Anuario Jurídico y Económico Escurialense, **LII (2019) 125-148 / ISSN: 1133-3677**

Nuevas tendencias en materia de protección de datos personales. La nueva Ley Orgánica y la jurisprudencia más reciente

New tendencies in personal data protection.
Analysis of the new Law and the recent case-law

Dra. Gemma MINERO ALEJANDRE
Universidad Autónoma de Madrid

Resumen: Este artículo busca realizar un estudio de dos cuestiones. La primera, los cambios introducidos en el ordenamiento jurídico español por la nueva Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales. La segunda, la jurisprudencia europea más reciente en materia de protección de datos.

Abstract: The aim of this study is to analyze two issues. Firstly, the changes that the new Law in Personal Data Protection has introduced in the Spanish system. Secondly, this article analyses the most recent European case-law on this issue.

Palabras clave: Protección de datos personales, derechos fundamentales, derechos digitales, derecho de desconexión digital.

Keywords: Personal data protection, fundamental rights, digital rights, right to disconnect.

Sumario:

I. Breve análisis de la nueva Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales.

II. Reflexiones sobre la jurisprudencia dictada por el Tribunal de Justicia de la Unión Europea en 2017 y 2018 en la materia.

III. Conclusiones.

IV. Bibliografía.

Recibido: noviembre 2018.
Aceptado: enero 2019.

I. BREVE ANÁLISIS DE LA NUEVA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES Y GARANTÍA DE LOS DERECHOS DIGITALES

El miércoles 21 de noviembre de 2018 el Pleno del Senado aprobaba el Proyecto de Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales, con 221 votos a favor, 21 en contra y ninguna abstención. Los citados votos en contra se corresponden con los partidos Unidos Podemos, Compromís, Nueva Canaria y Bildu. El Pleno ha aprobado el texto que salió adelante en el Congreso de los Diputados, al haberse rechazado las enmiendas que en su día fueron presentadas por Unidos Podemos, Compromís, Ciudadanos y el PDCat. Con fecha de 6 de diciembre de 2018 se publicaba en el BOE la nueva Ley Orgánica (BOE núm. 294), entrando en vigor al día siguiente.

Tal y como se explica en su primer artículo, la nueva Ley Orgánica busca no sólo transponer al ordenamiento jurídico español, con un severo retraso, el Reglamento General de Protección de Datos de 2016[1], que había entrado en vigor el 25 de mayo de 2018, sino que también se ha buscado complementar esta norma y garantizar la eficacia del funcionamiento de los llamados derechos digitales, conforme al mandato previsto en el artículo 18.4 de la Constitución Española[2]. Para ello el legislador parte de una afirmación que ya se llevaba años defendiendo en la doctrina y que había sido adoptada por la jurisprudencia del Tribunal Constitucional: la concepción de la protección de las personas físicas en relación con el tratamiento de datos personales como un derecho fundamental

1 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo 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 por el que se deroga la Directiva 95/46/CE. A nivel europeo, el derecho fundamental a la protección de datos personales se recoge en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea y en el artículo 16.1 del Tratado de Funcionamiento de la Unión Europea.

2 Este precepto constitucional dispuso que "la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos". Conocedor de la insuficiencia de la norma constitucional, el legislador español de 2018 indica en el artículo 2 de la nueva Ley Orgánica que el contenido de ésta "se aplica a cualquier tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero".

propio y completo, protegido por el artículo 18.4 de la Constitución Española, e independiente del resto de derechos fundamentales regulados en esta norma[3]. Este retraso en el cumplimiento de la obligación europea seguramente contribuye a la inminencia de la fecha de entrada en vigor de la nueva Ley Orgánica: el día siguiente de su publicación en el Boletín Oficial del Estado, por aplicación de la disposición final 16ª de esta Ley Orgánica. Como también explica la adopción en verano de 2018 de una norma transitoria, que aborda únicamente determinadas cuestiones que no son objeto de reserva de ley orgánica, para la adaptación del Derecho español al Reglamento General de Protección de Datos: el Real Decreto-ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos, entrado en vigor el 31 de julio de 2018[4].

Este cuerpo normativo se aprueba en mitad de una polémica con importantes repercusiones mediáticas, que tiene que ver con el contenido de uno de los preceptos regulados en la nueva Ley Orgánica. En efecto, la disposición final 3ª introduce una serie de modificaciones de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General. En particular, se añade un nuevo artículo, el 58 bis, que permite la recopilación de datos personales relativos a las opiniones políticas de los ciudadanos y el uso de éstos por partidos políticos

[3] Así se expone igualmente en la Exposición de Motivos de la nueva Ley Orgánica (punto primero). Ya en su sentencia núm. 94/1998, de 4 de mayo, el Tribunal Constitucional configuró el derecho fundamental a la protección de datos como una facultad del ciudadano para oponerse a que determinados datos personales sean usados para fines distintos a aquél que justificó su obtención. Sin embargo, hubo que esperar dos años más, en su sentencia núm. 292/2000, de 30 de noviembre, para encontrar un pronunciamiento en el que el TC considerase el derecho a la protección de datos personales como un derecho autónomo e independiente que consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Véanse, entre otros, MINERO ALEJANDRE, G., "Comentario a la STS de 21 septiembre 2015. Protección de datos personales", en *Cuadernos Civitas de Jurisprudencia Civil*, núm. 101 (2016) 269-287; LUCAS MURILLO DE LA CUEVA, P., «Título I. Disposiciones Generales», en TRONCOSO REIGADA, A. (Dir), *Comentarios a la Ley orgánica de Protección de Datos de Carácter Personal* 2010, Civitas, 2010, p. 79, y, de este mismo autor «La Constitución y el derecho a la autodeterminación informativa», en *Cuadernos de Derecho Público*, núm. 19-20 (2003) 27 y ss; y TRONCOSO REIGADA, A., *La protección de datos personales. En busca del equilibrio,* Tirant Lo Blanch, 2010, p. 70.

[4] En el punto primero de la Exposición de Motivos se justifica la adopción de esta norma de la siguiente manera: "En otras palabras, el objeto de este real decreto-ley se ciñe a la adecuación de nuestro ordenamiento al reglamento europeo en aquellos aspectos concretos que, sin rango orgánico, no admiten demora y debe entenderse sin perjuicio de la necesidad de una legislación orgánica de protección de datos que procure la plena adaptación de la normativa interna a los estándares fijados en la materia por la Unión Europea a través de una disposición directamente aplicable".

para la realización de actividades políticas durante el periodo electoral, así como el envío de propaganda electoral por medios electrónicos, incluyendo redes sociales y sistemas de mensajería[5]. Unidos Podemos, que había solicitado la retirada de este precepto, ha anunciado que llevará al Tribunal Constitucional el texto aprobado. Por su parte, la senadora socialista Begoña Nasarre, en relación a este polémico precepto, ha llamado la atención sobre la necesidad de regular un desarrollo reglamentario de la norma que despeje toda duda, acogiendo el llamamiento realizado por el Senador de ERC Miguel Ángel Estradé a recabar los informes jurídicos correspondientes para evitar aplicaciones indebidas de esta norma. En la fecha de cierre de este trabajo, dicho desarrollo reglamentario aún no se ha aprobado.

