Principios del tratamiento y derechos de los interesados en la nueva normativa de protección de datos personales. Consideraciones de carácter general y algunos apuntes para el ámbito universitario

Juan Pablo Aparicio Vaquero
Profesor Titular Derecho Civil
Universidad de Salamanca

1. Introducción al nuevo marco normativo

Cabe remontar los orígenes de la preocupación por la protección de los datos personales en Europa a finales de los años sesenta del siglo pasado: en 1968, el Consejo de Europa aprobó (*Resolución 509*) la creación de un Comité de Expertos para estudiar cómo proteger los derechos y libertades frente a los nuevos avances tecnológicos. Entre otros, el trabajo de estos expertos fue la base de sendas Resoluciones del Comité de Ministros del Consejo de Europa de septiembre de 1973 y 1974 (*Resoluciones 22* y *29*, respectivamente), que ya anticipaban las líneas generales de protección de las personas frente a las bases de datos electrónicas. Aun no siendo vinculantes, contenían algunos de los principios sobre protección de datos personales que han llegado hasta hoy, como los derechos de acceso, cancelación, calidad y seguridad de los datos, etc. Permitieron, además, alcanzar el primer texto vinculante con alcance europeo, el *Convenio 108 del Consejo de Europa* sobre protección de personas respecto del tratamiento automatizado de datos. En el marco de dicho Convenio, la libre circulación de datos de carácter personal sólo podría hacerse respetando los derechos y libertades fundamentales de las personas, para lo que se recogían una serie de principios que debían incorporar los Estados miembros a sus legislaciones internas: calidad de los datos, distinción por categorías con protección reforzada (ideológicos, de salud...) y seguridad de los mismos. España lo ratificó por Instrumento de 31 de enero de 1984, pero ya antes el propio constituyente de 1978 había sido receptivo a la necesidad de regular el uso de las nuevas tecnologías para no afectar a los derechos de las personas (art. 18.4 CE: "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").

La Unión Europea propuso una normativa de mínimos comunes a todos sus Estados miembros con la *Directiva 95/46/CE*, traspuesta en España a través de la LOPD de 1999, la cual, a su vez, derogó a la anterior LORTAD de 1992. Esta última, por su novedad, había sido una norma de gran éxito y repercusión, hasta el punto de que todavía hoy pueden encontrarse avisos en documentos y webs con referencias a ella, totalmente anticuados y no válidos.

El marco descrito ha estado vigente hasta la plena eficacia (el 25 de mayo de 2018) del *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* (Reglamento General de Protección de Datos, RGPD) y la nueva *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales* (LOPDyGDD), que entró en vigor el 7 de diciembre de 2018.

Frente a la normativa anterior, fragmentaria (territorialmente) y en algunos puntos ya obsoleta, el Reglamento europeo (instrumento normativo directamente aplicable en todos los Estados sin necesidad de transposición interna) supone una disposición actual y única, con pretensiones de establecer un régimen completo (99 artículos, precedidos por hasta 173 Considerandos) para toda la Unión, y aplicable a cualquiera que trate datos en el territorio de la misma. El Reglamento es de aplicación también a las empresas o responsables del tratamiento radicadas fuera de la Unión que ofrezcan servicios o bienes a interesados que residan en la Unión o controlen su comportamiento en territorio de la misma, consagrando así las interpretaciones de la Directiva 95/46 (art. 4, en consonancia con su Considerando 20) que venía haciendo (por ejemplo, en sus Dictámenes 1/2008, 5/2009, 8/2010 o 2/2013; también, en el Documento de Trabajo WP56, de 2002) el "Grupo de Trabajo del artículo 29" (órgano consultivo independiente creado por el art. 29 Directiva 95/46, y cuya labor y documentos resultan de gran utilidad para la interpretación de la normativa y sus soluciones, recomendaciones y propuestas han servido de base, en muchos casos, para el desarrollo del RGPD), aunque bajo una perspectiva distinta: supone un cambio del paradigma de protección. Efectivamente, bajo la normativa anterior, lo determinante era la ubicación de los medios o dispositivos que permitían el tratamiento, o que las empresas responsables tuvieran algún tipo de establecimiento en territorio de la Unión, mientras que ahora se pone el foco en las personas en cuanto destinatarias de los servicios o cuyo comportamiento es objeto de control, lo cual es plasmación de la necesa-

ria "orientación hacia las personas" que decía el referido Dictamen 8/2010 (Troncoso Reigada, 2013, p. 66). Evidentemente, dicho control se llevará a cabo a través de la recogida y tratamiento de datos a partir de sus dispositivos (teléfonos móviles, ordenadores, etc.), que son los que estarán físicamente en territorio de la Unión, pero el cambio de enfoque es indicativo de la preocupación del legislador.

La nueva LOPDyGDD, por su parte, pretende complementar al Reglamento europeo, aunque en gran parte es mera reproducción o reenvío al mismo; sin embargo, como apunta su nueva denominación, contiene una novedosa parte entre programática y positiva sobre derechos de las personas en la Sociedad de la Información (arts. 79-97, que recoge tanto derechos como mandatos al legislador) y hace uso, allá donde estaba permitido, de las facultades que da al legislador estatal el europeo para tomar ciertas decisiones (p. ej., rebajar la edad para la disposición de datos personales hasta los 14 años, art. 7), junto con el desarrollo de alguna otra cuestión que sí resulta novedosa al no haber sido tratada por el RGPD (así, entre otros, el tratamiento de los datos personales, archivos y contenidos de personas fallecidas, arts. 3 y 96 LOPDyGDD, o lo relativo a los sistemas de información de denuncias internas, art. 24; vid. más adelante).

Al tiempo de escribir estas líneas, no hay bibliografía de tipo monográfico exclusivamente sobre la nueva LOPDyGDD. Sí sobre el Reglamento, pudiendo encontrarnos obras a la manera de prontuarios o manuales prácticos junto con otras destinadas a académicos, profesionales del Derecho o expertos que requieran de un mayor análisis de la normativa, sus fundamentos e interpretaciones judiciales. Entre las primeras, pueden consultarse, entre otras muchas, las de López Álvarez (2016) y Aragonés Salvat (2016). Entre las segundas, la colectiva dirigida por Piñar Mañas (2016), o la de López Calvo (2017); o, contemplando también la reciente LOPDYGDD, el trabajo colectivo coordinado por López Calvo (2019).

Por su parte, la Agencia Española de Protección de Datos (AEPD) dispone en su web (https://www.aepd.es) de numerosas guías sobre los más diversos temas, tanto para ciudadanos (interesados, titulares de derechos) como para los responsables. En dicha página también pueden encontrarse sus resoluciones e informes, imprescindibles en la interpretación de la normativa de protección de datos.

