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).

servicios de telefonía fija, móvil o por Internet) la obligación de conservar una serie de datos de tráfico, localización y otros datos de sus usuarios que se generan como consecuencia del uso de los servicios. La finalidad de la conservación es que, con posterioridad, las autoridades policiales puedan reclamar tales datos a los operadores —previa autorización judicial— y utilizarlos en el curso de la investigación, prevención y persecución de delitos.

Si bien la Directiva 24/2006/CE no es la primera norma que regula la intervención de las autoridades policiales en las comunicaciones (materia ya tratada, por ejemplo, en las normas de interceptación), ni es el primer intento del legislador comunitario de regular una obligación general de conservación de los datos de tráfico y localización, sí se puede afirmar que la Directiva 24/2006/CE es uno de los pasos más contundentes dados por el legislador comunitario para controlar los posibles efectos nocivos de la tecnología en las sociedades democráticas. Tanto es así que las propias Autoridades Europeas de Protección de Datos, en el Dictamen 4/2005 del Grupo sobre Protección de Datos del Artículo 29 sobre la propuesta de la Directiva 24/2006/CE, no han dudado en señalar que esta nueva regulación «*nos sitúa frente a una decisión histórica*». Esta calificación se debe principalmente a que, mientras que la mayoría de las medidas legislativas adoptadas hasta la fecha actuaban de manera «reactiva» —esto es, cuando hay una sospecha de conducta antijurídica—, la obligación de conservar los datos impuesta a los operadores por la Directiva 24/2006/CE y por la Ley de Conservación de Datos se establece con carácter general (respecto de los datos de todos los usuarios de los servicios) y preventivo (sin necesidad de que existan sospechas de antijuricidad).

Este carácter general y preventivo fue examinado por el propio legislador durante la tramitación de la norma y originó un importante debate interno en diversas instituciones y autoridades comunitarias sobre el alcance y la proporcionalidad de la injerencia de los poderes públicos en los derechos y libertades individuales en una sociedad democrática, incluso en los casos en los que los fines perseguidos son legítimos. Esta cuestión ha generado también un intenso debate social y ha motivado que diversas asociaciones de usuarios hayan alegado que la norma supone un menoscabo de sus libertades desproporcionado a los fines perseguidos y, más en particular, que lesiona sus derechos fundamentales a la intimidad, al secreto de las comunicaciones y a la protección de los datos personales. Sin embargo, los riesgos de menoscabo de los mencionados derechos pretenden quedar mitigados por la propia norma, que establece que, si bien la conservación de los datos tiene un carácter general, la cesión de los datos a las autoridades policiales para la persecución de los delitos solamente podrá realizarse caso a caso, cuando exista una resolución judicial específica que ampare tal cesión.

Una última y necesaria consideración antes de comenzar el análisis de la norma es la de su impacto y consecuencias económicas. Para cumplir con la obligación de conservación, los operadores se van a ver obligados a almacenar millones de datos relativos a las comunicaciones realizadas por sus usuarios. El coste en el que deberán incurrir los operadores en la adaptación de sus sistemas para la recogida de los datos, en adquirir dispositivos con capacidad suficiente para almacenarlos y en implantar las medidas de seguridad adecuadas no es en absoluto despreciable. Este impacto económico, que deberá ser asumido por los operadores, es el principal argumento esgrimido por éstos para oponerse a la norma que, pese al rechazo manifestado por operadores y usuarios, ha sido finalmente adoptada.

Antecedentes legislativos

La Unión Europea y los Estados miembros han venido planteándose durante décadas la utilidad de establecer medidas generales de conservación de datos. Sin entrar a enumerar los numerosos convenios, dictámenes, recomendaciones y documentos de trabajo de las distintas autoridades españolas y europeas que han tratado esta cuestión, se exponen a continuación las disposiciones normativas que constituyen el antecedente más inmediato a la Ley de Conservación de Datos, tanto a escala comunitaria como nacional.

Los primeros antecedentes se encuentran en la Directiva 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y en la posterior Directiva 2002/58/CE, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y que deroga la Directiva 97/66/CE. En esta directivas se introduce la posibilidad de que los Estados miembros limiten el alcance de determinados derechos de protección de datos cuando tal limitación constituya una medida necesaria para la salvaguardia de intereses como la seguridad del Estado o la investigación de infraccio-

nes penales, si bien esta posibilidad se regula en unos términos algo imprecisos.