La nueva Ley Orgánica consta de 97 artículos, divididos en 10 títulos, 22 disposiciones adicionales, 6 disposiciones transitorias, una disposición derogatoria -de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y del Real Decreto-ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos- y 16 disposiciones finales. A continuación se destacan algunas de las principales novedades introducidas.

En primer lugar, debe hablarse de la regulación contenida en el artículo 3, destinado a la tutela de los datos personales de personas fallecidas. El lector debe partir, asimismo, de la regla prevista en el artículo 2.2.b: la nueva Ley Orgánica no se aplica a los tratamientos de datos de personas fallecidas, "sin perjuicio de lo establecido en el artículo 3". Este artículo 3 es novedoso, pues con anterioridad a su aprobación el fallecimiento de la persona conllevaba la extinción de la tutela de sus datos personales[6]. De forma paralela pero no

5 El texto del nuevo artículo 58 bis de la Ley 5/1985, de 19 de junio, del Régimen Electoral General, es el siguiente: "Utilización de medios tecnológicos y datos personales en las actividades electorales.

1. La recopilación de datos personales relativos a las opiniones políticas de las personas que lleven a cabo los partidos políticos en el marco de sus actividades electorales se encontrará amparada en el interés público únicamente cuando se ofrezcan garantías adecuadas.

2. Los partidos políticos, coaliciones y agrupaciones electorales podrán utilizar datos personales obtenidos en páginas web y otras fuentes de acceso público para la realización de actividades políticas durante el periodo electoral.

3. El envío de propaganda electoral por medios electrónicos o sistemas de mensajería y la contratación de propaganda electoral en redes sociales o medios equivalentes no tendrán la consideración de actividad o comunicación comercial.

4. Las actividades divulgativas anteriormente referidas identificarán de modo destacado su naturaleza electoral.

5. Se facilitará al destinatario un modo sencillo y gratuito de ejercicio del derecho de oposición."

6 Sobre este punto puede leerse MINERO ALEJANDRE, G., *La protección post mortem de los derechos al honor, intimidad y propia imagen y la tutela frente al uso de datos de carácter personal tras el fallecimiento,* Aranzadi, Navarra 2018.

idéntica a la regla prevista en la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen (artículos 4 a 6), la nueva Ley Orgánica de Protección de Datos Personales y garantía de derechos digitales, regula el núcleo de personas legitimadas para dirigirse al responsable o encargado del tratamiento al objeto de solicitar el acceso a los datos personales del fallecido y, en su caso, la solicitud de rectificación o supresión. Estos sujetos -"Las personas vinculadas al fallecido por razones familiares o de hecho así como sus herederos", dice el artículo 3.1, sin especificar el legislador un determinado grado de parentesco, por lo que esta referencia ha de interpretarse de manera amplia- tendrán legitimación para el acceso a los datos personales como regla general, y sólo carecerán de ella cuando la persona fallecida lo hubiera previsto así expresamente. A ello se añade -por mor del artículo 3.2- la legitimación para el acceso, rectificación y supresión de las personas o instituciones a las que el fallecido hubiese designado expresamente para ello, que habrán de actuar con arreglo a las instrucciones recibidas, previendo esta norma la regulación en real decreto de los requisitos y condiciones a aplicar para acreditar "la validez y vigencia de estos mandatos e instrucciones y, en su caso, el registro de los mismos"[7]. Finalmente, se prevé una regla especial para el caso de fallecimiento de menores o personas con discapacidad, indicando el artículo 3.3 que la legitimación para la tutela de sus datos personales podrá ejercerse "por sus representantes legales o, en el marco de sus competencias, por el Ministerio Fiscal, que podrá actuar de oficio o a instancia de cualquier persona física o jurídica interesada", en el primer caso, y, adicionalmente, en el caso de persona con discapacidad, "por quienes hubiesen sido designados para el ejercicio de funciones de apoyo, si tales facultades se entendieran comprendidas en las medidas de apoyo prestadas por el designado"[8].

Los artículos 4 a 10 de la nueva Ley Orgánica, que configuran su Título II, regulan los principios que han de regir el tratamiento y la protección de datos personales. A saber: la exactitud de los datos, el deber de confidencialidad, consentimiento del afectado por el tratamiento de datos, reglas sobre el

[7] Por tanto, la legitimación de este segundo grupo de sujetos se suma a la legitimación del primer grupo, tal y como se desprende el uso del adverbio "también".

[8] Todo ello se asemeja, pero no equivale de forma plena a la regulación contenida en la citada Ley Orgánica 1/1982, para la defensa de los derechos de la personalidad tras el fallecimiento de la persona. En la Ley de 1982 se regula la posibilidad de que la persona prevea en su testamento la identidad de la persona o personas físicas o jurídicas que puedan ejercitar las acciones de protección civil del honor, la intimidad o la imagen de una persona fallecida. No existiendo designación o habiendo fallecido la persona designada, se entienden legitimados para recabar la protección "el cónyuge, los descendientes, ascendientes y hermanos de la persona afectada que viviesen al tiempo de su fallecimiento" (artículo 4.2). A falta de todos ellos, el ejercicio de las acciones de protección corresponderá al Ministerio Fiscal en el plazo de 80 años desde el fallecimiento (artículo 4.3).

consentimiento de los menores de edad[9], el tratamiento de datos por obligación legal o de interés público o en ejercicio de los poderes públicos[10], así como el tratamiento de datos de categorías especiales[11] y de naturaleza penal[12].

En el Título III se regulan de forma detallada los derechos de las personas a la protección de sus datos personales. Entre ellos destaca el artículo 11, que prevé la regla de la información por capas, generalizada en caso de páginas web en las que se instalan mecanismos de almacenamiento masivo de datos personales, como son las cookies, pero también en el ámbito de la video-vigilancia. Esta norma prevé la posibilidad de suministrar al afectado únicamente la información básica, e indicar una dirección electrónica u otro medio que permita a dicho afectado acceder a la restante información de forma sencilla e inmediata. Por su parte, en los artículos 12 a 18 se regulan las formas de ejercicio de los derechos de acceso, rectificación, supresión -el llamado "derecho al olvido"-, limitación del tratamiento, portabilidad y oposición, realizando referencias constantes al Reglamento general de protección de datos. En particular, conforme al artículo 12.2, el responsable del tratamiento estará obligado a informar al afectado sobre los medios a su disposición para ejercer los derechos que le corresponden. Esos medios han de ser fácilmente accesibles para el afectado y, en todo caso, éste podrá optar por un medio diferente para su ejercicio, sin que esta diferente elección sea causa justificativa para denegar el ejercicio del derecho. De cara al ejercicio del derecho de rectificación, el artículo 14 obliga al interesado a acompañar, "cuando sea preciso, la documentación justificativa de la inexactitud o carácter incompleto de los datos objeto de tratamiento".

[9] En particular, el artículo 7 de la nueva Ley Orgánica prevé que el menor de edad pero mayor de catorce años puede consentir el tratamiento de sus datos personales. El tratamiento de datos personales de menores de catorce años, fundado en el consentimiento del menor, ha de completarse con el consentimiento del titular de la patria potestad o tutela.

[10] Previendo el artículo 8 la posibilidad de que el tratamiento de datos personales se funde en el cumplimiento de una obligación legal exigible al responsable o en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable.