2. En torno al valor de la protección de los datos personales

El derecho a la protección de los datos personales se erige hoy en día no solo como una garantía o instrumento al servicio de otros derechos como el

honor, la imagen personal o la intimidad, sino que tiene una auténtica *entidad propia* como derecho fundamental (STC 254/1993, de 20 de julio) y de la personalidad, con un contenido y principios propios, y con mecanismos de protección *ad hoc*, tales como la existencia de una autoridad de control independiente.

Así se contiene, p. ej., en la *Carta de los Derechos Fundamentales de la UE*, de 2000 (art. 8), y así lo considera nuestro Tribunal Constitucional: consiste, dice, "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. Estos poderes (...) se concretan en la facultad de *consentir la recogida,* la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir (...) requiere como complementos indispensables (...) la facultad de *saber* en todo momento *quién dispone* de esos datos personales y *a qué uso los está sometiendo*, y (...), el poder *oponerse* a esa posesión y usos" (STC 292/2000, de 30 de noviembre).

Este contenido esencial del derecho a la protección de datos hace que se hable de él también como "libertad informática" o "autodeterminación informativa", y es lo que, aun cuando coincide con la intimidad en cuanto ambos protegen la vida privada del individuo (y, en este sentido, son plenamente compatibles), lo diferencia de ella: junto al poder de resguardar la vida privada de la publicidad no deseada (intimidad) la persona puede controlar, además, su información o datos personales, incluso aunque éstos sean públicos o no íntimos (STC 11/1998, de 13 de enero).

El gran reto social del momento es la interiorización por parte de todos (ciudadanos, poderes y funcionarios públicos, responsables del tratamiento, prestadores de servicios de la Sociedad de la Información...), de los derechos y deberes que contiene la normativa de protección de datos como algo propio: más allá de la mera imposición por la ley, la asunción de una auténtica *cultura de protección de datos*, en la que los sujetos sean conscientes del valor de sus datos personales (tanto desde la perspectiva de control de su propia intimidad personal y familiar como, en su caso, desde la económica, si desearan explotarlos) y las empresas y administraciones públicas realicen tratamientos lícitos, leales y transparentes como parte de su propia *responsabilidad social*. En este punto, la educación digital de la ciudadanía y la formación de los trabajadores y empleados públicos son los pilares básicos de dicha cultura de protección de datos personales.

3. Algunos conceptos básicos

El art. 4 RGPD define los conceptos propios de esta materia, tales como "dato de carácter personal", "fichero", "tratamiento de datos", "responsable del tratamiento", "encargado del tratamiento", "interesado", "seudonimización", "encargado del tratamiento", "consentimiento del interesado", "violación de la seguridad"... Destacamos brevemente algunos de ellos para una correcta aproximación al tema.

3.1. Dato de carácter personal (dato personal)

Un *"dato personal"* es cualquier *información* concerniente a las *personas físicas* identificadas o que permita su identificación (identificables) de manera directa o indirecta (mediante un número, una característica propia, etc.). Esta persona concernida es el afectado o *"interesado"* (terminología del nuevo RGPD), el titular (terminología clásica española) de los datos que son objeto de tratamiento. De forma intuitiva y directa, son datos de carácter personal el nombre y apellidos de una persona, su número de documento de identificación, su dirección postal y número de teléfono, una fotografía en la que aparezca, una grabación de su voz, un informe sobre su estado de salud...

Además, y por lo que ahora nos interesa, se han considerado "datos de carácter personal", p. ej., las respuestas escritas de un aspirante en un examen profesional, así como las eventuales anotaciones del examinador (STJUE de 20 de diciembre de 2017, asunto C-434/16, *caso Nowak*): las respuestas, explican los párrafos 37 y siguientes de la sentencia, revelan el conocimiento, competencias, proceso de reflexión, discernimiento y capacidad de análisis del examinando, junto con información sobre su escritura (si está hecho a mano); permiten también valorar su capacidad y aptitud para el oficio y la utilización de estos datos afecta directamente a los intereses de aquél, pues condiciona sus oportunidades de acceso a una profesión o empleo al que aspira. Las anotaciones del profesor, además de ser datos personales de éste (también revelan, cabe deducir aunque no lo diga la sentencia, sus procesos lógicos de pensamiento, la forma en que imparte una materia, su propia escritura...) afectan igualmente al aspirante en cuanto revelan sus conocimientos y competencias.

Esta consideración de los exámenes tiene indudable repercusión en el ámbito universitario, dado que sobre las pruebas de evaluación (los exámenes físicos en papel) se abre la posibilidad para el estudiante de solicitar los derechos de acceso, cancelación y rectificación (aunque, por lo que respecta a este último, lógicamente no puede entenderse que le permita alterar

las respuestas incorrectas dadas para mejorar su calificación; párrafo 52 STUJE caso *Nowak*). Precisamente, en el caso, el Sr. Nowak trató de ejercer su derecho de acceso para poder obtener su examen escrito ante la desestimación de su reclamación por el suspenso en una prueba para el cuerpo de auditores públicos de Irlanda, pretensión que fue rechazada por la Autoridad irlandesa al considerar que el examen no contenía datos personales (de manera que no se le facilitó ni original ni copia del mismo, lo que hubiera sido de utilidad para la preparación de su recurso). El Tribunal Europeo, como se ha dicho, dio la razón al demandante.

En nuestro ordenamiento, el acceso a las pruebas escritas por la vía de la protección de datos sirve de complemento a lo establecido en la normativa administrativa (art. 53.1.*a* LPAC) sobre derecho del administrado a obtener en cualquier momento copia de toda la documentación de un procedimiento administrativo que le afecte (p. ej., acceder a su examen para poder reclamar fundadamente la calificación).

3.2. En torno al tratamiento de datos de carácter personal: tratamiento, fichero, responsable y encargado

Los datos personales pueden ser recabados, grabados y conservados (almacenados), modificados o borrados (pudiendo también ser bloqueado el acceso a los mismos) por terceros. Todas estas operaciones y procedimientos técnicos (todas en su conjunto o cualquiera de ellas de forma individual) son denominadas *"tratamiento de datos"*. Éste suele hacerse sobre (o iniciarse, o dar como resultado) un *"fichero de datos"*, un conjunto organizado de datos de carácter personal, cualquiera que fuera la modalidad o forma de su creación, almacenamiento, organización y acceso. La persona física o jurídica que tiene (de forma individual o conjuntamente con otra) la facultad de decisión sobre tal fichero (su creación, finalidad, contenido, medios, uso...) es el *"responsable del fichero"* o *"responsable del tratamiento"* (expresiones ahora sinónimas). Éste puede ser, sin mayores inconvenientes, una persona privada o pública, como una Universidad, que hagan el tratamiento por sí mismos o mediante un *"encargado del tratamiento"*, que lo hace "por cuenta" de aquél (el responsable decide que el tratamiento se haga y su finalidad, realizándolo materialmente dicho encargado, en virtud del contrato que une a ambos, con las garantías y contenidos que establecen las normas). En el ámbito universitario, p. ej., la externalización del servicio de correo electrónico de los empleados y estudiantes a una empresa privada convierte a ésta en encargada del tratamiento por cuenta de la Universidad responsable.

