LA PROTECCIÓN DE LOS DATOS PERSONALES COMO EXCEPCIÓN A LA OBLIGACIÓN DE REUTILIZACIÓN DE LA INFORMACIÓN DEL SECTOR PÚBLICO[1]

José María de la Cuesta Sáenz
Catedrático de Derecho Civil
Universidad de Burgos

SUMARIO: I. Estado actual de la protección de los datos personales en España.

II. Conceptos básicos. 1. Conceptos generales en materia de datos personales. 2. Datos personales cuya publicación haya permitido con anterioridad su titular. 3. La figura del Delegado de Protección de Datos. 3.1 Requisitos de los DPD. 3.2 Caracterización de los DPD. 3.3 Funciones de los DPD. 4. La variedad de datos personales objeto de tratamiento en la Universidades.

III. Regulaciones contractuales y sistemas alternativos de resolución de litigios en materia de DPD.

IV. Conclusiones acerca de la protección de los datos personales como excepción a la obligación de autorizar la reutilización de la información del sector público. 1. Criterios de la libertad de publicar datos personales. 2. Efectividad de la protección de los datos personales. 3. Tutela judicial efectiva. 4. Datos abiertos. 5. Cauces de aplicación de la protección de los datos personales.

[1] Este trabajo se ha realizado en el marco del proyecto de investigación "Propiedad intelectual y *Open Data* en la Universidad: intersección entre propiedad intelectual, reutilización de la información del sector público y la protección de datos" DER2016-75709-R (MINECO/FEDER/UE) del que es investigadora principal Raquel de Román, y se ha publicado en 2020 por la editorial Comares como parte de la monografía "Información en abierto y propiedad intelectual en la Universidad".

I. Estado actual de la protección de datos personales en España. El Reino de España había atendido a la puesta en marcha de la protección de los derechos fundamentales a la intimidad personal y familiar y al honor contemplados en el artículo 18 de la Constitución española, entre otras normas, mediante la Ley Orgánica 1/1982 de 5 de mayo, pero en lo referente a la protección de los datos personales hubo que esperar a la Ley Orgánica 5/1992 de 29 de octubre, de Regulación del Tratamiento Automatizado de Datos Personales (LORTAD).

El Tribunal Constitucional[2] por su parte en la sentencia 94/1998 de 4 de mayo recordó la existencia de un derecho fundamental al control de los propios datos personales, y poco después la Ley Orgánica 15/1999 de Protección de Datos de Carácter personal, vino a reemplazarla al trasponer la

[2] El Tribunal constitucional en su sentencia 254/1993 de 20 de julio había rechazado la idea de que el artículo 18.4 de la Constitución se limitase a otorgar una protección meramente negativa a los datos personales como faceta del derecho a la intimidad. En tal sentido ver A. OLLERO TASSARA "De la protección de la intimidad al poder de control sobre los datos personales. Exigencias jurídico-naturales e historicidad de la jurisprudencia constitucional", en *Academia de Ciencias Morales y Políticas,* 2008, págs. 7 a 179, y más recientemente afirma "emerge una buena noticia: ha nacido un nuevo derecho fundamental", ver "Controllo di constituzionalità: tra tradizione e globalizazione. Il caso spagnolo", en *Archivio giuridico*. Año CLI, fasc. 2 (2019), pág. 247, y ahora también en "Genética, el individuo y la familia", en *A Justiça constitucional face aos desenvolvimentos tecnológicos,* 3ª *Conferência quadrilateral,* Lisboa,-Portugal, 10 a 12 de outubro de 2019.

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

Posteriormente, comenzado el siglo XXI inciden de nuevo en materia de protección de datos el artículo 8 del Carta de Derechos Fundamentales de la Unión Europea y el artículo 16.1 de Tratado de Funcionamiento de la Unión Europea.