[11] En este punto el artículo 9 prevé un plus al consentimiento del afectado, determinando que dicho consentimiento "no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico", sino que el tratamiento habrá de estar amparado en "una norma con rango de ley, que podrá establecer requisitos adicionales relativos a su seguridad y confidencialidad". "En particular, dicha norma podrá amparar el tratamiento de datos en el ámbito de la salud cuando así lo exija la gestión de los sistemas y servicios de asistencia sanitaria y social, pública y privada, o la ejecución de un contrato de seguro del que el afectado sea parte".

[12] Conforme al artículo 10, el tratamiento de datos personales relativos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas, para fines distintos de los de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, sólo podrá llevarse a cabo cuando se encuentre amparado en una norma de rango legal.

En lo que respecta al derecho al olvido, el interesado podrá solicitar al responsable del tratamiento la supresión de los datos personales que le conciernan -y de cualquier réplica de éstos- sin dilación indebida cuando concurran determinadas circunstancias expresamente tipificadas, principalmente las siguientes: a) los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo; b) el interesado retire el consentimiento en que se basa el tratamiento; c) los datos personales hayan sido tratados ilícitamente. Con todo, el ejercicio del derecho al olvido no será posible cuando el concreto tratamiento sea necesario: a) para ejercer el derecho a la libertad de expresión e información; b) para el cumplimiento de una obligación legal que requiera el tratamiento; c) por razones de interés público en el ámbito de la salud pública; d) con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, en la medida en que la supresión de los datos pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento, o e) para la formulación, el ejercicio o la defensa de reclamaciones.

Los artículos 19 a 27, que configuran el Título IV, regulan una serie de reglas especiales aplicables a tratamientos concretos, como son el tratamiento de datos de contacto, de empresarios individuales y de profesionales liberales, los sistemas de información crediticia, los sistemas de exclusión publicitaria, los sistemas de información de denuncias internas, los tratamientos con fines de video-vigilancia, los tratamientos de datos en el ámbito de la función estadística pública y con fines de archivo en interés público por parte de las Administraciones Públicas y tratamiento de datos relativos a infracciones y sanciones administrativas.

Entre las reglas, puede destacarse la licitud del tratamiento de los datos de contacto y en su caso los relativos a la función o puesto desempeñado de las personas físicas que presten servicios en una persona jurídica siempre que el tratamiento se refiera únicamente a los datos necesarios para su localización profesional y su finalidad sea únicamente mantener relaciones de cualquier índole con la persona jurídica en la que el afectado preste sus servicios. Esta misma regla se aplica al tratamiento de los datos relativos a los empresarios individuales y a los profesionales liberales, cuando se refieran a ellos únicamente en dicha condición y no se traten para entablar una relación con los mismos como personas físicas. Será lícito el tratamiento de datos personales que tenga por objeto evitar el envío de comunicaciones comerciales a quienes hubiesen manifestado su negativa u oposición a recibirlas; y a tal efecto, podrán crearse sistemas de información para identificar a los afectados. Asimismo, se prevé que cuando un afectado manifieste a un responsable su deseo de que sus datos no sean tratados para la remisión de comunicaciones comerciales, éste deba informarle de los sistemas de exclusión publicitaria existentes.

En relación al tratamiento de datos con fines de video-vigilancia, se permite la captación de imágenes de la vía pública cuando fuese necesario para garantizar la seguridad de bienes o instalaciones estratégicos o de infraestructuras vinculadas al transporte, sin que en ningún caso pueda suponer la captación de imágenes del interior de un domicilio privado. Habrá de informarse de la colocación del dispositivo de grabación en lugar suficientemente visible, informando de la posibilidad de ejercitar los derechos regulados en los artículos 12 a 18. Los datos así captados serán suprimidos en el plazo de un mes, salvo cuando tuvieran que ser conservados para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones, debiendo en este último supuesto poner las imágenes a disposición de la autoridad competente.

Por su parte, en relación a sistemas de información crediticia, se presume lícito el tratamiento de datos personales relativos al incumplimiento de obligaciones dinerarias, financieras o de crédito, siempre que los datos hayan sido facilitados por el acreedor y éste hubiera informado de la posibilidad de inclusión en el sistema de información crediticia en el momento de la contratación y los datos se refieran a deudas ciertas, vencidas y exigibles, cuya existencia o cuantía no hubiese sido objeto de reclamación administrativa o judicial por el deudor o mediante un procedimiento alternativo de resolución de disputas vinculante entre las partes. La entidad que mantenga el sistema de información crediticia deberá notificar al afectado la inclusión de tales datos y le informará sobre la posibilidad de ejercitar los derechos regulados en los artículos 12 a 18. Únicamente podrá mantener los datos mientras persista el incumplimiento, con el límite máximo de cinco años desde la fecha de vencimiento de la obligación dineraria, financiera o de crédito.

El Título V se ocupa de la regulación de las obligaciones del responsable y del encargado del tratamiento. En primer lugar, habrán de valorar si procede la realización de la evaluación de impacto en la protección de datos, teniendo en cuenta el especial riesgo que podría producirse, entre otros supuestos, cuando el tratamiento pudiera generar situaciones de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico, moral o social significativo para los afectados, cuando el tratamiento implicase una evaluación de aspectos personales de los afectados con el fin de crear o utilizar perfiles personales de los mismos, en particular mediante el análisis o la predicción de aspectos referidos a su rendimiento en el trabajo, su situación económica, su salud, sus preferencias o intereses personales, su fiabilidad o comportamiento, su solvencia financiera, su localización o sus movimientos y cuando se produzca un tratamiento masivo que implique a un gran número de afectados o conlleve la recogida de una

gran cantidad de datos personales. En segundo lugar, los responsables y encargados del tratamiento deberán mantener el registro de actividades de tratamiento. El responsable del tratamiento estará obligado a bloquear los datos cuando proceda a su rectificación o supresión, lo que implicará la adopción de medidas técnicas y organizativas, para impedir su tratamiento, incluyendo su visualización, excepto para la puesta a disposición de los datos a los jueces y tribunales, el Ministerio Fiscal o las Administraciones Públicas competentes.

Conforme al artículo 34, los responsables y encargados del tratamiento deberán designar un delegado de protección de datos -persona que habrá de acreditar la obtención de una titulación universitaria que acredite conocimientos especializados en el derecho y la práctica en materia de protección de datos- cuando se trate de las siguientes entidades: a) Los colegios profesionales y sus consejos generales; b) Los centros docentes que ofrezcan enseñanzas en cualquiera de los niveles establecidos en la legislación reguladora del derecho a la educación, así como las Universidades públicas y privadas; c) Las entidades que exploten redes y presten servicios de comunicaciones electrónicas conforme a lo dispuesto en su legislación específica, cuando traten habitual y sistemáticamente datos personales a gran escala; d) Los prestadores de servicios de la sociedad de la información cuando elaboren a gran escala perfiles de los usuarios del servicio; e) Las entidades de ordenación, supervisión y solvencia de entidades de crédito; f) Los establecimientos financieros de crédito; g) Las entidades aseguradoras y reaseguradoras; h) Las empresas de servicios de inversión, reguladas por la legislación del Mercado de Valores; i) Los distribuidores y comercializadores de energía eléctrica y los distribuidores y comercializadores de gas natural; j) Las entidades responsables de ficheros comunes para la evaluación de la solvencia patrimonial y crédito; k) Las entidades que desarrollen actividades de publicidad y prospección comercial; l) Los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes; m) Las entidades que tengan como uno de sus objetos la emisión de informes comerciales que puedan referirse a personas físicas; n) Los operadores que desarrollen la actividad de juego a través de canales electrónicos, informáticos, telemáticos e interactivos, conforme a la normativa de regulación del juego; ñ) Las empresas de seguridad privada; y o) Las federaciones deportivas cuando traten datos de menores de edad.