3.3. Borrado, seudonimización y anonimización

Aunque la cancelación suele referirse a la supresión o *borrado* del dato, también caben otras alternativas, como la *seudonimización* (*palabro* que hace referencia al proceso por cuya virtud el dato en sí mismo ya no se refiere a una persona en concreto, pero aun así resulta posible identificar a su titular utilizando información adicional, por lo que todavía queda sujeto a ciertas garantías), o la *anonimización* completa que, en cuanto impide definitivamente la relación del dato con *una* persona en concreto, lo despoja de su carácter personal y, por lo tanto, resulta ya de libre utilización (a efectos estadísticos, p. ej.: aun suprimida una determinada información de un estudiante, puede quedar en el sistema que hubo "una" persona en tal o cual situación).

4. Principios del tratamiento de datos

Los principios del tratamiento de datos son las ideas o razones que fundamentan e informan no sólo la regulación contenida en la norma, sino todo tratamiento de datos que pueda lícitamente hacerse por parte de los responsables. Los recoge el Reglamento en los arts. 5 a 11 y, en las acertadas palabras de Puyol Montero, "van más allá de los meros fundamentos, puesto que tienen naturaleza normativa y van a informar e integrar la interpretación de toda esta normativa (...) supliendo directamente las múltiples lagunas legales que se puedan producir en la propia regulación, a consecuencia de la imparable evolución de la tecnología" (Puyol Montero, en Piñar Mañas, dir, 2016, p. 135). Se formulan, en ocasiones, como conceptos jurídicos indeterminados (lealtad, transparencia, interés del responsable...), y tienen su plasmación concreta en los derechos del interesado y en las correspondientes obligaciones del responsable.

4.1. El consentimiento como principal legitimador del tratamiento, y algunas excepciones de interés para el ámbito universitario

El principio esencial en torno al cual gira toda la normativa de protección de datos de carácter personal es el de la *autodeterminación de su titular*: el *consentimiento* es el criterio legitimador (base jurídica) principal de cualquier tratamiento, a salvo las excepciones legalmente contempladas. Consiste, básicamente, en una *manifestación de voluntad libre*, *inequívoca*, *específica* e *informada*, mediante la cual el interesado permite el tratamiento.

El consentimiento puede ser prestado incluso por menores de edad mayores de 14 años por sí solos, salvo que la ley exija también la concurrencia de los titulares de la patria potestad o tutela (art. 7.1 LOPDyGDD, por explícito ejercicio por el legislador español de la delegación contenida en el art.

13 RGPD). Esta habilitación de los menores no afecta a su capacidad para contratar, la cual se sigue rigiendo por las normas civiles; en la práctica, ello supone que, por ejemplo, un menor no emancipado no pueda realizar un determinado contrato de cierta relevancia (como matricularse en la Universidad) sin el consentimiento de sus padres o tutores pero, dándose éste, será dicho menor quien pueda disponer de sus datos en el marco de tal contrato.

A partir del RGPD, el consentimiento ha de ser *siempre*, para cualquier tratamiento en que se requiera (y cualquier tipo de dato personal), *expreso*, resultado de una conducta positiva, "afirmativa", no cabiendo el consentimiento tácito (p. ej., no es práctica admisible ya dar al interesado "premarcada" la casilla del consentimiento, ha de marcarla él mismo: art. 4.11 RGPD). Como regla general, la forma que debe adoptar el consentimiento depende de los datos que deban ser objeto de tratamiento, llegando incluso a estar prohibido, como principio general, el tratamiento de determinadas categorías de datos personales (datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física), *salvo* que concurra alguna de las excepciones previstas (art. 9.2 RGPD): entre otras, el consentimiento *explícito* del interesado (entiéndase, por lo tanto, "expreso" y *ad hoc*, no el genérico para tratar sin más datos personales), la disposición legal, que sea necesario el tratamiento para la protección de intereses vitales del titular, o que tales datos hayan sido hechos manifiestamente públicos por éste.

Existen, no obstante, casos *excepcionales* en que cabe el tratamiento sin el consentimiento previo del interesado (art. 6.1 RGPD), pues concurren otras causas legitimadoras que ampara el lícito tratamiento de datos personales; entre otras, se encuentran el *cumplimiento del contrato* que une a las partes (p. ej., el de enseñanza o prestación de servicios de educación, de manera que si el titular, estudiante, no autoriza el tratamiento, el contrato devendría de imposible cumplimiento: no podría identificársele, tramitar los distintos procedimientos de gestión, asignarle cursos, asignaturas y grupos, ser calificado, cobrar la matrícula...), la existencia de un *interés legítimo del responsable* (concepto éste sumamente amplio y que ha sido objeto de crítica pues permite, entre otros, el *marketing* directo), o una *disposición legal* que lo autorice. Un ejemplo de esta última lo constituye la Disposición Adicional 21ª de la *Ley Orgánica 4/2007, de 12 de abril, por la que se modifica la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades*, por cuya virtud no es preciso el consentimiento de los estudiantes para la publicación de los

resultados de las pruebas, ni del personal universitario para la publicación de los resultados de los procesos de evaluación de la actividad docente, investigadora y de gestión; no obstante, dichas publicaciones deben hacerse conforme a lo previsto en la Disposición Adicional 7ª LOPDyGDD, de manera que si se publica un listado, éste debe contener sólo los DNI o, a lo sumo, los nombres y apellidos junto con cuatro dígitos aleatorios del documento. La mayoría de reglamentos de evaluación prevén la publicación solo por DNI, lo cual constituye una buena práctica.

La publicación de listados que incluyen datos personales es práctica habitual en las Universidades, no sólo con calificaciones, sino en otros muchos casos: censos electorales, solicitantes y admitidos a pruebas de acceso a plazas y candidatos propuestos para las mismas, becas y ayudas al estudio o a proyectos (igualmente, solicitantes y beneficiarios), asignaciones de trabajos de fin de grado o máster, etc. A todos ellos es aplicable esta DA 7ª LOPDyGDD. También se verían afectados por la necesidad de limitar los datos hechos públicos los portales de transparencia (DA 2ª de la misma norma), exigiéndose, según los casos, consentimiento expreso de los interesados o disociación de los datos, entre otras medidas.