En España, coincidiendo con la tramitación de la Directiva 2002/58/CE, se incluyó en el texto de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico, la obligación de los prestadores de servicios de comunicaciones de retener los datos de tráfico. Sin embargo, como había ocurrido con las Directivas 95/46/CE y 2002/58/CE, la vaguedad de sus términos y la remisión a una regulación de desarrollo que nunca se concretó hicieron que esta obligación de conservación no llegara a materializarse. Los artículos de la Ley 34/2002 que regulaban esta cuestión han sido derogados expresamente por la Ley de Conservación de Datos.

Así las cosas, no ha sido hasta la aprobación de la Directiva 24/2006/CE y su fiel transposición en España por medio de la Ley de Conservación de Datos cuando se ha concretado y hecho efectiva en nuestro país la obligación de conservación de datos por los operadores y su ulterior cesión a las autoridades policiales para la persecución de infracciones penales.

Estructura de la Ley

La Ley de Conservación de Datos, que entró en vigor a los veinte días de su publicación el pasado mes de octubre, cuenta con un breve texto de diez artículos, agrupados en tres capítulos, y con una serie de disposiciones adicionales y finales. Entre estas materias finales está, por ejemplo, la obligación de identificar a los usuarios de las tarjetas prepago de servicios telefónicos (que hasta el momento permanecían anónimos) o la modificación de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones (la «*Ley General de Telecomunicaciones*») para adaptarla a las novedades introducidas por la propia Ley de Conservación de Datos y, más en particular, en lo relativo al secreto de las comunicaciones.

El contenido de la Ley de Conservación de Datos

Objeto de la Ley

La Ley de Conservación de Datos tiene un doble objeto: (i) imponer a los operadores la obligación de conservación de los datos de tráfico, localización e identificación de usuarios; y (ii) regular los términos de la cesión de tales datos a las autoridades policiales al amparo de la correspondiente autorización judicial y para fines de detección, investigación y enjuiciamiento de delitos graves.

Aunque la génesis de la Directiva 24/2006/CE se encuentra en la lucha contra el terrorismo y la delincuencia organizada, tanto la Directiva 24/2006/CE como la Ley de Conservación de Datos han desechado la idea de limitar su alcance a la persecución de los delitos de terrorismo. Tampoco han optado por establecer un listado cerrado de delitos. Por el contrario, ambas normas han optado por delimitar el alcance de la obligación de cesión a la investigación y enjuiciamiento de «*delitos graves*», remitiéndose a lo que se establezca en el Código Penal o en las leyes penales especiales en cada momento para concretar este concepto.

La única excepción a esta regla la encontramos en la disposición adicional única, que señala que la obligación de identificación de los usuarios de los servicios de telefonía mediante tarjetas de prepago tiene como finalidad la «*investigación, detección y enjuiciamiento de un delito*», sin exigir que la infracción deba ser calificada como «grave».

Sujetos afect1ados

Este apartado se referirá a los operadores (como los sujetos obligados por la Ley), a las autoridades policiales nacionales (como beneficiarios de la cesión de los datos) y, finalmente, a los usuarios de los servicios de comunicación (como titulares de los datos que serán conservados).

(i) *Los operadores*

Los sujetos obligados a conservar y, en su caso, a ceder los datos son, de acuerdo con la dicción literal de la Ley, los «*operadores que prestan servicios de comunicaciones electrónicas disponibles al público o que explotan una red pública de comunicaciones electrónicas*» en España. Esta definición debe integrarse con las definiciones de estos servicios que se encuentran en las normas de telecomunicaciones y, en particular, en la Ley General de Telecomunicaciones, a la que la Ley de Conservación de Datos se remite expresamente. Así, en el concepto de operador se encuentran incluidos, entre otros, los proveedores de acceso a Internet y los operadores de telefonía fija, móvil o por Internet, aunque la constante evolución de los medios de comunicación hace complicado avanzar el tipo de comunicación y las categorías de operadores que deberán tenerse en cuenta en el futuro a los efectos de la aplicación de las normas de conservación de datos.