Conforme prevé el artículo 36, el delegado de protección de datos actuará como interlocutor del responsable o encargado del tratamiento ante la Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos, pudiendo emitir recomendaciones en el ámbito de sus competencias. El delegado de protección de datos, persona física, no podrá ser removido ni sancionado por el responsable o el encargado por desempeñar

sus funciones salvo que incurriera en dolo o negligencia grave en su ejercicio, y se deberá garantizar su independencia dentro de la organización, debiendo evitarse cualquier conflicto de intereses. Cuando el delegado aprecie la existencia de una vulneración relevante en materia de protección de datos lo documentará y lo comunicará inmediatamente a los órganos de administración y dirección del responsable o el encargado del tratamiento.

Finalmente, los artículos 38 y 39 regulan los llamados Códigos de conducta y certificación, regulados igualmente en el Reglamento general de protección de datos. Los códigos de conducta serán vinculantes para quienes se adhieran a los mismos, de forma que los responsables o encargados del tratamiento que se adhieran al código de conducta se obligan a someter al organismo o entidad de supervisión -cuya acreditación corresponde a la Entidad Nacional de Acreditación y será comunicada a la Agencia Española de Protección de Datos y a las autoridades de protección de datos de las Comunidades Autónomas- las reclamaciones que les fueran formuladas por los afectados por los tratamientos de sus datos personales, y además podrán voluntariamente y antes de llevar a cabo el tratamiento, someter al citado organismo o entidad de supervisión la verificación de la conformidad del mismo con las materias sujetas al código de conducta. En todo caso, el afectado podrá formular posteriormente la reclamación ante la Agencia Española de Protección de Datos.

El Título VI regula las reglas aplicables a las transferencias internacionales de datos. Se sigue con ello lo dispuesto en el Reglamento General de Protección de Datos, estableciéndose los procedimientos a emplear por las autoridades de protección de datos para las normas corporativas vinculantes y los supuestos de autorización de una determinada transferencia, debiendo informar los responsables del tratamiento a los afectados con carácter previo a la transferencia.

El Título VII regula la organización y el funcionamiento de la Agencia Española de Protección de Datos y de las Autoridades autonómicas de protección de datos, determinando, entre otros aspectos, su régimen jurídico, presupuestario y de personal, así como sus funciones y potestades. Ello se complementa con las disposiciones transitorias reguladoras del estatuto de la Agencia.

Por su parte, en los artículos 63 a 69, que configuran el Título VIII, se regula el régimen jurídico de los procedimientos sancionadores por vulneración de la normativa de protección de datos tramitados por la Agencia Española de Protección de Datos. En el procedimiento más común, esto es, aquel que se inicia en relación a la falta de atención de una solicitud de ejercicio de los derechos establecidos en los artículos, la Agencia Española de Protección de Datos tiene un plazo de 6 meses para resolver, a contar desde la notificación

al afectado del acuerdo de admisión. Transcurrido ese plazo, el interesado podrá considerar estimada su reclamación. Antes de la adopción del acuerdo de inicio del procedimiento, y una vez admitida a trámite la reclamación si la hubiese, la Agencia Española de Protección de Datos podrá llevar a cabo actuaciones previas de investigación para la mejor determinación de los hechos y las circunstancias que justifican la tramitación del procedimiento. Durante la realización de las actuaciones previas de investigación o iniciado un procedimiento para el ejercicio de la potestad sancionadora, la Agencia Española de Protección de Datos podrá acordar motivadamente las medidas provisionales necesarias y proporcionadas para salvaguardar el derecho fundamental a la protección de datos, como pueden ser, entre otras el bloqueo cautelar de los datos, la cesación del tratamiento y la obligación inmediata de atender el derecho solicitado.

Ello se complementa con el Título IX, en el que se prevé el régimen sancionador. Los artículos 72 a 74 regulan los listados enumerativos de las infracciones muy graves -por ejemplo, la utilización de los datos para una finalidad no compatible con aquella para la que fueron recogidos, sin contar con el consentimiento del afectado y sin tener base legal para ello-, graves -por ejemplo, no poder acreditar la realización de esfuerzos razonables para verificar la validez del consentimiento prestado por un menor de edad o por el titular de su patria potestad o tutela -y leves- entre otros, el incumplimiento de la obligación de suprimir los datos referidos a una persona fallecida cuando ello fuera exigible conforme al artículo 3-, siendo aplicable los tipos de sanciones previstas en el artículo 83, apartados 4 a 6 del Reglamento, en función del nivel de gravedad del incumplimiento –pudiendo llegar la multa administrativa a los 20.000.000 de euros o, tratándose de una empresa, a una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, si es esta segunda cifra mayor-.

Por último, el Título X, sobre "Garantía de los derechos digitales", enuncia un elenco de derechos digitales de los ciudadanos y regula la garantía de estos en los artículos 79 a 97. Como principio basilar, se prevé la aplicación plena en Internet de los derechos y libertades consagrados en la Constitución y en los Tratados Internacionales. Los prestadores de servicios de la sociedad de la información y los proveedores de servicios de Internet contribuirán a garantizar su aplicación. Con ello se busca la actualización de la Constitución a la era digital y se eleva a rango constitucional una nueva generación de derechos digitales, con anclaje en el artículo 18 de la Carta Magna.

Entre otros, destaca el derecho a la educación digital, de donde se infiere el principio programático de que el sistema educativo garantizará la plena

inserción del alumnado en la sociedad digital y el aprendizaje de un uso de los medios digitales que sea seguro y respetuoso con la dignidad humana y los valores constitucionales. De ahí la obligación de las Administraciones educativas de incluir la competencia digital en el diseño del bloque de asignaturas de libre configuración, previendo del riesgo derivado de la inadecuada utilización de las TIC, con especial atención a las situaciones de violencia en la red.

Asimismo puede destacarse la regulación del derecho de rectificación en Internet. En particular, se prevé la obligación de los responsables de redes sociales y servicios equivalentes de adoptar protocolos adecuados para posibilitar el ejercicio de este derecho ante los usuarios que difundan contenidos que atenten contra el derecho al honor, la intimidad personal y familiar en Internet y el derecho a comunicar o recibir libremente información veraz. Además, se especifica el deber de los medios de comunicación digitales que atiendan la solicitud de rectificación formulada contra ellos de publicar de forma visible en sus archivos digitales un aviso aclaratorio que ponga de manifiesto que la noticia original no refleja la situación actual del individuo.