4.2. Licitud, lealtad y transparencia. Algunos casos problemáticos en el ámbito universitario

Más allá de tal autodeterminación, y en relación con el tratamiento en sí, éste debe ser *lícito*, *leal* y *transparente*, adjetivos todos ellos que pretenden asegurar la existencia de bases legales para el tratamiento (el consentimiento del interesado o, como se ha visto, una causa justificada amparada por la normativa de protección de datos personales u otra norma habilitante) y que el interesado sepa o pueda saber en todo momento que se están recogiendo, utilizando, consultando o tratando de cualquier otra manera sus datos personales, así como la forma y finalidad de dicho tratamiento (Considerando 39 RGPD). La *transparencia* se vincula, además, a la *información* que el interesado debe tener (y, por lo tanto, facilitarla constituye una obligación del responsable) sobre diversos extremos del tratamiento de sus datos personales: existencia del fichero y tratamiento, su finalidad, identificación del responsable, destinatarios de la información (si van a ser cedidos a terceros), carácter obligatorio o no de las respuestas a las preguntas que se le formulan, consecuencias de la obtención de los datos o la negativa a la misma, conocimiento de sus derechos como titular de los datos y cómo y ante quién ejercerlos, etc. (arts. 12 y ss. RGPD).

Desde el punto de vista práctico, puede presentarse la información por "capas" o "niveles": una primera, más directa y breve (una ventana emergen-

te, unos párrafos de aviso...), con remisión (un enlace, por ejemplo) a una segunda más detallada y técnica (una página específica sobre protección de datos, u otro documento aparte). Con independencia de la información suministrada en el momento de la matrícula, la mejor práctica en el caso de las Universidades implica facilitarla nuevamente (aun de forma breve, destacando la finalidad y los derechos del interesado) en cada documento en que se pidan datos y en cada servicio que preste a través de la Red (p. ej., campus virtuales, editores de blogs, repositorios de trabajos..., en la referida forma de "capas").

En definitiva, no caben tratamientos opacos o al margen, si no de la voluntad (pues, como hemos visto, existen algunos que no requieren consentimiento del interesado), sí de su conocimiento. No obstante, la existencia de una causa legal legitimadora hace que, en ocasiones, el interesado desconozca o bien el propio tratamiento en sí (al menos, de inicio), o bien no pueda ejercer sobre el mismo sus derechos en toda su plenitud. Tal puede suceder, en el ámbito que nos ocupa, cuando se contemplen procedimientos de quejas o evaluaciones de actividad anónimas (en ambos casos).

La cuestión de la admisión o no de *quejas, reclamaciones o denuncias anónimas* en una Administración Pública como la Universidad (al menos, para la persona o miembro de la misma frente a la cual se plantean: p. ej., que fuera desconocida para los profesores la identidad de los alumnos que presentan una queja por la llevanza de su docencia) no es cuestión a resolver por aplicación de la normativa de protección de datos, sino por la normativa administrativa correspondiente, en valoración de los intereses afectados, tanto del administrado como del funcionario o personal contratado. El art. 24 LOPDyGSS se limita a reconocer, desde la perspectiva de la protección de datos personales, la licitud de un sistema que permitiera poner en conocimiento de entidades de Derecho privado y Administraciones Públicas la comisión en su seno de conductas contrarias a la normativa general o sectorial aplicable, limitando luego el acceso a los datos contenidos en dichos sistemas para garantizar la confidencialidad de los afectados (en particular, los que pongan tales hechos en conocimiento de la entidad). Por lo tanto, si una Universidad llegara a desarrollar un procedimiento de quejas o reclamaciones que permitiera el anonimato o, en aplicación de los oportunos y vigentes procesos de instrucción por parte del órgano correspondiente (Comisión de Docencia, Defensor del Universitario...), se previera o adoptara de forma temporal el secreto de actuaciones, en aplicación de lo previsto en el citado precepto, la Universidad, en cuanto Administración Pública responsable, sí vendría obligada a garantizar dicho anonimato y/o preservar la confidencialidad de la queja, estando igualmente amparada por ese artículo para no dar dicha información al posible afectado/inves-

tigado (interesado, desde la perspectiva de la protección de datos), en los términos previstos en la normativa que regulara tal procedimiento, mientras éste durara.

Cuestión también problemática es la de las *encuestas de satisfacción* de los estudiantes sobre la labor de los docentes, las cuales, siendo anónimas, afectan a la carrera profesional de los profesores (se utilizan para los procesos de acreditación, p. ej.): ¿podrían éstos ejercitar los derechos de oposición o supresión (vid. más adelante) respecto tales encuestas y de los resultados que les afecten (presumiblemente, frente a las que no les resulten favorables)? No es propiamente un procedimiento de queja o denuncia, por lo que no tiene cabida en el arriba citado precepto, pero sí es cierto que están vinculadas a la misión realizada en interés público por la Universidad y su calidad (que es un fin esencial de la política universitaria, *ex* art. 31 LOU); de hecho, en los estatutos de las Universidades, por ejemplo, se contemplan los planes de evaluación de calidad, la obligación del personal docente de someterse a dichos planes y el derecho de los alumnos a participar en los mismos, vinculado a su derecho a recibir una educación universitaria de calidad (así, respectivamente, arts. 107 y 146, 143.f y 154.c de los Estatutos de la Universidad de Salamanca). También entre las funciones de las Agencias de Calidad están las de evaluar la actividad de la docencia impartida por el profesorado (arts. 32 LOU para la Agencia Nacional de Evaluación de la Calidad y Acreditación, y 36 LUCyL para la Agencia regional de Castilla y León, p. ej.), para lo que pueden utilizarse, entre otros medios, dichas encuestas previstas en los planes de las Universidades.

Téngase en cuenta que la calidad en la enseñanza superior es valor y objetivo no sólo de los participantes en la vida universitaria, sino de la sociedad en general, lo que puede amparar estos tratamientos. Mas, siendo lícitos, todavía podrían venir restringidos, al menos temporalmente, en ejercicio de los principios de limitación de la finalidad y del plazo de conservación: sólo debieran utilizarse, en lo que afectara a los titulares, a los efectos de asegurar la mejora de la calidad de su actividad docente (por lo que la existencia de incentivos relacionados con la misma o su exigencia en procedimientos de acreditación debieran estar directamente vinculadas a la misma y suficientemente motivada su relación) y destruirse (o anonimizarse) una vez cumplieran dicha finalidad, sin almacenarse por más tiempo.