En cumplimiento de esas previsiones se intensificaron los trabajos y multiplicaron los impulsos orientados a lograr una regulación más uniforme del derecho fundamental a la protección de datos de carácter personal en pleno progreso de la globalización, y la Comisión publica el 4 de noviembre de 2010 una comunicación titulada "un enfoque global de la protección de los datos personales en la Unión Europea"[3], y el 25 de enero de 2012 otra sobre "La protección de la privacidad en un mundo interconectado. Un marco europeo de protección de datos para el siglo XXI"[4], que inician la reforma del marco europeo, reforma que culmina en la aprobación del Reglamento UE nº 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 de protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de los mismos, que deroga la Directiva 95/46/UE.

Este proceso en el que se transita de la Directiva armonizadora, al Reglamento de aplicación directa (o en algún otro caso, a la Directiva de armonización total), ha tenido lugar en muy distintos campos del Derecho de la Unión europea, habiendo obedecido siempre a la búsqueda de una mayor eficacia y a la evitación del efecto paradójicamente diversificador que produce la concesión de amplios márgenes a los Estados miembros a la hora de trasponer las Directivas a sus respectivos ordenamientos jurídicos[5].

El tránsito indicado de un Derecho armonizador a otro de aplicación directa a todos los Estados miembros de la Unión, tiene pues como fin, evitar esa

[3] COM(2010)609
[4] (COM(2012)9 final
[5] Hay ejemplos en la regulación del desarrollo rural como faceta estructural de la Política Agrícola Común en la que se pasó de las Directivas de los primeros años 70 (llamadas socio-estructurales) a los Reglamentos de aplicación directa primero en agrupaciones de productores (1978) y los sucesivos reglamentos posteriores en materia de desarrollo rural desde el 797/1985, al vigente 1308/2013, y en materia de protección de los consumidores y usuarios, en la que las viejas directivas se sustituyeron por una Directiva de armonización total

posible dispersión que puede producirse y que aleja las legislaciones de los distintos Estados y frustra el proceso armonizador, como efecto perverso de márgenes concedidos a los Estados miembros de la UE excesivamente amplios, que se ha observado en ocasiones. Frente a ese efecto solo cabe utilizar la Directiva de armonización completa (como se hizo en 2011 en materia de protección de los consumidores), o el todavía más expeditivo medio que representa el Reglamento de aplicación directa, que se hace necesario para lograr ese marco europeo de protección de datos para el siglo XXI[6].

Por otra parte, el Tribunal de Justicia de la Unión Europea, hubo de pronunciarse en alguna ocasión sobre aspectos relacionados con la protección de datos y así, en los asuntos C-362/14 y C-201/14 , resolvió sobre la exigencia de ”puerto seguro” y su incumplimiento mediante transferencia de datos a servidores sitos en EE.UU., y sobre la necesidad de previa comunicación al interesado, a efectos del ejercicio de sus derechos de oposición y rectificación, de la transferencia de datos personales entre administraciones. En ambos vicios han incidido numerosas administraciones públicas europeas, y por lo que respecta a España, es notorio el desparpajo con el que lo ha hecho la AEAT, o el lamentable espectáculo que se ha vivido con ocasión de los dos *referenda* realizados estos últimos años en Cataluña, o más recientemente con la publicación de los datos personales de la denunciante en un proceso penal por agresión sexual.

En todo caso, la intención del Legislador español, tal y como por el momento expresa el Preámbulo de la Ley Orgánica 3/2018 de 5 de diciembre[7] (en adelante LOPDGDD), va más allá de la mera transposición del Reglamento, puesto que pretende, dentro de los límites que el Reglamento establece, aplicar la propia tradición española en materia de protección de datos personales[8].

---

[6] El civilista J. Plaza Penades, en la comparecencia ante la Comisión de Justicia del Congreso de los Diputados de 15 de marzo de 2018 habla, no sin cierta exageración, de “cambio de paradigma” para referirse a este cambio más bien instrumental.

[7] Apartado III *in fine*.