(ii) *Los agentes facultados*

El legislador nacional hace uso de la libertad otorgada por la Directiva 24/2006/CE a los Estados miembros para designar las autoridades policiales nacionales a las que se podrán ceder los datos conservados y, en el artículo 6 de la Ley, señala cuáles son los agentes facultados para acceder a los datos conservados por los operadores.

En concreto, tienen la consideración de «*agentes facultados*» únicamente los miembros de las Fuerzas y Cuerpos de Seguridad y los funcionarios de la Dirección Adjunta de Vigilancia Aduanera, en ambos casos cuando desempeñen funciones de policía judicial, así como el personal del Centro Nacional de Inteligencia en el curso de las investigaciones de seguridad sobre personas o entidades. La Ley de Conservación de Datos se remite a la legislación específica de cada uno de los mencionados cuerpos para determinar el contenido y límite de sus potestades y establece que el acceso de los agentes facultados a los datos deberá estar amparado siempre por una resolución judicial. Hay que apuntar que la definición de los sujetos destinatarios de los datos establecida en la disposición adicional única, que se refiere a la identificación de usuarios en los servicios de telefonía mediante tarjetas de prepago, es ligeramente distinta a la de los agentes facultados establecida en el cuerpo de la Ley con carácter general.

(iii) *Los usuarios*

Los usuarios de los servicios de comunicaciones electrónicas y de redes públicas de comunicación, que podrán ser personas físicas o jurídicas, se ven afectados por la norma en tanto que determinados datos relativos a las comunicaciones que realicen serán recogidos y almacenados por los operadores y podrán ser posteriormente cedidos a los agentes facultados para su uso en la investigación de delitos graves.

La injerencia en los derechos de los usuarios a la intimidad, al secreto de las comunicaciones —que protege no sólo el contenido de la comunicación, sino también otros aspectos como, por ejemplo, la identidad de los interlocutores— y a la protección de los datos personales que supone la obligación de conservación, aunque evidente, queda al menos parcialmente mitigada por el establecimiento de las garantías contenidas en la propia Ley de Conservación de Datos y que tienen por objeto respetar los pronunciamientos que, en relación con el derecho al secreto de las comunicaciones, ha venido emitiendo el Tribunal Constitucional. Entre estas cautelas destacan dos: en primer lugar, que los datos que van a ser conservados sean datos vinculados a la comunicación pero que en ningún caso revelarán el contenido de ésta; y, en segundo lugar, que la cesión de tales datos afectará a una comunicación concreta, y exigirá, en todo caso, autorización judicial previa.

Otra de las garantías establecidas en favor de los usuarios es la aplicación de las normas de protección de datos personales al tratamiento que realicen los operadores, para garantizar la calidad, confidencialidad y seguridad de los datos conservados. En este sentido, los usuarios gozarán de los derechos y las garantías reconocidas en la Ley Orgánica de Protección de Datos y su normativa de desarrollo, con la excepción de algunas previsiones específicas respecto al ejercicio de los derechos de acceso y cancelación de los datos, puesto que se ha considerado que el ejercicio por los usuarios de tales derechos respecto de los datos conservados supondría un obstáculo insalvable para la consecución de la finalidad de investigación y detección de delitos que la Ley persigue.

El derecho a la protección de datos personales se reconoce únicamente respecto de los datos de las personas físicas. Sin perjuicio de la defectuosa redacción del artículo 8 de la Ley (que establece únicamente que las normas de protección de datos serán «*aplicables a los datos contemplados en la presente Ley*»), parece desprenderse de la norma la intención de que las normas de seguridad en materia de protección de datos personales se apliquen también a los datos de los usuarios personas jurídicas, atribuyendo competencias en esta materia a la Agencia Española de Protección de Datos (de forma similar a la técnica empleada en materia de *spam* en las normas de comercio electrónico y de telecomunicaciones).

Datos objeto de conservación

Los datos que deben ser conservados son los datos de tráfico, localización y otros datos necesarios para identificar al abonado o usuario registrado, pero en ningún caso incluyen datos relativos al contenido de las comunicaciones.

La norma española, en el artículo en el que detalla los datos concretos que quedan sujetos a la obliga-

ción de conservación, ha reproducido, casi con exactitud, el listado contenido en la Directiva 24/2006/CE. Este listado comprende los datos necesarios para: (i) rastrear e identificar el origen y el destino de la comunicación; (ii) determinar su fecha, hora y duración; (iii) identificar el tipo de comunicación y el equipo de comunicación utilizado; e (iv) identificar la localización en los casos de equipos de comunicación móvil.