4.3. Limitación de la finalidad y minimización de datos

Todo tratamiento debe tener una *finalidad determinada* (no caben expresiones genéricas), *explícita* (conocida, debe ser comunicada al interesado) *y legítima* (conforme con la normativa, ha de tener una base que lo legitime:

consentimiento, norma, contrato...), no pudiendo ser usados los datos personales para otros fines incompatibles; es lo que se conoce como *"limitación de la finalidad"*. Además, los datos de carácter personal sólo se podrán recoger y tratar cuando sean *adecuados*, *pertinentes* y *no excesivos* en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido (*principio de minimización de datos*): para la tramitación, por ejemplo, de una beca o ayuda que sólo dependa, según sus bases, del expediente académico, no deben solicitarse otros datos referentes a la situación familiar o económica (aunque haya otras que sí dependan de tales extremos y en cuyo marco sí puedan recabarse tales datos).

4.4. Indemnidad y confidencialidad

Durante un tratamiento de datos, debe mantenerse su ***exactitud***, rectificándose o suprimiéndose los que sean inexactos, y garantizarse su ***integridad*** y ***confidencialidad***, mediante la adopción de medidas técnicas y organizativas para asegurar su indemnidad y conservación, impidiendo pérdidas, alteraciones y accesos no autorizados a los mismos. Frente a la regulación anterior, el RGPD y la nueva LOPDyGDD no establecen unos niveles de seguridad detallados, pero sí indican que han de ser "adecuados", teniendo en cuenta los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los (variables) riesgos de probabilidad y gravedad para los derechos y libertades de las personas físicas.

Producida una *brecha de seguridad*, hay obligación de notificación de la misma, en plazo breve, tanto a la entidad de control como a los interesados.

4.5. Limitación del tiempo de conservación

Los datos, además, no pueden permanecer en poder del responsable de forma ilimitada, pues han de preservarse sólo durante el tiempo que sea necesario para alcanzar la finalidad prevista (*limitación del plazo de conservación*).

La función de la Universidad en relación con la expedición de títulos y que las calificaciones sean requeridas, a efectos de requisitos o méritos, en procesos posteriores, legitima que, aun habiendo alcanzado el título correspondiente, los datos personales de un alumno relacionados con su expediente académico sigan en poder de dicha institución (itinerario académico, calificaciones, convocatorias agotadas, asignaturas reconocidas, créditos cursados, etc.), para la emisión de certificados, p. ej. En relación con exámenes y trabajos, dado que contienen datos personales de los estudiantes (según el citado *caso Nowak*), dicho plazo quedaría presumiblemente vin-

culado al de evaluación y posterior reclamación de las calificaciones obtenidas: más allá del mismo, en cuanto las reclamaciones habrían de ser desestimadas por estar fuera de plazo, se ha cumplido con la finalidad del tratamiento, y los exámenes y trabajos deberían destruirse.

En general, los distintos estatutos reglamentos de evaluación de las Universidades contemplan tal obligación de conservación limitada (así, arts. 143.i de los Estatutos y 13 del Reglamento de la Universidad de Salamanca, en que se habla del siguiente proceso de matriculación o un año), aunque puede surgir un conflicto con las instrucciones o protocolos de funcionamiento de las Agencias de Calidad autonómicas cuando en los procesos de renovación de acreditaciones obligan a presentar, entre la documentación requerida para valorar los distintos ítems de rendimiento, transparencia, etc., pruebas de evaluación de alumnos de varios cursos anteriores. El fundamento del tratamiento que realizan las Agencias (que no son órganos superiores a las Universidades, sino externos a las mismas y con distintas funciones) suele estar basado en el interés público, que es el mismo (en parte, junto con los consentimientos del personal, estudiantes, etc.) que ampara a las Universidades públicas; de hecho, p. ej., la Agencia de Calidad del Sistema Universitario de Castilla y León (ACSUCYL), en cumplimiento de la obligación de informar, cita como bases del tratamiento que realiza el art. 6.1.e RGPD, la Ley Orgánica de Universidades y la Ley autonómica[1].

Parece clara la contradicción en los procedimientos de aplicación de las mismas normativas, entre los procedimientos de las Universidades, que pueden llevar a destruir en breve lapso los exámenes y trabajos de evaluación (es decir, "cancelar" los datos personales, desde la perspectiva de la normativa que nos ocupa) y los de las agencias de calidad, que "obligan" (si no se quiere recibir una evaluación negativa o menos positiva del Título) a conservarlos íntegros (con las propias anotaciones de los profesores, en su caso) por un período más largo, agravando así también la responsabilidad en la que pueden incurrir las Universidades por su mantenimiento, con los riesgos que ello implica. Cabría también la posibilidad de que un estudiante quisiera ejercitar su derecho de supresión para pedir la eliminación de sus exámenes (por la razón que fuera, que no ha de ser justificada, pero podría querer que, dada su relevancia como persona pública, no salgan a la luz por filtraciones), una vez evaluado y superados los plazos de reclamación, por lo que no sería posible facilitarlos a la Agencia de calidad si ésta los reclamara para integrar el portafolio de evaluación del Título... ¿o podría negarse la Universidad a tal petición del interesado sobre la base de que aún

1 Véase la primera capa o nivel en http://www.acsucyl.es/acsucyl/export/system/modules/org.opencms.module.acucyl/elements/galleries/galeria_descargas_2018/ACSUCYL_PPD_BuzonesContacto.pdf, con acceso el 31 de enero de 2019.

pueden serle reclamados por dicha Agencia? Realmente, la misión pública de la Universidad se agota con sus funciones de docencia e investigación, no propiamente las de "revisión" de sus títulos, de manera que solo una interpretación muy amplia de lo que es la "calidad" universitaria y del papel de la institución docente y la agencia podrían justificarlo.

4.6. Proactividad y privacidad desde el diseño y por defecto

Todo responsable del tratamiento debe ser capaz de demostrar el cumplimiento de estos principios (***responsabilidad proactiva***), que se materializan a lo largo de toda la norma en forma, como se ha dicho, de derechos de los titulares y las numerosas obligaciones de los responsables y encargados del tratamiento.

Además, plasmación concreta y directa de esa actitud proactiva son también las llamadas "privacidad desde el diseño" (*privacy by design*) y "privacidad por defecto" (*privacy by default*), que implican, respectivamente, tener en consideración desde el principio la protección de datos como un elemento más de cualquier proyecto tecnológico, empresarial o de gestión administrativa (y no sólo un añadido final), así como limitar por defecto los datos de los usuarios de un servicio que se hacen públicos, de manera que sean los propios interesados quien, mediante una expresa manifestación de voluntad, decidan cuáles pueden serlo. En un rápido e intuitivo ejemplo, un prestador de servicios de red social deberá dar a una nueva cuenta el nivel más alto de privacidad, haciendo públicos por defecto los menores datos posibles, y sólo cuando el usuario expresamente lo permita a través de las opciones de configuración de dicha cuenta. De igual manera, en el ámbito universitario, la operativa a través de un campus virtual que permita también las relaciones entre los estudiantes debiera operar con la mayor de las reservas, debiendo ser ellos los que decidan qué datos propios quieren que conozcan los demás compañeros e, incluso, el personal docente, que debiera tener solo acceso por defecto a los datos que identifiquen al alumno, sin más, de cara a permitir la interacción con él y, en su caso, la evaluación: así, puede ser de interés para el profesor la convocatoria o unidad de permanencia en que se encuentra el alumno en su asignatura, pero no el resto de su expediente, calificaciones en otras materias, etc.