[8] Ello no obstante, el Prof. Plaza Penades en la Comparecencia citada en la nota precedente critica que el Proyecto de Ley orgánica no tenga reflejo en el Código civil, así como la ausencia de disposiciones generales y definiciones que el intérprete debe buscar en el Reglamento UE y no en la Ley, lo que dificulta su actividad. La Profesora Moro Almaraz estima que esa asumida complementariedad del Proyecto de LO vino impuesta por el Dictamen del Consejo de Estado que vetaba cualquier reproducción del Derecho de la UE. Por el contrario, el Prof. Piñar Mañas en la sesión de 27 de febrero de 2018 compareció y expuso la

II. Conceptos básicos.

1. Conceptos generales en materia de datos personales: su regulación. Interesa en primer lugar sentar la premisa de que la citada LOPDGDD española de 3 de diciembre de 2018 no reproduce las definiciones del Reglamento UE nº 2016/679 porque se ha seguido el dictamen en tal sentido formulado por el Consejo de Estado, lo que no ha dejado de producir alguna incomodidad en los intérpretes[9], ya que hará necesario tener presentes ambos textos tras de la entrada en vigor de la nueva LOPDGDD. Interesa también determinar con precisión el ámbito de aplicación de la Ley Orgánica que nos ocupa, y que, de entrada, se circunscribe a la "persona física", según establece su artículo 1 apartado a).

No hay lugar, por lo tanto, para plantearse la extensión de la protección de datos personales a las personas jurídicas, lo que excluye cualquier vacilación al respecto, semejante a la que tuvo lugar durante cierto tiempo en España con la protección del derecho al honor, y resulta ciertamente una clarificación importante y digna de alabanza tanto respecto de la aplicación directa, como respecto de la aplicación analógica, ya que ambas están terminantemente excluidas, lo que hace ociosa e impertinente cualquier digresión sobre el particular.

Ni que decirse tiene que no sólo es acertada esta decisión por evitar trabajo al intérprete, sino también por cuestiones de fondo, ya que falta por completo la identidad de razón que pudiese justificar la analogía entre persona física y jurídica, en materia de derechos fundamentales.

Desde el punto de vista contrario, es decir, respondiendo a la pregunta acerca de contra quién se protegen y reservan los datos personales, también parece claro que se trata de un derecho dotado de protección absoluta, o en la terminología tradicional, con protección *erga omnes*, lo que aproxima los datos personales a los llamado bienes de la personalidad, es decir, al deber

---

corrección técnica del Proyecto y de los trabajos de la Sección de Derecho Público de la Comisión de Codificación en su elaboración.

[9] Ver Consejo de Estado Dictamen sobre el Anteproyecto de Ley Orgánica de Protección de Datos Personales, de 26 de octubre de 2017 (Documento CE-D-2017-757, apartado de cuestiones previas, y consideraciones del Prof. J. Plaza Penades, citadas en la nota 5 *supra*

general de respeto a la persona de que muy atinadamente trataba F. de Castro[10].

En cuanto al ámbito objetivo, es decir, en lo relativo a los comportamientos o conductas que contempla la Ley Orgánica, ésta se aplicará a cualquier tratamiento "total o parcialmente automatizado" de los datos personales contenidos o destinados a ser incluidos en un fichero, aunque la LOPDGDD en su artículo 2 apartados 3 y 4 precisa la exclusión de los tratamientos realizados al amparo de la Ley Electoral General, los realizados en el ámbito de las instituciones penitenciarias y los derivados de los Registros Civil, de la Propiedad y Mercantiles que remite a su legislación específica[11], y los realizados con ocasión de la tramitación por los órganos judiciales de los procesos en que sean competentes, así como del tratamiento realizado dentro de la gestión de la Oficina Judicial, pero prevé la exclusión de los protocolos notariales pese a su indudable analogía.