Además, la Ley de Conservación de Datos incluye en su ámbito de aplicación la conservación de los datos relativos a las denominadas «*llamadas telefónicas infructuosas*», entendiendo como tales las comunicaciones en las que se realiza con éxito una llamada telefónica que, sin embargo, no tiene contestación o en las que en la contestación ha intervenido el operador. Por el contrario, quedan excluidos de las obligaciones de conservación los datos relativos a las «*llamadas no conectadas*», esto es, los casos en los que se realiza sin éxito una llamada telefónica y sin que haya habido intervención del operador.

Una de las cuestiones que la Ley de Conservación de Datos ha querido dejar resuelta es la de la identificación de los usuarios de teléfonos móviles que funcionan bajo la modalidad de prepago. Ha quedado demostrado que este tipo de servicios, que amparan el anonimato del usuario, son los que de manera más frecuente se utilizan en la comisión de actos delictivos. Por ello, la disposición adicional única de la Ley obliga a los operadores de servicios de telefonía móvil que comercialicen servicios de tarjetas de prepago a llevar, desde la entrada en vigor de la Ley, un libro-registro en el que conste la identidad de los usuarios que adquieran una tarjeta de este tipo, quedando tales datos sometidos a la Ley de Conservación de Datos. Lo anterior dejaba sin resolver la situación de las tarjetas prepago adquiridas con anterioridad a la entrada en vigor de esta Ley, para las que se ha establecido que los operadores dispondrán de un plazo de dos años para cumplir con las obligaciones de identificación señaladas, transcurrido el cual deberán anular o desactivar aquellas tarjetas cuyos titulares no hayan podido identificar (y sin perjuicio de la compensación que, en su caso, pueda corresponder al titular de las tarjetas por el saldo pendiente de consumo).

El periodo de conservación de los datos

Una de las cuestiones más debatidas de la Ley (y que afecta de una manera más directa a los costes que deberán asumir los operadores) es la referida al periodo de conservación de los datos. Mientras que la Directiva 24/2006/CE se limita a establecer que el periodo de retención no deberá ser inferior a seis meses ni superior a dos años —dejando al arbitrio del legislador nacional la determinación del plazo concreto dentro de los límites señalados—, la norma española ha optado por una solución que parece, al menos en parte, provisional.

En concreto, de acuerdo con lo establecido en el artículo 5 de la Ley, la obligación de conservación cesará a los doce meses computados desde la fecha en que se haya producido la comunicación, aunque reglamentariamente y previa consulta a los operadores, se podrá ampliar o reducir el plazo de doce meses para determinados datos hasta un máximo de dos años o un mínimo de seis meses. Los criterios que se tendrán en cuenta para determinar la conveniencia de establecer plazos reducidos o ampliados son, principalmente, el coste del almacenamiento de los datos y el interés de los datos para la investigación de delitos graves, sin perjuicio de otros criterios que puedan ser expuestos por los operadores en el preceptivo trámite de consulta. De este modo, hasta que reglamentariamente no se establezca otra cosa, todos los datos sujetos a la obligación de conservación se deberán almacenar durante el plazo de doce meses señalado por defecto.

Hay que destacar, por último, que el legislador nacional no ha hecho valer hasta el momento la previsión contenida en la Directiva 24/2006/CE por la que se permite a los Estados miembros una ampliación limitada del período máximo de conservación de dos años, previo control de la Comisión Europea y justificación de las «*circunstancias especiales*» que justifiquen la medida.

La obligación de ceder los datos

La Directiva 24/2006/CE dirige un mandato al legislador nacional para que garantice que los datos conservados puedan transmitirse «*sin demora*» cuando las autoridades competentes así lo soliciten. Para observar este mandato, la norma española ha establecido las reglas que los operadores deberán seguir para la cesión de los datos a los agentes facultados.

El presupuesto esencial de toda cesión es la existencia de una resolución judicial que así lo requiera y que deberá determinar los datos conservados que han de ser cedidos y el plazo de ejecución de la orden de cesión. En el caso de que la resolución no establezca un plazo concreto, la cesión deberá efec-

tuarse en el plazo de las setenta y dos horas contadas a partir de las ocho horas del día laborable siguiente a aquél en el que el operador reciba la orden. Las cualidades que la Ley predica respecto de la resolución judicial es que deberá ser conforme con los principios de necesidad y proporcionalidad y con lo previsto al respecto en la Ley de Enjuiciamiento Criminal.