4.7. Responsabilidad e indemnización del daño causado

Producida una *violación de estos principios* (no cumplimiento de tales deberes o infracción de aquellos derechos), se siguen las oportunas *responsabilidades*, de tipo administrativo y civil (e, incluso, penal, en su caso).

Desde el punto de vista administrativo, las infracciones pueden desembocar en importantes sanciones económicas para el responsable o encargado, aunque en este punto las administraciones públicas gozan de un importante privilegio: pueden recibir un "simple" apercibimiento (en su caso, con propuesta de las correspondientes acciones disciplinarias), en lugar de la multa administrativa (art. 83.7 RGPD y, en su desarrollo, haciendo uso de la opción que permite, art. 77 LOPDyGDD, en cuyo punto 1.*i* se mencionan expresamente las Universidades públicas). Desde la perspectiva civil, y con independencia de las sanciones administrativas (multas o apercibimiento), todo responsable (también las administraciones públicas y, por lo tanto, las Universidades) y encargado vienen obligados (solidariamente, pudiendo resarcirse luego entre ellos en función de su responsabilidad en la causación del daño) a indemnizar el daño causado al interesado, que puede reclamar judicialmente (arts. 82 RGPD y 30.2 LOPDyGDD; vid., entre otros, el trabajo de Rubi Puig, 2018).

5. Los derechos del interesado

Los principales derechos del interesado son el derecho de *acceso* (art. 15 RGPD), el derecho de *rectificación* (art. 16 RGPD), de *supresión* (art. 17 RGPD; en la terminología española hasta el momento se denominaba "cancelación") y el derecho de *oposición* (art. 21 RGPD). Son los llamados, por sus iniciales (al menos, hasta ahora), derechos ARCO. A ellos se añaden, en el Reglamento y en la LOPDyGDD, otros nuevos no reconocidos con anterioridad, como son el de *limitación del tratamiento* (art. 18) y *portabilidad de los datos* (art. 20). El sistema se cierra con el *derecho a la información* (vinculado a la transparencia y a la prestación de consentimiento para el tratamiento, ya expuestos; arts. 13 y 14 RGPD), *a no ser objeto de decisiones basadas únicamente en tratamientos automatizados*, incluida la elaboración de perfiles (art. 22) y el *derecho a la indemnización* en caso de daño (art. 82, ya también referido).

En la LOPDyGDD, se regulan en los arts. 12 a 18, con (ab)uso de la técnica de reenvío a la norma comunitaria, sumándose en los arts. 79 y ss. las llamadas "garantías de los derechos digitales", algunas programáticas y ejercitables por la ciudadanía frente a las autoridades públicas (neutralidad de la red, acceso universal a Internet, educación digital) y otros (olvido, los relacionados con el trabajo, la rectificación en Internet, portabilidad en redes, etc.) auténticos derechos (o modalizaciones de los ARCO) del interesado directamente frente a los responsables del tratamiento.

Los derechos ARCO son derechos *personalísimos* (se deniegan si no queda acreditada la identidad de quien los pretende ejercer, como titular o afecta-

do, o no se acredita debidamente la representación) e *independientes* (ninguno de ellos es requisito previo para el ejercicio de los otros), y su *ejercicio* ha de ser *sencillo* y *gratuito* (aunque puede conllevar coste su ejercicio excesivo o infundado, especialmente por su carácter repetitivo, o a través de cauces no habilitados al efecto por el responsable; vid. arts. 12.5 y 15.3 RGPD y 13.4 LOPDyGDD).

5.1. Acceso

Mediante el *derecho de acceso*, el interesado puede pedir al responsable del fichero que le informe sobre qué datos suyos están siendo sometidos a tratamiento, el origen de dichos datos, derechos que tiene como interesado, si se van a tomar decisiones automatizadas, el plazo de conservación y las comunicaciones realizadas o que se prevén hacer de los mismos y sus destinatarios. El responsable del fichero debe facilitar al titular una copia de los datos y toda la información expresada, por medios electrónicos y formatos de uso común, si el interesado presentó la solicitud electrónicamente. Ejercitado el derecho de acceso por el afectado, se considerará excesiva una nueva petición si no han transcurrido seis meses desde la última consulta, salvo que se acredite un interés justificado (art. 13.3 LOPDyGDD).

5.2. Rectificación y supresión. El derecho al olvido

Los *derechos de rectificación* y/o *supresión* (arts. 16 y 17 RGPD) de los datos son, a su vez, deberes del propio responsable del fichero, pues éste puede estar obligado a actuar de oficio (sin que el afectado se lo pida). Luego, bien sea a instancia del titular, bien por propia iniciativa, el responsable está obligado a rectificar y/o suprimir (borrar, cancelar, anonimizar…) los datos cuando el tratamiento no se ajuste a la ley, sean inexactos o incompletos, o cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

Una *modalización* del derecho de cancelación o supresión la supone el llamado *"derecho al olvido"*, que finalmente no consta como derecho autónomo en el RGPD, pero sí recibe desarrollo explícito en la LOPDyGDD (arts. 93 y 94). Por tal se entiende, desde hace unos años, el derecho de las personas a que sus datos o informaciones relativas a ellas (en especial, pero no solo, las que son accesibles por Internet) sean bloqueados o suprimidos por parte de quien los tenga en su poder, bien sea porque afectan a sus derechos fundamentales (como honor, intimidad o propia imagen), bien por haber quedado obsoletos debido al paso del tiempo. La expresión "derecho al olvido" es de origen extrajurídico y no deja de ser ejercicio del derecho de supresión, incluso cuando se dirige frente a intermediarios como los bus-

cadores, toda vez que éstos son considerados auténticos "responsables del tratamiento" de datos (STJUE 13 de mayo de 2014, asunto C-131/12, caso *Mario Costeja*). De hecho, en esta concepción, la cancelación de los datos es sólo exigible frente a los buscadores, redes sociales o proveedores de intermediación, no frente a los medios en los que consta (Prensa, archivos de Televisión o Radio), por ejemplo, la noticia que afecta a la persona (en el propio caso referido y, más recientemente, STS de 15 de octubre de 2015): la noticia puede permanecer tal cual, y puede ser objeto de búsqueda a través de los buscadores internos del medio de comunicación (hemeroteca digital), aunque no sea accesible desde los buscadores genéricos.