Además, de nuevo desde el punto de vista subjetivo, la Ley Orgánica en su artículo 2.2 a), por remisión al artículo 2.2 del RGPD excluye de su ámbito de aplicación los tratamientos automatizados total o parcialmente, que lleven a cabo personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.

Novedad, relativa, pero destacable de la Ley Orgánica 3/2018 es el tratamiento de los datos personales de las personas fallecidas, que, aunque en principio resulta excluido por el artículo 2.2 b) del ámbito de aplicación de la LO, en congruencia con el hecho de que han dejado de ser datos correspondientes a personas una vez extinguida la personalidad por la muerte, lo hace no obstante objeto de una regulación específica.

En efecto, el artículo 3 regula el acceso "de las personas vinculadas al fallecido por razones familiares o de hecho así como sus herederos", y, en su caso, el derecho de rectificación y de supresión, en lo que resulta un ejemplo

[10] F: DE CASTRO Y BRAVO, *Derecho civil de España*, T. II, *Derecho de la persona*, ed. Instituto de Estudios Políticos, Madrid, 1952, págs. 35 y ss.

[11] Ver la propuesta de I. VIVAS TESÓN, "El nuevo régimen de protección de datos y el Registro de la Propiedad", *Derecho Privado y Constitución*, nº 33(2018), pág. 155, pero lo cierto es que se trata de una remisión vacía de contenido por el momento, ya que tal regulación no existe por l momento en materia de Registro de la Propiedad y Registros Mercantiles. Por el contrario, no hay exclusión semejante para los protocolos notariales que quedan sometidos plenamente a la normativa contenida en el RGDP y en la LOPDP. Ver en tal sentido FERNÁNDEZ LOZANO, J.L., "La protección de datos y la función pública notarial", en *Revista Jurídica del notariado*, nº 108-109, enero-junio 2019, págs. 116 y ss.

más del deber general de respeto a la persona que puede que se haga valer por un tal vez demasiado amplio círculo de allegados, en modo parejo a la posibilidad que los herederos tienen de proseguir acciones de filiación (tanto de reclamación como de impugnación según los arts. 132, 133 y 136 del Código civil), sin que en absoluto se trate de una personalidad prolongada más allá de la muerte[12], como lo pone de relieve que tal posibilidad pueda ser prohibida expresamente no sólo por disposiciones legales, sino también por voluntad expresa del difunto.

Los artículos 4 y siguientes de la Ley Orgánica de PDGDD, establecen los principios que han de regir la protección de datos personales, principios que a su vez resultan ser aplicaciones, bien del principio de legalidad (v.gr. los arts. 4 y 9), bien del principio de libertad (v.gr. artículos 6 y 7).

Novedad también digna de ser destacada es la previsión del consentimiento de los menores de edad que posibilita el artículo 7.1 de la LOPDP "El tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de catorce años".

La regulación de nuevo se aproxima a la de los bienes de la personalidad, en este caso a la que se contiene en el artículo 162. 2º, núm. 1º del Código civil que exceptúa de la representación legal de los padres "los actos relativos a derechos de la personalidad u otros que el hijo, de acuerdo con las leyes y con sus condiciones de madurez, pueda realizar por sí mismo[13]".

En efecto, el artículo 7 de la LOPDP parece coincidente en la medida en que establece que sólo puede fundarse el tratamiento de los datos de un menor en su propio consentimiento si es mayor de catorce años, lo que significaría que hasta esa esa edad, solamente se podría llevar a cabo tratamiento total o parcialmente automatizado de los datos de los menores, con su consentimiento prestado con asistencia de quienes ejerzan la función parental.