Especialmente interesante resulta también el artículo 88, en el que se regula el derecho a la desconexión digital en el ámbito laboral, que se traduce en la facultad de los trabajadores y los empleados públicos de desconectar de la atención a las comunicaciones digitales a fin de garantizar, fuera del tiempo de trabajo legal o convencionalmente establecido, el respeto de su tiempo de descanso, permisos y vacaciones, así como de su intimidad personal y familiar. Ello busca potenciar el derecho a la conciliación de la actividad laboral y la vida personal y familiar, debiendo sujetarse a lo establecido en la negociación colectiva. El ámbito de aplicación de este derecho incluye a los trabajadores que ocupen puestos directivos y los supuestos de realización total o parcial del trabajo a distancia.

A modo de cita ejemplificativa, este Título IX regula asimismo el derecho a la intimidad frente al uso de dispositivos de video-vigilancia y de grabación de sonidos en el lugar de trabajo, el derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral y el derecho al olvido en las búsquedas en Internet y en las redes sociales y servicios equivalentes[13]; la

[13] El artículo 93.1 prevé: "Toda persona tiene derecho a que los motores de búsqueda en Internet eliminen de las listas de resultados que se obtuvieran tras una búsqueda efectuada a partir de su nombre los enlaces publicados que contuvieran información relativa a esa persona cuando fuesen inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieren devenido como tales por el transcurso del tiempo, teniendo en cuenta los fines para los que se recogieron o trataron, el tiempo transcurrido y la naturaleza e interés público de la información.

Del mismo modo deberá procederse cuando las circunstancias personales que en su caso invocase el afectado evidenciasen la prevalencia de sus derechos sobre el mantenimiento de los enlaces por el servicio de búsqueda en Internet.

obligación de los centros educativos y cualesquiera personas físicas o jurídicas que desarrollen actividades en las que participen menores de edad de garantizar el derecho a la protección de datos personales de los menores, en la publicación o difusión de sus datos personales a través de servicios de la sociedad de la información. Especial relevancia tiene asimismo el artículo 96, en donde se regula el derecho al testamento digital[14]. Esta norma destaca que las personas vinculadas al fallecido por razones familiares o de hecho, así como sus herederos podrán dirigirse a los prestadores de servicios de la sociedad de la información al objeto de acceder a dichos contenidos e impartir las instrucciones que estimen oportunas sobre su utilización, destino o supresión. Cuando la persona hubiera establecido unas concretas instrucciones para el ejercicio de su testamento digital, los legitimados habrán de ejercitar el derecho de acceso con vistas a dar cumplimiento de esas instrucciones. Esta opción no será posible cuando la persona fallecida lo hubiese prohibido expresamente o así lo establezca

Este derecho subsistirá aun cuando fuera lícita la conservación de la información publicada en el sitio web al que se dirigiera el enlace y no se procediese por la misma a su borrado previo o simultáneo".

Por su parte, el artículo 94.1 dicta: "Toda persona tiene derecho a que sean suprimidos, a su simple solicitud, los datos personales que hubiese facilitado para su publicación por servicios de redes sociales y servicios de la sociedad de la información equivalentes". Sin embargo, tal y como seguidamente aclara este precepto, con el fin de evitar el riesgo asociado a la censura, el derecho al olvido en las redes sociales no permite a su titular pretender la supresión de cualquier dato personal proporcionado por un tercero persona física.

En lo que al derecho al olvido en Internet se refiere, nos remitimos a MINERO ALEJANDRE, G., "Presente y futuro de la protección de datos personales. Análisis normativo y jurisprudencial desde una perspectiva nacional y europea", en *Anuario Jurídico y Económico Escurialense,* L (2017) 13-58.

[14] Este precepto se aplica siempre que no exista una regla de Derecho civil, foral o especial, en la Comunidad Autónoma en la que hubiera fallecido la persona, tal y como prevé el artículo 96.4. Hasta la fecha, únicamente puede englobarse en este supuesto Cataluña, cuyo parlamento aprobó la Ley 10/2017, de 27 de junio, de las voluntades digitales y de modificación de los libros segundo y cuarto del Código civil de Cataluña. El artículo 6 de la citada Ley 10/2017 añade un artículo, el 411-10 (Voluntades digitales en caso de muerte), al capítulo I del título I del libro cuarto del Código Civil de Cataluña, relativo a las sucesiones. Esta norma prevé que las voluntades digitales se puedan ordenar por medio de los siguientes instrumentos: a) testamento, codicilo o memorias testamentarias; b) si la persona no ha otorgado disposiciones de última voluntad, mediante un documento que debe inscribirse en el Registro de voluntades digitales, cuya creación se prevé asimismo en este precepto. Igualmente interesante es el artículo 1 de la Ley 10/2017, que modifica el art. 222-2 del Código Civil de Cataluña –sobre el poder en previsión de pérdida sobrevenida de capacidad, incluido en su libro segundo, relativo a la persona y a la familia-, para añadir un nuevo número 4. Se permite que en el poder otorgado por la persona, por medio de escritura pública, para el caso de que por causa de una enfermedad o deficiencia persistente de carácter físico o psíquico, no pudiese gobernarse por sí mismas, esa persona establezca la gestión de sus voluntades digitales y el alcance de las mismas. En caso de que no haya una declaración de voluntades digitales, el apoderado podrá comunicar a los prestadores de servicios la pérdida sobrevenida de capacidad de su poderdante y solicitar la cancelación de sus cuentas activas.

una ley, con la excepción del acceso por los herederos a los contenidos que pudiesen formar parte del caudal relicto. Los legitimados podrán decidir asimismo acerca del mantenimiento o eliminación de los perfiles personales de personas fallecidas en redes sociales o servicios equivalentes, a menos que el fallecido hubiera decidido acerca de esta circunstancia, en cuyo caso se estará a sus instrucciones. Esta norma prevé el desarrollo reglamentario de los requisitos y condiciones para acreditar la validez y vigencia de los mandatos e instrucciones.

Finalmente ha de destacarse el elevado número de leyes modificadas por las disposiciones finales de la recién aprobada Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales. Entre otras, la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil; la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa; la Ley Orgánica, 6/1985, de 1 de julio, del Poder Judicial; la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas; la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno; la Ley 14/1986, de 25 de abril, General de Sanidad; la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica; la Ley Orgánica 2/2006, de 3 de mayo, de Educación; la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades; el Texto Refundido de la Ley del Estatuto de los Trabajadores; el Texto Refundido de la Ley del Estatuto Básico del Empleado Público; y, como ya se ha indicado anteriormente, la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General.

II. REFLEXIONES SOBRE LA JURISPRUDENCIA DICTADA POR EL TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA EN 2017 Y 2018 EN LA MATERIA

En este trabajo únicamente se abordan las sentencias dictadas durante el proceso de tramitación de la nueva Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales[15]. Entre ellas debemos destacar la resolución dictada por el Tribunal de Justicia de la Unión Europea con fecha de 20 de diciembre de 2017, asunto Peter Nowak contra Data Protection Commissioner, C-434/16, en relación a la realización, corrección y revisión de exámenes.

