisión o matización sobre los límites del control empresarial en virtud de lo establecido en el artículo 20.3 del ET, relativo al alcance de la protección de la intimidad. Así, afirma que *«la garantía de la intimidad también se extiende a los archivos personales del trabajador que se encuentran en el ordenador»*. Es verdad que el TS considera que en el presente caso ello podría ser más discutible, pues no se trataba de *«comunicaciones, ni de archivos personales, sino de los denominados archivos temporales, que son copias que se guardan automáticamente en el disco duro de los lugares visitados a través de Internet»*, tratándose, más bien, *«de rastros o huellas de la «navegación» en Internet y no de informaciones de carácter personal que se guardan con carácter reservado»*.

Pero el TS entiende que *«estos archivos también entran, en principio, dentro de la protección de la intimidad, sin perjuicio de lo ya dicho sobre las advertencias de la empresa. Así lo establece la sentencia de 3 de abril de 2007 del Tribunal Europeo de Derechos Humanos cuando señala que están incluidos en la protección del artículo 8 del Convenio Europeo de derechos humanos «la información derivada del seguimiento del uso personal de Internet» y es que esos archivos pueden contener datos sensibles en orden a la intimidad, en la medida que pueden incorporar informaciones reveladores sobre determinados aspectos de la vida privada (ideología, orientación sexual, aficiones personales, etc.)»*.

Aplicando la anterior doctrina al supuesto que enjuicia, el TS considera que dado que los archivos temporales registraron la actividad del director general, la medida adoptada por la empresa de analizar su contenido *«sin previa advertencia sobre el uso y el control del ordenador, supone una lesión a su intimidad»*. Y si bien el TS admite que el examen inicial del ordenador podía justificarse por la existencia de un virus informático, lo que no encuentra justificación es que la actuación empresarial no se detuviera en *«tareas de detección y reparación, sino que* [...] *«se siguió con el examen del ordenador» para entrar y apoderarse de un archivo cuyo examen o control no puede considerarse que fuera necesario para realizar la reparación interesada»*.

Por último, y como se apuntaba al comienzo, aunque la Sentencia supone una novedad importante y otorga una significada, aunque relativa, seguridad jurídica acerca de algunos de los puntos controvertidos hasta la fecha sobre este tipo de control empresarial, lo cierto es que, probablemente, deja sin contestación todavía algunos aspectos sobre esta materia. El principal aspecto no aclarado vendría referido al derecho al secreto de las comunicaciones y su incidencia en los límites y la forma del control empresarial de los medios informáticos. Así, las comunicaciones de carácter personal que realice el empleado utilizando los medios de la empresa (por ejemplo, el correo electrónico), en principio, estarán protegidas por el secreto de las comunicaciones (no solo por el derecho a la intimidad) y, por ello, cabría preguntarse si bastará con que el empresario prohíba dichas comunicaciones personales, para que éste pueda revisar el contenido de tales comunicaciones si el empleado, incumpliendo la prohibición empresarial establecida, finalmente las realiza.

En este sentido, debe recordarse que el artículo 197 del Código Penal establece una pena para aquellos que se apoderen de mensajes de correo electrónico o cualesquiera otros documentos o efectos personales de terceros o intercepten sus telecomunicaciones. Es igualmente necesario recordar que el artículo 18.3 de la Constitución Española garantiza el secreto de las comunicaciones, salvo resolución judicial, requisito éste que, a día de hoy, es irrealizable en el ámbito de la jurisdicción social española.

Por ello, sin perjuicio de la importante novedad y efecto clarificador de la Sentencia comentada, será

necesario seguir atentos a los pronunciamientos que se produzcan sobre esta materia y que pudieran, en su caso, aclarar los aspectos aún necesitados de clarificación sobre los límites y la forma del control empresarial de la utilización de los medios informáticos por parte de los empleados.

Conclusiones

La sentencia admite que el empresario puede controlar el uso del ordenador facilitado al trabajador y que ese control está amparado y regulado por el artículo 20.3 del ET y no por el artículo 18 del ET. No obstante, al existir en la empresa ciertas expectativas razonables de intimidad en relación con el uso del ordenador, entra en juego el derecho a la intimidad por lo que la empresa debe advertir, previamente, a los trabajadores de las reglas de uso de los medios electrónicos y de los controles que se pueden efectuar.

Por último, y sin perjuicio de lo anterior, seguirá siendo recomendable, además de la realización de esas advertencias previas, que en los controles que se lleven a cabo se respeten el principio y los criterios de proporcionalidad, en los términos que ha establecido el Tribunal Constitucional y que han sido seguidos por los tribunales laborales, sobre todo en aquellos casos en los que el resultado del control llevado a cabo haya de servir como prueba en un procedimiento judicial de carácter laboral, como seguramente sucederá en la mayoría de supuestos.

SERGIO PONCE RODRÍGUEZ (*)

LA CONSERVACIÓN DE LOS DATOS POR LOS OPERADORES DE SERVICIOS DE COMUNICACIONES ELECTRÓNICAS. ANÁLISIS DE LA LEY 25/2007, DE 18 DE OCTUBRE, SOBRE CONSERVACIÓN DE DATOS RELATIVOS A LAS COMUNICACIONES ELECTRÓNICAS Y A LAS REDES PÚBLICAS DE COMUNICACIONES

Introducción

Son dos los hitos normativos recientes en materia de protección de datos. Por un lado, está la Ley 25/2007, de 18 de octubre, sobre conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones (la «*Ley de Conservación de Datos*» o la «*Ley*») y que se analizará en este artículo. Por otra parte, está la recentísima publicación el pasado 19 de enero del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (respectivamente, el «*Reglamento*» y la «*Ley Orgánica de Protección de Datos*») y cuyo clausulado será analizado en próximos números de esta publicación.

Acostumbrados como estamos a que nuevas tecnologías alteren nuestra vida cotidiana y contribuyan a la paulatina invasión de nuestra intimidad, no nos debe extrañar que el legislador nacional y el comunitario se ocupen con determinación de regular el uso de los datos personales en una sociedad cada vez más tecnológica. Precisamente esta creciente preocupación social y política por un uso potencialmente nocivo de los avances tecnológicos en comunicaciones electrónicas —especialmente tras los graves atentados terroristas de Madrid y Londres— es la que ha impulsado la aprobación de la Directiva 24/2006/CE sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones (la «*Directiva 24/2006/CE*»). La transposición al ordenamiento español de la Directiva 24/2006/CE es el principal objetivo de la Ley de Conservación de Datos.

La obligación de conservar los datos responde a la voluntad de los Estados de acceder a determinados datos relativos a las comunicaciones realizadas por los ciudadanos, para luchar contra el terrorismo, la delincuencia organizada y otra serie de delitos graves que pueden encontrar en las comunicaciones electrónicas y en el uso de redes públicas nuevas formas de delinquir o de mantenerse impunes. Históricamente, los operadores de este tipo de servicios podían mantener en sus archivos sólo aquellos datos necesarios para la prestación del servicio y su facturación. Sin embargo, estos datos se habían manifestado insuficientes para las autoridades policiales, bien porque no contenían todos los extremos necesarios para una actuación eficaz, bien porque los datos eran cancelados por los operadores una vez terminaban sus responsabilidades por la facturación.

Por todo ello, la Directiva 24/2006/CE y su transposición española imponen a los prestadores de servicios de comunicaciones electrónicas y de redes públicas de comunicación (p.e., los prestadores de

(*) Abogado del Área Fiscal y Laboral de Uría Menéndez (Madrid).