Protección y seguridad de los datos conservados. La aplicación de las normas de protección de datos personales

El tratamiento de los datos que realicen los operadores, tanto durante la recogida y almacenamiento de los datos como en su posterior cesión en virtud de una resolución judicial, deberá cumplir una serie de requisitos de seguridad que impidan el uso de los datos para fines distintos de los establecidos en la Ley, su destrucción o pérdida accidental o su tratamiento o divulgación no autorizados. Para asegurar la debida protección de los datos conservados y el respeto al derecho a la protección de datos de los usuarios, la Ley exige a los operadores la adopción de las garantías establecidas en la normativa de protección de datos personales y, más en particular, de las medidas de seguridad técnicas y organizativas contenidas en la Ley Orgánica de Protección de Datos y en su normativa de desarrollo.

En concreto, las normas españolas de protección de datos establecen una serie de medidas de seguridad mínimas obligatorias y que se clasifican en tres niveles (básico, medio y alto) en función del tipo de datos y tratamientos realizados. Las medidas de seguridad mínimas obligatorias que el reciente Reglamento de desarrollo de la Ley Orgánica de Protección de Datos ha asignado a los ficheros de datos de tráfico y de localización son las de nivel medio, junto con la medida de seguridad de nivel alto relativa al registro de accesos. La asignación de este nivel de medidas de seguridad ha contado con la oposición de los operadores, que tendrán el plazo de un año desde la entrada en vigor del citado Reglamento para implantar las medidas de seguridad de nivel medio y de dieciocho meses para implantar la medida de nivel alto exigida. La implantación en los sistemas de los operadores de las medidas de seguridad de nivel medio y alto requeridas supondrá a los operadores importantes costes y complicaciones técnicas, que se sumarán a los costes en los que deberán incurrir en cumplimiento de los deberes de conservación.

Régimen sancionador

El incumplimiento de las obligaciones previstas en la Ley se sancionará de acuerdo con lo dispuesto en la Ley General de Telecomunicaciones, cuyas sanciones, en los casos más graves, pueden llegar a la imposición de multas por un importe no inferior al tanto, ni superior al quíntuplo, del beneficio bruto obtenido como consecuencia de la infracción o, en caso de que no resulte posible aplicar este criterio, por importe máximo de dos millones de euros. Además, en función de las circunstancias, se podrán imponer otras sanciones como una inhabilitación para prestar servicios de hasta de cinco años o la publicación de la sanción.

Este régimen sancionador propio de la normativa administrativa de telecomunicaciones debe entenderse sin perjuicio de la aplicación de los otros dos regímenes sancionadores previstos expresamente en la Ley: el penal (por incumplimientos de la obligación de cesión de los datos a los agentes facultados establecida en una resolución judicial) y el administrativo sancionador previsto en la Ley Orgánica de Protección de Datos (por infracciones en materia de protección de datos personales). En este último caso, será la Agencia Española de Protección de Datos la autoridad pública encargada de velar por el cumplimiento de las normas de protección de datos ya mencionadas.

Como ocurre con otras normas, la coexistencia de varios regímenes sancionadores para el control de una misma actividad (aunque protegiendo bienes jurídicos distintos) puede dar lugar, en algún caso, a problemas prácticos de interpretación. Dadas las importantes sanciones establecidas en la Ley General de Telecomunicaciones, las cuantiosas multas previstas en las normas de protección de datos y la relevancia de los procesos penales, cabe plantearse cuál será la postura que adoptarán las distintas autoridades competentes ante esta pluralidad de regímenes sancionadores en aquellos supuestos en los que sea difícil deslindar los bienes jurídicos lesionados. A la luz del precedente existente en materia de *spam*, cabe anticipar, al menos en el caso de usuarios personas físicas, que se apliquen cumulativamente la Ley y la normativa de protección de datos.