Cabe, sin embargo, formularse algunas preguntas al respecto, de las que la primera es si están los datos personales incluidos en los derechos de la

[12] F. DE CASTRO Y BRAVO, *op. cit.*, págs., 146 y 147. Respecto de los datos de los fallecidos, ver MARTÍNEZ MARTÍNEZ, N. "Reflexiones en torno a la protección *post mortem* de los datos personales y la gestión de la transmisión *mortis causa* del patrimonio digital tras la aprobación de la LOPDGDD", en *Derecho Privado y Constitución*, nº 35 (2019), págs. 169 y ss,

[13] Ver sobre esa disponibilidad de los menores en relación con el sexo que publica el Registro Civil, la reciente STC 99/2019 de 18 de julio en su fundamento jurídico noveno.

personalidad o no, ya que en caso de respuesta negativa a este interrogante podría entenderse que los padres representan a los menores a estos efectos hasta que éstos cumplan catorce años.

La doctrina parece convencida por lo general de que el nombre es un derecho de la personalidad[14], y los códigos civiles del pasado siglo XX pasaron a considerarlo como derecho de la personalidad[15], lo que debería extenderse a todos los signos distintivos de la persona física, y por ende a los datos personales, todo lo cual, conduce a entender que en rigor este artículo 8 del Reglamento UE no remite a la representación de los titulares de la patria potestad o tutores en cuanto a consentimiento del tratamiento de datos de los menores de catorce años a efectos de los servicios de la sociedad de la información, salvo en los casos en que la ley exija la asistencia de los titulares de la patria potestad o de la tutela[16].

La segunda cuestión se refiere a la indicación en el texto de la LOPDGDD de una edad tan peculiar como la edad de catorce años, jamás tenida por significativa con anterioridad en nuestro ordenamiento jurídico, salvo a efectos de otorgamiento del testamento notarial (artículo 663 1º del Código civil *a contrario sensu*). Pero la explicación es muy simple puesto que se trata de la edad mínima que fijaba como exigible para la validez del consentimiento del menor el Reglamento publicado por RD 1720/2007, de 21 de diciembre de desarrollo de la LOPD 15/1999 de 13 de diciembre[17].

En todo caso se excluye de la posible validación por consentimiento del afectado el tratamiento de ciertos datos cuya finalidad sea identificar la

---

[14] En tal sentido J. CASTÁN TOBEÑAS, *Derecho civil español, común y foral,* 14ª ed., a cargo de J. DE LOS MOZOS DE LOS MOZOS, T. 1 VOL II, pág., 377, Reus, Madrid, 1987,

[15] En tal sentido F. DE CASTRO Y BRAVO, "Los llamados derechos de la personalidad", *Anuario de Derecho* Civil, 1959, fasc. 4, pág.1.244.

[16] Ver M. ARIAS POU, cap. VIII de *Reglamento general de protección de datos***,** dirigido por J.C. Piñar Mañas, ed. Reus, Madrid, 2016, pág. 175. El tema ha sido abordado también en la Comparecencia ante la Comisión de Justicia del Congreso de los Diputados de 15 de marzo de 2018 por el civilista J. Plaza Penades quien afirmaba que, a su juicio, "los dieciseis años sigue siendo una edad óptima para estos menesteres", aclarando que en último término un consentimiento del menor puede ser declarado nulo si le perjudica conforme al artículo 3 de la Ley Orgánica de Protección del Menor

[17] Anteriormente la cuestión del consentimiento de los menores estaba regida por un Real Decreto que previó tal posibilidad a partir de los 14 años (art. 13 RD 1720/2007 de 21 de diciembre que aprueba el Reglamento de desarrollo de la LO 15/1999 de 13 de diciembre). Indica A. PIÑAR REAL, "Tratamiento de los datos de los menores de edad", en *Reglamento general de protección de datos*, dirigido por J.L. Piñar Mañas, Madrid, 2016, pág. 202, que, tras la entrada en vigor del Reglamento UE, ha pasado a ser de 16 años. Posteriormente la entrada en vigor el pasado día 6 de diciembre de 2018 de la nueva LOPDP ha vuelto a modificar la edad para el consentimiento que ha vuelto a ser de 14 años.

ideología, la afiliación sindical, la religión, la orientación sexual, las creencias, o el origen racial o étnico, si bien el artículo 13 excluye de la ilicitud el tratamiento de los datos que hayan sido publicados por el propio interesado, lo que parece poco probable tratándose de menores de catorce años.