Esta sentencia ha sido recientemente matizada por el TC en STC nº 58/2018, de 4 de junio, que cree que el uso de nombres propios como criterio de búsqueda y localización de noticias en una hemeroteca digital puede vulnerar el art. 17 RGPD: la función de búsqueda de la noticia en dicha hemeroteca puede quedar garantizada de otras maneras, sin necesidad de acudir al nombre y apellidos de personas sin relevancia pública, pues siempre será posible, si existe una finalidad investigadora en la búsqueda de información alejada del mero interés periodístico en la persona investigada, localizar la noticia mediante una búsqueda temática, temporal, geográfica o de cualquier otro tipo.

En todo caso, habrá que ver el recorrido de esta doctrina, pues el choque con la libertad de información es evidente, y ha sido puesto de manifiesto por el Tribunal Europeo de Derechos Humanos, tan solo unos días después de la decisión de nuestro Tribunal Constitucional, en sentencia de 28 de junio de 2018 (caso M.L. y W.W. c. Alemania), en la que se pronuncia a favor de mantener inalteradas las hemerotecas y de que la prensa elija el modo de presentación de la información en un caso determinado, como salvaguarda del propio derecho del público a recibirla. De esta manera, no sería aplicable el derecho al olvido en las hemerotecas de los medios, en línea con lo afirmado por el Tribunal Supremo español.

5.3. Limitación del tratamiento

El *derecho a la limitación del tratamiento* es una novedad del RGPD, que permite al interesado "limitar" el tratamiento de sus datos en determinadas circunstancias, a la espera de ver si los datos son exactos, o qué intereses prevalecen, en lugar de pedir la supresión; esto es, ejercitado este derecho, sólo podrían seguir tratándose con su consentimiento expreso, o para la protección de sus intereses, o por razones de interés público.

5.4. Portabilidad

Nuevo también es el *derecho a la portabilidad* de los datos, que supone, cuantitativa y cualitativamente, un paso más allá del tradicional derecho de acceso: en ciertos casos, el titular puede solicitar al responsable la entrega de los datos que le facilitó, y que lo haga en un formato estructurado, de uso común y lectura mecánica, *para dárselos a otro responsable*; puede solicitar, incluso, que tales datos se transmitan directamente entre ambos responsables (el antiguo y el nuevo), si es técnicamente posible. En el actual contexto de portabilidades telefónicas, redes sociales (el art. 95 LOPDyGDD lo contempla expresamente en este supuesto), servicios financieros *on line* y servicios de *cloud computing*, la utilidad de un derecho con tal alcance parece incuestionable, aunque pueden presentarse también importantes dificultades en su implementación práctica (por ejemplo, ¿*quid* de los datos generados durante el servicio que puedan ser propios del responsable?); además, ni el Reglamento ni la LOPDyGDD aclaran de cuánto tiempo dispone el primer responsable para dar respuesta a la petición del titular.

5.5. Oposición

El *derecho de oposición*, por su parte, permite al usuario impedir el tratamiento cuando los datos se hayan obtenido sin su consentimiento, en el marco de los intereses lícitos del responsable o en ejercicio del interés público, y haya motivos relacionados con su situación particular que justifiquen su petición de no tratamiento.

5.6. La valoración del comportamiento y elaboración de perfiles automáticos

Mediante el ejercicio del derecho a que no se tomen decisiones individuales automatizadas o se elaboren perfiles de igual forma, los interesados pueden impugnar actos que supongan valoración de su comportamiento y que tengan repercusiones jurídicas (p. ej., rendimiento laboral, crédito...) sobre la única base de un tratamiento de datos de carácter personal que incluya definición de sus características o personalidad, salvo que haya alguna causa legitimadora (celebración o ejecución de un contrato entre responsable e interesado, autorización legal, consentimiento explícito previo); es de gran relevancia en ámbitos como los seguros, banca, salud...

5.7. Los derechos digitales en el ámbito del trabajo

Dentro de las *garantías de los derechos digitales* que recoge la LOPDyGDD como gran novedad, por último, cabe mencionar algunos derechos relacionados con el trabajo cuyo reconocimiento expreso y tratamiento siste-

mático permite ahora darles una auténtica dimensión de protección de la esfera privada de los trabajadores. Así, como gran novedad en España (en otros países, como Francia, ya se había reconocido), se consagra el *derecho a la desconexión digital en el ámbito laboral* (art. 88), cuyo ejercicio puede resultar de gran interés para el personal docente universitario (en particular, al que realiza, además, tareas de gestión). Por virtud de este nuevo derecho, los trabajadores y empleados públicos tienen derecho a que se limite el uso de las tecnologías de la información y comunicaciones (TIC; en referencia, sobre todo, al uso de correo electrónico, mensajería instantánea, o al más tradicional y simple "teléfono" como tal), fuera del tiempo de trabajo legal o pactado, de manera que se respeten tanto su tiempo de descanso como su intimidad personal y familiar.

Se recogen también el *derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral* (art. 87), que protege la intimidad de los trabajadores y empleados públicos cuando utilizan los medios electrónicos puestos a su disposición por el empleador, quien solo podrá acceder a los contenidos de los mismos a los solos efectos de controlar el cumplimiento de las obligaciones de aquéllos, previo el establecimiento, junto con los representantes de los trabajadores, de los criterios de utilización de los dispositivos; y los *derechos a la intimidad frente al uso de dispositivos de videovigilancia y grabación de sonidos en el lugar de trabajo* (limitando los fines y lugares en que pueden instalarse; art. 89), *y ante la utilización de sistemas de geolocalización* (art. 90). A todos ellos, se pueden añadir más garantías como resultado de la negociación colectiva (art. 91).

6. Una última cuestión: introducción al papel del Delegado de Protección de Datos

Aunque la labor de supervisión general del cumplimiento de la normativa de protección de datos recae en las autoridades de control territoriales (en España, la Agencia Española de Protección de Datos, sin perjuicio, dentro de sus limitadas competencias, de las agencias autonómicas donde las hubiera) en el concreto ámbito de cada empresa o administración pública es el Delegado de Protección de Datos (DPD o DPO, por sus siglas en inglés, *Data Protection Officer*), el encargado de controlar el cumplimiento de la normativa de protección de datos por parte del responsable, y servir de enlace entre éste y la autoridad de control. Entre otras funciones, el Delegado asesorará al resto de servicios de la empresa o administración en todo lo que tenga que ver con protección de datos personales, contribuyendo en el diseño de procesos, dando respuestas a cuestiones del personal e interviniendo activamente en su formación sobre esta materia.