Consideraciones finales

La Ley de Conservación de Datos es el fruto de un intenso debate jurídico, social y económico que ha durado décadas. A pesar de que la obligación de conservación de datos no ha resultado una sorpresa

para los diversos agentes económicos involucrados, su implantación no deja de plantear numerosas cuestiones de índole práctica. La Ley establece un período de seis meses para que los operadores puedan adaptar sus equipos para cumplir las obligaciones de conservación y cesión de datos. Esta adaptación puede resultar compleja y más teniendo en cuenta que se requiere un desarrollo normativo adicional para completar algunas de las cuestiones planteadas por la Ley (p.e., la reducción o ampliación de algunos plazos de conservación o el formato electrónico definitivo en el que los operadores deberán ceder los datos a los agentes facultados, que se deberá determinar por las autoridades en un plazo de máximo de tres meses desde la aprobación de la Ley).

A nadie se le escapa la complejidad de regular aspectos tecnológicos en continua evolución como los que se abordan en la Directiva 24/2006/CE y en su transposición española. Esto ha hecho que el propio legislador comunitario anticipe la necesidad de revisar de manera constante la regulación de la obligación de conservación, las categorías de datos conservados y los sujetos obligados. En este sentido, la Directiva 24/2006/CE establece que, con anterioridad al 15 de septiembre de 2010, la Comisión presentará al Parlamento Europeo y al Consejo una evaluación de la aplicación de la Directiva 24/2006/CE y su impacto en operadores económicos y consumidores, «*teniendo en cuenta los avances en la tecnología de las comunicaciones electrónicas*». Por ello, es posible anticipar que, aunque la Ley de Conservación supone un primer paso en la regulación de la obligación de conservar los datos, estamos ante una norma que sufrirá una continua revisión.

LETICIA LÓPEZ-LAPUENTE GUTIÉRREZ (*)

LA DIRECTIVA 2007/64/CE, SOBRE SERVICIOS DE PAGO EN EL MERCADO INTERIOR

La Directiva 2007/64/CE, de 13 de noviembre de 2007, sobre servicios de pago en el mercado interior, por la que se modifican las Directivas 97/7/CE, 2002/65/CE, 2005/60/CE y 2006/48/CE y por la que se deroga la Directiva 97/5/CE (en adelante, la «Directiva»), tiene como objetivo instaurar un marco jurídico armonizado, necesario para el correcto funcionamiento del mercado único de los servicios de pago, en el que se pretende suprimir los impedimentos de entrada de nuevos proveedores de servicios. Este nuevo marco reforzará la competencia y ofrecerá a los usuarios un mayor número de opciones y un nivel de protección más elevado.

La Directiva pretende facilitar la iniciativa de autorregulación adoptada por el sector de los pagos en el marco del «Consejo Europeo de Pagos» (*European Payments Council*), consistente en desarrollar, de aquí a 2010, normas técnicas y comerciales comunes para los pagos en euros y crear así una zona única de pago en euros (*Single Euro Payment Area* - «SEPA»)

Ha sido publicada en el Diario Oficial de la Unión Europea (DOUE) el pasado 5 de diciembre de 2007. No obstante, se establece un plazo amplio para su transposición al derecho nacional por los estados miembros, que expirará el 1 de noviembre de 2009.

Ámbito de aplicación

La Directiva se aplicará a todos los servicios de pago que se realicen dentro de la Comunidad, es decir, cuando al menos uno de los proveedores de servicios de pago esté situado en territorio europeo, a excepción de los títulos III y IV (vid. infra) que serán de aplicación únicamente cuando ambos proveedores de servicios estén situados en la Comunidad. Además hemos de tener en cuenta que será de aplicación tanto si los servicios de pago se efectúan en euros, como en cualquier moneda de un estado miembro fuera de la zona euro.

Categorías de proveedores de servicios de pago a las que se dirige la Directiva

La Directiva distingue y se dirige a seis categorías diferentes de proveedores de servicios de pago: (i) las entidades de crédito; (ii) las oficinas de cheques postales, que prestan servicios de pago; (iii) las entidades de dinero electrónico; (iv) las entidades de pago, como nueva categoría regulada por la Directiva; (v) el Banco Central Europeo y los bancos centrales nacionales; y (vi) los Estados miembros y sus autoridades regionales y locales.

Servicios de pago considerados en la Directiva

En la categoría de «servicios de pago» con arreglo al Anexo de la Directiva se incluyen las actividades consistentes en: (i) servicios que permiten el depó-

(*) Abogada del Área de Derecho Mercantil de Uría Menéndez (Madrid).