El Sr. Nowak suspendió una de las pruebas organizadas por el Colegio de Auditores Públicos de Irlanda, en cuya realización se permitía a los aspirantes la

[15] Para un estudio sobre la jurisprudencia anterior, nos remitimos a MINERO ALEJANDRE, G., "Presente y futuro de la protección de datos personales. Análisis normativo y jurisprudencial desde una perspectiva nacional y europea", en *Anuario Jurídico y Económico Escurialense,* L (2017) 13-58.

consulta de libros y documentos. Presentó una reclamación de impugnación del resultado, que fue desestimada. Tras ello solicitó el acceso a los datos de carácter personal que le concernían sobre dicho examen, que igualmente fue desestimado, al entender el citado Colegio que el documento no contenía datos personales. El Sr. Nowak se dirige al Comisario de Protección de Datos de Irlanda, quien entiende que, como regla general, los exámenes no son objeto de estudio por esta institución y sostiene no haber apreciado una infracción de fondo de la normativa de protección de datos, puesto que el material respecto del que el reclamante pretende ejercitar el derecho de rectificación no constituye un dato de carácter personal.

El Sr. Nowak interpone recurso, que es inadmitido por el Circuit Court irlandés y posteriormente es desestimado tanto por la High Court como por la Court of Appeal. Cuando el asunto llega a la Supreme Court, este tribunal decide suspender el procedimiento y preguntar al TJUE si las respuestas escritas de un aspirante y las anotaciones de su examinador pueden considerarse datos personales conforme a la normativa europea.

En su contestación, el TJUE aplica la Directiva 95/46/CE, y no así el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, que deroga la citada Directiva y está vigente en la actualidad. No procede la aplicación de la norma reglamentaria a los hechos que dieron lugar a la cuestión prejudicial puesto que tuvieron lugar antes de su entrada en vigor. Ambas normas regulan, en lo que aquí interesa, el concepto de dato personal, los derechos de acceso y rectificación, sus limitaciones y el derecho de oposición.

En relación a esta norma, el TJUE llama la atención sobre la amplitud del ámbito de aplicación de la Directiva y el carácter heterogéneo de los datos de carácter personal protegidos en ella (en particular, en la definición de dato personal prevista en el artículo 2.a, como "toda información sobre una persona física identificada o identificable"). En palabras del TJUE, el objetivo del legislador europeo es atribuir al concepto de datos personal "un significado muy amplio, que no se ciñe a los datos confidenciales o relacionados con la intimidad, sino que puede abarcar todo género de información, tanto objetiva como subjetiva, en forma de opiniones o apreciaciones, siempre que sean «sobre» la persona en cuestión". Esta afirmación no resulta novedosa, pues ya se contenía en jurisprudencia europea previa, en la que se había calificado como dato personal la información sobre las retribuciones de cargos públicos, el dato de la dirección del domicilio particular de una persona o información sobre la profesión y aficiones de una persona, ligada a su nombre. En la sentencia

de 2018 el TJUE va un paso más allá y sostiene que la exigencia de que la información trate "sobre" la persona en cuestión se cumple cuando, debido a su contenido, a su finalidad o a sus efectos, dicha información está relacionada con una persona concreta.

En particular, sostiene el TJUE que esta condición se cumple en el caso concreto, toda vez que el sujeto que realiza el examen puede ser identificado con su número de identificación expresado en el escrito del examen o en su cubierta delantera. Por tanto, la entidad que organiza el examen dispone de los datos necesarios que permiten identificar sin dificultades o dudas a la persona.

Carece de relevancia en este análisis el hecho de que el examinador pueda o no identificar al candidato en el momento de la corrección, y ello porque la norma europea no exige que toda la información que permita identificar al interesado tenga que encontrarse en poder de una sola persona.

Tranquiliza leer que el TJUE sostenga que las preguntas de examen per se no se subsumen dentro del concepto de dato personal. Sin embargo, las respuestas escritas proporcionadas por un aspirante en un examen sí son datos relacionados con su persona, dado que revelan informaciones sobre ésta relacionadas con el nivel de conocimientos y el grado de competencia en un área determinada, el proceso de reflexión, el discernimiento y la capacidad de análisis del propio aspirante, su capacidad profesional individual y completamente personal y su aptitud para ejercer el oficio de que se trate, así como, cuando el examen esté escrito a mano, información caligráfica de la persona que lo realiza, pudiendo dichos datos tener efectos en los intereses del aspirante relacionados con el acceso a la profesión en cuestión.

La misma conclusión se extiende a las anotaciones del examinador sobre las respuestas del aspirante. Se entiende que dichas anotaciones son datos que se refieren al citado aspirante, dado que dichas anotaciones expresan la valoración del examinador sobre los conocimientos y competencias del aspirante y documentan la evaluación de los resultados. Además, esta afirmación no puede quedar desvirtuada como tal por el hecho de que las citadas anotaciones también sean datos personales que conciernen al propio examinador, y no sólo al aspirante.

El hecho de que la calificación de las respuestas de un examen y los comentarios de evaluación del docente merezcan la calificación de datos personales del aspirante –y, por otro lado, de datos personales del propio docente o examinador- no permiten al sujeto examinado pretender un ejercicio de los derechos de acceso y rectificación que busque la alteración de las citadas respuestas. Por tanto, el TJUE impide que la vis atractiva de la normativa de

protección de datos personales se traduzca por el afectado por el tratamiento de sus datos personales en la posibilidad de rectificar a posteriori las respuestas incorrectas. Si bien los errores del aspirante no son inexactitudes sobre la que aplicar el derecho de rectificación, el TJUE sí cita algunos ejemplos de lo que serán consideradas inexactitudes a estos efectos, que habrán de ser valorados por el tribunal nacional. A saber: "cuando por error las hojas de los exámenes se hayan entremezclado de tal modo que las respuestas de otro aspirante se hayan atribuido al aspirante afectado, o cuando se haya perdido una parte de los folios que contienen las respuestas de ese aspirante, dando lugar a que esas respuestas queden incompletas, o incluso cuando las eventuales anotaciones del examinador no documenten correctamente la valoración que éste ha dado a las respuestas del aspirante de que se trate".

Partiendo de estas conclusiones preliminares, el TJUE infiere de la máxima del interés legítimo de quien participa como aspirante en un examen la facultad de éste a oponerse a que sus respuestas y las anotaciones de su examinador sean comunicadas a terceros sin su consentimiento. Consecuentemente, de ello se deduce la obligación de la entidad organizadora del examen de garantizar que esas respuestas y anotaciones sean almacenadas de tal forma que se impida a terceros acceder a ellas de manera ilícita. Pero a ese examen se suma la necesidad de analizar si resultan de aplicación o no algunos de los límites al derecho a la protección de datos personales previstos en la Directiva 95/46/CE y en el Reglamento (UE) 2016/679, entre otros los referidos a la necesidad de salvaguardar los derechos y libertades de otras personas, así como objetivos importantes de interés público general de la UE o del Estado miembro.

El TJUE entiende el derecho de acceso por parte del aspirante a sus respuestas y a las anotaciones de su examinador, como paso previo para valorar la exactitud o no de esos datos personales, y justifica su existencia en la necesidad de garantizar la protección del derecho a la intimidad del aspirante en lo que respecta al tratamiento de sus datos. Valoración que el TJUE lleva a cabo con independencia de si el aspirante tiene o no ese derecho de acceso en virtud de la normativa nacional aplicable al procedimiento de examen, toda vez que "la protección del derecho fundamental al respeto de la intimidad implica, en especial, que toda persona física pueda cerciorarse de que los datos personales que le conciernen son exactos y se utilizan de manera lícita". Por tanto, se trataría de una suerte de eficacia directa horizontal de la norma europea entre relaciones de particulares o particular-Estado -lo cual no deja de ser sorprendente-, y cuya razón de ser es un derecho personalísimo, el derecho a la intimidad.