La novedad de esta figura que introdujo el RGPD es relativa: lo es para España, cuya legislación hasta el momento no la recogía, pero no para otros Estados miembros, en los que ya existía con carácter obligatorio (así, Alemania), u opcional (por ejemplo, Austria u Holanda). En un término medio, el Reglamento no ha impuesto una obligación general de nombramiento de un DPD para todo responsable o encargado del tratamiento, pero sí para las administraciones públicas (salvo la judicial en el desempeño de su función) y para las entidades que monitoricen datos personales a gran escala, en particular si lo hacen sobre categorías especiales de datos (art. 37). El art. 34.1.*b in fine* LOPDyGDD se refiere expresamente a la obligación de tener DPD por parte de las Universidades públicas y privadas.

El DPD puede ser una persona física o jurídica, y perteneciente al personal de la propia entidad, o subcontratada, pero es su característica esencial, aunque fuera nombrado entre el personal interno, que actúa siempre con independencia respecto del resto de órganos, incluidos los de dirección; en este punto, se asemeja al propio Defensor Universitario, en nuestro ámbito.

Tanto el Reglamento como la LOPDyGDD señalan que puede elegirse a cualquier persona (jurídica o física) según sus cualidades y atendiendo a sus conocimientos especializados del Derecho y la práctica de la materia de protección de datos, lo cual no obliga a ser licenciado o graduado en Derecho, aunque la AEPD lo considera aconsejable. Esos conocimientos pueden justificarse, entre otras formas, vía lo previsto en el art. 35 LOPDyGDD, que consagra lo que ya viene haciendo la AEPD: el seguimiento de cursos de certificación. La AEPD ha diseñado un proceso de homologación de tales cursos, de manera que, en el futuro próximo, la mayoría de DPO serán profesionales juristas o informáticos con dicha formación *ad hoc*, siquiera sea por la propia exigencia del mercado, que presumiblemente excluirá a quienes, aun teniendo conocimientos, no se encuentren en posesión de un título obtenido en un curso homologado.

En el ámbito universitario se han extendido distintas prácticas, y podemos encontrarnos tanto con Delegados profesores de Derecho especializados en este campo (miembros del Personal Docente e Investigador de la propia institución), como con informáticos pertenecientes al Personal de Administración y Servicios, que asumen estas tareas, en ocasiones con algún tipo de comité de apoyo que incluye técnicos y juristas. En otros casos, se cuenta con el asesoramiento externo de empresas dedicadas a proveer este servicio, o que lo asumen directamente, con personas de contacto en la institución (a través de la Secretaría General, habitualmente).

Sobre la figura del DPD, con enfoque práctico (propone varios casos prácticos con soluciones) y con mención ya de la nueva LOPDyGDD, puede verse en un trabajo de Simón Castellano (2018).

Normativa citada

CE: Constitución Española, de 27 de diciembre de 1978, *Boletín Oficial del Estado* nº 311, de 29 de diciembre de 1978.

Convenio 108: Convenio nº 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981, *Boletín Oficial del Estado* nº 274, de 15 de noviembre de 1985.

Directiva 95/46: Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, 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.

Estatutos USAL: Estatutos de la Universidad de Salamanca, aprobados por Acuerdo 19/2003, de 30 de enero, de la Junta de Castilla y León, *Boletín Oficial de Castilla y León* nº 22 de 3 de febrero de 2003; modificados por Acuerdo Acuerdo 38/2011, de 5 de mayo, de la Junta de Castilla y León, *Boletín Oficial de Castilla y León* nº 90 de 11 de mayo de 2011

LOPD: Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter Personal (disposición derogada), *Boletín Oficial del Estado* nº 298, de 14 de diciembre de 1999.

LOPDyGDD: Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, *Boletín Oficial del Estado* nº 294, de 6 de diciembre de 2018.

LORTAD: Ley Orgánica 5/1992, de 29 de Octubre, de Regulación del Tratamiento Automatizado de Datos de carácter personal (disposición derogada) *Boletín Oficial del Estado* nº 262, de 31 de octubre de 1992.

LOU: Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, *Boletín Oficial del Estado* nº 307, de 24 de diciembre de 2001.

LPAC: Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, *Boletín Oficial del Estado* nº 236, de 2 de octubre de 2015.

LUCyL: Ley 3/2003, de 28 de marzo, de Universidades de Castilla y León, *Boletín Oficial de Castilla y León* nº 65, de 4 de abril de 2003.

Resolución 509: Resolución 509/1968 de la Asamblea del Consejo de Europa relativa a "Los derechos humanos y los nuevos logros científicos y técnicos".

Resolución 22: Resolución 73/22 del Comité de Ministros del Consejo de Europa relativa a "La protección de la vida privada de las personas físicas respecto de los bancos de datos electrónicos en el sector privado", de 26 de septiembre de 1973.

Resolución 29: Resolución 74/29 del Comité de Ministros del Consejo de Europa relativa a "La protección de la vida privada de las personas físicas respecto a los bancos de datos electrónicos en el sector público" de 20 de septiembre de 1974.

RGPD: 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 (*Reglamento General de Protección de Datos*). *Diario Oficial de la Unión Europea,* L 119/1, de 4 de mayo de 2016.

Reglamento de Evaluación de la Universidad de Salamanca, aprobado en la sesión del Consejo de Gobierno de 19 de diciembre de 2008, modificado en las sesiones del Consejo de Gobierno de 30 de octubre de 2009 y 28 de mayo de 2015.

Bibliografía citada

ARAGONÉS SALVAT, J. (2016), *GDPR (General Data Protection Regulation), el nuevo Reglamento Europeo de Protección de Datos*, edita Ateneu Privacy Consulting, Tortosa.

LÓPEZ ÁLVAREZ, L. F. (2016), *Protección de datos personales: adaptaciones necesarias al nuevo Reglamento europeo*, edt. Francis Lefebvre (col. Claves Prácticas), Madrid.

LÓPEZ CALVO, J. (2017), *Comentarios al Reglamento Europeo de Protección de Datos*, edt. Sepin, Madrid.

LÓPEZ CALVO, J. (coord., 2019), *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD*, Wolters Kluwer, Madrid, 2019.

PIÑAR MAÑAS, J. L. (dir., 2016) *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*, edt. Reus, Madrid.

RUBÍ PUIG, A. (2018), "Daños por infracciones del derecho a la protección de datos personales. El remedio indemnizatorio del artículo 82 RGPD", *Revista de Derecho Civil*, vol V, nº 4, pp. 53-87, disponible en http://www.nreg.es/ojs/index.php/RDC/article/view/354, con último acceso el 29-I-2019.

SIMÓN CASTELLANO, P., *El desempeño de las funciones de Delegado de Protección de Datos, Wolters Kluwer*, Madrid, 2018.

TRONCOSO REIGADA, A. (2013), "Las redes sociales a la luz de la propuesta de reglamento general de protección de datos personales" Parte uno, *IDP* nº 15, pp. 61-75.