Los derechos reconocidos a las personas de cuyos datos personales se trata con respecto el tratamiento de éstos, se contemplan en los artículos 11 a 18 de la Ley Orgánica, y se mantienen en lo esencial similares a la legislación precedente, aunque su definición es más rigurosa y merece capítulo aparte el estudio detallado de los mismos a la luz del conjunto de la nueva regulación.

2. Los datos personales cuya publicación haya permitido con anterioridad su titular.

Tanto la legislación precedente, como el Reglamento UE que entró en vigor el día 26 de mayo de 2018, excluyen en todo caso la ilicitud del tratamiento de los datos personales cuya publicación haya permitido con anterioridad su titular, incluso cuando se trate de datos de categorías especialmente protegidas como los que contempla el artículo 9.1 de la LOPD "que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas o la filiación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física"[18].

La significación de esa publicación previa que excluiría la ilicitud del tratamiento dista sin embargo de ser clara, porque no es unívoco el concepto publicación y la idea misma de publicidad ya que los Registros públicos están precisamente destinados a esa publicidad, desde el propio Registro Civil que publica el estado civil de las personas físicas, y en el que la persona ingresa

[18] Sobre los datos relativos a las opiniones políticas, ha recaído recientemente la sentencia del Tribunal Constitucional 76/2019 de 22 de mayo, que anula la Disposición Final 2.3 de la LOPDGDD acogiendo uno de los argumentos esgrimidos por el Defensor del Pueblo que interpuso el recurso de inconstitucionalidad, concretamente el argumento de la falta de concreción legal de las garantías para el perfilado de las personas por parte de los partidos políticos con finalidad electoral, que la Ley remite al desarrollo reglamentario

sin que se cuente con su voluntad, pasando por los Registros de la Propiedad y Mercantiles, los protocolos notariales, algunos registros centrales y los registros administrativos y fiscales en los que el ingreso podría ser "voluntario", ya que todos ellos son objeto de publicidad formal más o menos restringida[19].

En este punto hay que tener presente que los fenómenos del terrorismo y del blanqueo de capitales de procedencia ilícita, han dado lugar en el siglo XXI junto con la informatización de tales Registros, a ficheros públicos como el índice notarial único[20] o el registro de titularidades reales en el caso español, que constituyen bases de datos de gigantescas proporciones, y consistentes en buena parte en datos personales. ¿Qué ha entenderse entonces por publicación? No resulta fácil la respuesta y merece un estudio más profundo del que aquí puede darse.

Tal vez por ello, el artículo 77 de la LOPDGDD, establece un régimen de responsabilidad especial para los entes del apartado 1, (el subapartado i) se refiere a las Universidades Públicas), a los que no se aplica el régimen sancionador de los artículos 70 a 76 de la LOPDGDD sino un régimen alternativo en que si los "responsables o encargados enumerados en el apartado 1 ", cometiesen alguna de las infracciones a que se refieren los artículos 72 a 74, la autoridad de protección de datos que resulte competente habría de dictar resolución sancionando a las mismas con apercibimiento. La resolución establecerá las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido".

Es decir: en virtud del citado texto, este apartado que me ha correspondo desarrollar ofrece, pese a su indudable interés, poco amparo a los administrados, y entre tanto la aplicabilidad directa del Reglamento a partir del día 26 de mayo tampoco ofrecía otras más claras perspectivas de

[19] Uno de los Registros de más restringido acceso es sin duda el Registro Central de Actos Última Voluntad, por obvias razones de reserva de las voluntades testamentarias en vida de los testadores.