En segundo lugar, el TJUE reconoce el derecho del aspirante a solicitar al responsable del tratamiento de datos que, transcurrido un determinado período de

tiempo, se destruyan sus respuestas al examen y las correspondientes anotaciones del examinador. La justificación se encuentra en el hecho de que el artículo 6 de la Directiva 95/46/CE únicamente permite que los datos personales sean conservados durante un período no superior al necesario para la consecución de los fines para los que fueron recogidos o tratados. De manera ciertamente sorpresiva -por extralimitada de las funciones interpretativas del TJUE en el análisis de una cuestión prejudicial-, este tribunal concluye que en este caso dicho período necesario ya había transcurrido, pues el examen estaba definitivamente concluido y no podía ser objeto de recurso, de tal forma que las respuestas y anotaciones habían perdido su valor probatorio. Por tanto, habría de permitirse al aspirante solicitar al responsable del tratamiento la destrucción de sus datos personales.

La sentencia del Tribunal de Justicia de la Unión Europea de 10 de julio de 2018, asunto Tietosuojavaltuutettu[16], C–25/17, igualmente debe destacarse. El supuesto de hecho era el siguiente. En septiembre de 2013, la Comisión de protección de datos finlandesa adoptó, a instancias del Supervisor de protección de datos finés, una resolución mediante la cual se prohibía a la comunidad de los Testigos de Jehová recoger o tratar datos personales en relación con la actividad de predicación puerta a puerta llevada a cabo por sus miembros sin que concurrieran los requisitos legales para el tratamiento de tales datos regulados en la ley finlandesa de protección de datos. Durante las actividades de predicación, los miembros de esta comunidad realizan anotaciones sobre las visitas efectuadas a personas que ellos mismos no conocían previamente, como son el nombre y la dirección de las personas contactadas, así como en información sobre sus convicciones religiosas y su situación familiar. Estos datos se recogen a modo de recordatorio y con el fin de poder ser recuperados para una eventual visita posterior, sin que los interesados hayan dado su consentimiento ni hayan sido informados. Las citadas visitas de los predicadores se realizan siguiendo el mapa de distribución de zonas coordinado por la comunidad. Además, las congregaciones de la comunidad llevan un registro de las personas que han manifestado el deseo de no recibir más visitas de los miembros predicadores. De la resolución administrativa finlandesa nace la obligación de la citada comunidad religiosa de dejar de recoger, dentro de un plazo de seis meses, datos personales para los fines de la comunidad sin cumplir los citados requisitos. La comunidad de los Testigos de Jehová recurrió dicha resolución ante el Tribunal de lo Contencioso- Administrativo de Helsinki, que anuló la resolución en cuestión, al entender que la actividad no supuso un tratamiento ilícito de datos personales. Por su parte, el Supervisor de protección de datos recurrió dicha sentencia. El tribunal finés remitente se inclina a considerar

[16] Supervisor de protección de datos, Finlandia.

que la actividad de predicación puerta a puerta llevada a cabo por los miembros de una comunidad religiosa, como la comunidad de los Testigos de Jehová, no está comprendida entre las actividades excluidas del ámbito de aplicación de la Directiva 95/46 en virtud de su artículo 3.2, pero, al albergar dudas sobre el carácter doméstico o no de dicho tratamiento y sobre la aplicación o no a la comunidad religiosa del concepto de responsable del tratamiento, plantea cuestión prejudicial.

En la sentencia de 10 de julio de 2018 el TJUE sostiene que la Directiva 95/46/CE, en relación con el artículo 10.1, de la Carta de los Derechos Fundamentales de la Unión Europea, debe interpretarse en el sentido de que la recogida de datos personales llevada a cabo por miembros de una comunidad religiosa en relación con una actividad de predicación puerta a puerta y el tratamiento posterior de esos datos no constituyen ninguno de los tratamientos que el artículo 3.2 de la citada Directiva excluye de su ámbito de aplicación, esto es, no se trata de un uso de datos personales efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas, ni es un tratamiento que tenga por objeto la seguridad pública, la defensa, la seguridad del Estado y las actividades del Estado en materia penal. En efecto, dicha actividad está dirigida hacia el exterior de la esfera privada de los miembros predicadores, y esta comunidad no se trata de una organización estatal que pueda englobarse en los fines públicos citados.

Además, el TJUE califica de "fichero", en el sentido del artículo 2, letra c), de la Directiva 95/46/CE, el conjunto de datos personales recogidos en relación con una actividad de predicación puerta a puerta, consistentes en nombres, direcciones y otra información relativa a las personas contactadas, siempre que los datos estén estructurados según criterios determinados que permitan, en la práctica, recuperarlos fácilmente para su utilización posterior, para preparar visitas posteriores y para gestionar los registros de personas que no desean volver a ser contactadas. Explica el TJUE que para que dicho conjunto de datos esté comprendido en ese concepto no es preciso que incluya fichas, catálogos específicos u otros sistemas de búsqueda. Por todo ello, el Alto Tribunal europeo sostiene que la citada comunidad religiosa es responsable, junto con sus miembros predicadores, de los tratamientos de datos personales efectuados por estos últimos en relación con una actividad de predicación puerta a puerta organizada, coordinada y fomentada por dicha comunidad, pues la comunidad determina, junto con los predicadores, la finalidad y los medios de los tratamientos de datos personales de las personas afectadas, sin que haga falta demostrar que la comunidad ha impartido a sus miembros instrucciones por escrito o consignas en relación con esos tratamientos.

Una última sentencia europea cuyo análisis resulta interesante en este estudio es la dictada por el Tribunal de Justicia de la Unión Europea el 2 de octubre de 2018, asunto Ministerio Fiscal, C-207/16, en la que se resuelve una cuestión prejudicial planteada por la Audiencia Provincial de Tarragona. En ella, el TJUE interpreta el artículo 15.1 de la Directiva 2002/58/CE (Directiva sobre la privacidad y las comunicaciones electrónicas), a la luz de los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea, y concluye que el acceso de las autoridades públicas a los datos que permiten identificar a los titulares de las tarjetas SIM activadas con un teléfono móvil sustraído, como los nombres, los apellidos y, en su caso, las direcciones de dichos titulares, constituye una injerencia en los derechos fundamentales de estos, consagrados en los citados artículos de la Carta de los Derechos Fundamentales, que no presenta una gravedad tal que exija que dicho acceso deba limitarse, en el ámbito de la prevención, investigación, descubrimiento y persecución de delitos, a la lucha contra la delincuencia grave.