[20] Sobre el particular ha pronunciado recientemente una muy interesante conferencia el Dr. D. Juan Alvarez-Sala Walther en la sesión de 10 de mayo de 2018 de la Academia Matritense del Notariado, titulada "La función notarial entre la privacidad y la transparencia" *Anales Academia Sevillana del Notariado, Clausura Curso Académico 2017-2018.* Respecto del Registro de la Propiedad, ver I. Vivas Tesón, "El nuevo régimen de protección de datos y el Registro de la Propiedad", en *Derecho Privado y Constitución*, nº 33 (2018), págs. 117 y ss.

efectividad de la protección de los datos personales constantes en ficheros públicos.

3. La figura del "Delegado de protección de datos personales".

El Capítulo III de la Ley Orgánica[21], en su artículo 34 contempla, define, e impone imperativamente a la amplia serie de sujetos que enumera, contar con la figura del "Delegado de protección de datos personales", entre las cuales el apartado 1 b) del artículo se refiere expresamente a las Universidades públicas y privadas.

Se trata de un tema de la máxima importancia y bastante cargado de problemas[22], tanto en lo que se refiere entidades privadas como públicas. En las segundas, como el caso de la Universidades públicas, parece, por lo general, improcedente la externalización, que permite ampliamente el artículo 36 del RGPD, al menos en aquellas que cuenten, como por lo general ocurrirá, con personal permanente perteneciente a cuerpos funcionariales de profesores de áreas de conocimiento jurídicas relacionadas con el derecho público y privado aplicable, y con personal de Administración y Servicios de muy elevada cualificación en materia jurídica.

Las razones de esta opción, radican en que de este modo y mediante la redacción cuidadosa de un Reglamento que establezca su Estatuto, es posible garantizar el cumplimiento de las exigencias de independencia y autonomía, así como la cualificación profesional y la asunción de un coste razonable, por cuanto podría ser retribuida su actividad mediante descarga parcial de docencia y aplicación analógica de un complemento retributivo, sin tener que crear puestos específicos en la Relación de Puestos Trabajo, puesto que el artículo 38.6 del Reglamento establece que el delegado de protección de datos podrá desempeñar otras funciones y cometidos. El responsable y/o encargado del tratamiento garantizará que dichas funciones no den lugar a conflicto de intereses".

[21] Desarrolla la figura introducida por el Reglamento (UE) 2016/679 de Parlamento Europeo y del Consejo de 27 de abril de 2016, que entró en vigor el día 26 de mayo de 2018.
[22] Ver en tal sentido D. LÓPEZ CARBALLO-ÉCIJA, "¿Por qué es tan difícil designar un responsable de protección de datos?, diario *Expansión*, 2 de marzo de 2018.

Desde luego, la figura es más exigente en cuanto a cualificación especializada que la del Defensor del Universitario, pero es sin duda el Claustro quien debería designarlo, por las razones de independencia y autonomía de la alta dirección que concurren en ambas figuras, pero presenta o podría presentar alguna analogía cuando surgen conflictos. En efecto el artículo 35 de la LOPDGDD establece que "el delegado de protección de datos, sea una persona física o jurídica deberá reunir los requisitos establecidos en el artículo 37.5 del Reglamento (UE) 2017/679, lo que se deberá demostrar "entre otros medios, a través de mecanismos voluntarios de certificación que tendrán particularmente en cuenta la obtención de una titulación universitaria que acredite los conocimientos especializados en el derecho y la práctica en materia de protección de datos".

Por lo tanto, la pregunta acerca de si las universidades tanto públicas como privadas deben designar delegado de protección de datos personales debe responderse afirmativamente, y ambas podrán optar por que sea externo, pero ciertamente en las públicas, parece más simple y adecuado a la realidad que se trate de un órgano interno.