El supuesto de hecho que dio origen al litigio es el siguiente. El Sr. Hernández Sierra presentó una denuncia ante la Policía por un robo con violencia, durante el cual resultó herido y le sustrajeron la cartera y el teléfono móvil. La Policía Judicial presentó un oficio ante el juez instructor solicitando que se ordenase a diversos proveedores de servicios de comunicaciones electrónicas la transmisión de los números de teléfono activados, desde la fecha del robo, con el código relativo a la identidad internacional del equipo móvil (código IMEI), así como los datos personales o de filiación de los titulares o usuarios de los números de teléfono correspondientes a las tarjetas SIM activadas con dicho código, como su nombre, apellidos y, en su caso, dirección. El juez instructor denegó la diligencia solicitada, por entender que la ley española aplicable al caso limitaba la cesión de los datos conservados por las operadoras de telefonía a los delitos graves. Con arreglo al Código Penal español, los delitos graves son los sancionados con una pena de prisión superior a cinco años, mientras que los hechos presuntos no parecían ser constitutivos de delito grave. El Ministerio Fiscal interpuso recurso de apelación contra dicho auto ante el tribunal remitente, defendiendo la aplicación de la sentencia del Tribunal Supremo, de 26 de julio de 2010, relativa a un caso similar, en la que se acordó la cesión de los datos. La Audiencia Provincial plantea cuestión prejudicial y expone la reciente modificación de la Ley de Enjuiciamiento Criminal a la hora de determinar el nivel de gravedad de un delito.

En su análisis, el TJUE parte de la siguiente regla: conforme al principio de proporcionalidad, en el ámbito de la prevención, investigación, descubrimiento y persecución de delitos una injerencia grave en la esfera de la protección de datos personales sólo se puede justificar en base al objetivo de luchar contra

la delincuencia que a su vez esté también calificada de "grave". En cambio, cuando la injerencia que implica dicho acceso para la protección de datos personales no es grave, puede estar justificada por el objetivo de prevenir, investigar, descubrir y perseguir "delitos" en general.

Pues bien, en relación al asunto litigioso en cuestión, entiende el Alto Tribunal europeo que los datos a los que se refiere la solicitud de acceso controvertida solo permiten vincular, durante un período determinado, la tarjeta o tarjetas SIM activadas con el teléfono móvil sustraído y los datos personales o de filiación de los titulares de estas tarjetas SIM. Sin embargo, sin un cotejo con los datos relativos a las comunicaciones realizadas con esas tarjetas SIM y de localización, estos datos no permiten conocer la fecha, la hora, la duración o los destinatarios de las comunicaciones efectuadas con las tarjetas SIM en cuestión, ni los lugares en que estas comunicaciones tuvieron lugar. Por tanto, dichos datos no permiten extraer conclusiones precisas sobre la vida privada de las personas cuyos datos se ven afectados, y la injerencia en los derechos fundamentales de los individuos cuyos datos se ven afectados no puede calificarse de "grave". Por todo ello, la injerencia que supone el acceso a dichos datos puede estar justificada por el objetivo de prevenir, investigar, descubrir y perseguir "delitos" en general, al que se refiere el artículo 15. 1 de la Directiva 2002/58, sin que sea necesario que dichos delitos estén calificados como "graves".

III. CONCLUSIONES

A día de hoy, la amplitud del ámbito de aplicación de la normativa europea de protección de datos es innegable. Su repercusión se extiende a prácticamente todas las facetas diarias de las personas. Ello se debe a la extensiva regulación de los ámbitos afectados por la normativa de protección de datos personales, así como a la interpretación realizada por los tribunales, abarcando, entre otros campos, el comportamiento durante las pruebas de evaluación académica de docentes, estudiantes, opositores y el tratamiento de los datos almacenados en teléfonos móviles para la investigación de delitos.

Esta tendencia se refuerza con la lectura de la nueva Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales, que reconoce sub-categorías del derecho fundamental a la protección de datos hasta ahora insólitas. Entre ellas, destaca el derecho a la desconexión digital en el ámbito laboral y el derecho al testamento digital, así como la obligación de los responsables de redes sociales de adoptar protocolos para posibilitar el ejercicio del derecho de rectificación en Internet cuando el contenido publicado atente contra los derechos de la personalidad.

A ello se une el reconocimiento de la protección de los datos personales de personas fallecidas, lo que se traduce en la posibilidad de solicitar el acceso a los datos personales del fallecido y, en su caso, exigir su rectificación o supresión, pudiendo ejercitar estas acciones los familiares y herederos del fallecido, así como las personas expresamente designadas para ello por el fallecido. La implantación de esta tutela post mortem de los datos personales qué duda cabe que generará importantes problemas cuando quien ejercite las correspondientes acciones no siga, a juicio del resto de legitimados, las instrucciones recibidas de la persona fallecida. Está por ver cuál sea la implementación de la regulación que se apruebe acerca del registro de instrucciones *post mortem*, cuyo desarrollo reglamentario se prevé en la nueva Ley Orgánica.

Esta vis atractiva del derecho a la protección de datos personales y la tendencia jurisprudencial en la que ha derivado contrasta con la modificación por esta nueva Ley Orgánica de la Ley Orgánica de Régimen Electoral General para permitir la recopilación y uso por los partidos políticos de los datos personales relativos a las opiniones políticas de los ciudadanos. Las consecuencias de la implementación de esta norma serán objeto de importantes debates jurídicos en un futuro próximo.

IV. BIBLIOGRAFÍA

- ESPÍN, E., "Los derechos de la esfera personal", en *Derecho Constitucional,* LÓPEZ GUERRA y otros (Dir.), Tirant Lo Blanch, Valencia 1994.

- HERNÁNDEZ LÓPEZ, J. M., *El derecho a la protección de datos personales en la doctrina del Tribunal Constitucional*, Aranzadi, Cizur Menor, Navarra 2013.

- LUCAS MURILLO DE LA CUEVA, P., "El derecho a la autodeterminación informativa y las garantías de su efectividad", en LUCAS MURILLO DE LA CUEVA, P., y PIÑAR MAÑAS, J. L. (Dir.), *El derecho a la autodeterminación informativa*, Fundación Coloquio Jurídico Europeo, 2009.

- LUCAS MURILLO DE LA CUEVA, P., "Título I. Disposiciones Generales", en *Comentarios a la Ley orgánica de Protección de Datos de Carácter Personal,* TRONCOSO REIGADA, A. (Dir.), Civitas, Madrid 2010.

- LUCAS MURILLO DE LA CUEVA, P., "La Constitución y el derecho a la autodeterminación informativa", en *Cuadernos de Derecho Público,* núm. 19-20 (2003) 27 y ss.

- MINERO ALEJANDRE, G., *La protección post mortem de los derechos al honor, intimidad y propia imagen y la tutela frente al uso de datos de carácter personal tras el fallecimiento,* Aranzadi, Navarra, 2018.

- MINERO ALEJANDRE, G., "Presente y futuro de la protección de datos personales. Análisis normativo y jurisprudencial desde una perspectiva nacional y europea", en *Anuario Jurídico y Económico Escurialense,* L (2017) 13-58.

- PAZOS CASTRO, R., "El mal llamado derecho al olvido en la era de Internet", en *Boletín del Ministerio de Justicia,* núm. 2183 (2015).

- PEGUERA POCH, M., "Publicidad online basada en comportamiento y protección de la privacidad", en RALLO LOMBARTE, A., y MARTÍNEZ MARTÍNEZ, R. (coord.), *Derecho y redes sociales*, Aranzadi (Navarra), 2010.

- TRONCOSO REIGADA, A. *La protección de datos personales. En busca del equilibrio,* Tirant lo Blanch, Valencia 2010.