En efecto las Universidades públicas tienen en el Derecho español posterior a la Constitución española de 1978, la consideración de administraciones públicas prestadoras del servicio público de le enseñanza superior por lo que, conforme al artículo 37.1 a) del RGPD deben de contar con la figura del Delegado, que además les viene impuesta por su contemplación especifica en artículo 34 b) LOPDGDD como entidades obligadas a designar DPD en su calidad de "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"), y que en todo caso les vendría impuesta por el artículo 37. 1 b) del RGDP, por cuanto el tratamiento de datos a realizar en las universidades, tanto públicas como privadas requiere" una observación habitual y sistemática de interesados a gran escala".

Consecuentemente con lo anteriormente expuesto, habría que entender que la obligación de designar Delegado de Protección de datos habría nacido para las Universidades Públicas españolas desde la entrada en vigor del RGPDP, es decir, el pasado día 26 de mayo de 2018, no solo en virtud de la aplicabilidad directa de los Reglamento de la UE en todos sus Estados miembros, sino también porque el Reglamento (UE) 2016/679 previó una prolongada *vacatio legis* de año y medio con la finalidad de asegurar su inmediata aplicación, que se ha cumplido en otros estados miembros, pero no en España.

Lo cierto es que el flagrante retraso en que nos hemos situado, aunque estaría sancionado de acuerdo con el artículo 83.4 a) RGPD, con multas de hasta 10.000.000€ impuestas al responsable por la autoridad de control bajo la salvaguarda de los Tribunales, no es previsible que genere consecuencias sancionatorias tal y como se deduce de los matices que introduce el propio artículo 83 en su apartado 1.

Por su parte la LOPDGDD en su artículo 73 bajo la letra v) enumera entre las infraccione graves la consistente en "el incumplimiento de la obligación de designar Delegado de protección de datos cuando sea exigible su nombramiento de acuerdo con el artículo 37 del Reglamento (UE) 2016/679 y el artículo 34 de la Ley Orgánica".

El artículo 77.1 i) de la LOPDGDD somete a las Universidades públicas como responsables de infracciones, a un régimen especial que se contiene en el apartado 2 del mismo artículo, según el cual "la autoridad de protección de datos que resulte competente dictará resolución sancionando a las mismas con apercibimiento. La resolución establecerá asimismo las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido. El apartado 3 añade: "sin perjuicio de lo establecido en el apartado anterior, la autoridad de protección de datos propondrá también la iniciación de actuaciones disciplinarias cuando existan indicios suficientes para ello. En este caso el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación", lo que reconduce estas infracciones a un régimen disciplinario muy alejado del común que prevé el RGPD y que desarrolla la LOPDGDD.

3.1.Requisitos del Delegado de Protección de Datos.

El artículo 37.5 del RGDP establece que el DPD será designado "atendiendo a sus cualidades profesionales y, en particular a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones indicadas en el artículo 39".

La formación del DPD deberá ser acreditada por el organismo de control, para quienes hayan superado las pruebas establecidas al esquema formativo establecido por tal organismo, que en el caso de España.

El cumplimiento de los mencionados requisitos, a tenor del artículo 35 de la LOPDGDD, "podrá demostrarse entre otros medios, a través de mecanismos voluntarios de certificación que tendrán particularmente en cuenta la obtención de una titulación universitaria que acredite conocimientos especializados en el derecho y la práctica en materia de protección de datos".

La referencia a los mecanismos voluntarios de certificación remite de acuerdo con el artículo 42 RGPD a los aprobados por la autoridad de control, y en consecuencia al esquema formativo establecido por tal organismo.

No obstante, más allá de estas reglas generales, la complejidad y especificidad de la organización administrativa de las universidades públicas, podría hacer aconsejable a los efectos de asegurar los conocimientos especializados del derecho de que trata la normativa europea y la LOPDP, la prueba de cierto grado de conocimiento del derecho universitario y de la práctica universitaria de protección de datos.

3.2. Caracterización del DPD en las universidades públicas: su inserción en la estructura organizativa de la Universidad.

La regulación del DPD en el RGPD es bastante abierta, ya que como se indicó puede ser persona jurídica o persona física, y puede ser externo o estar integrado en la organización en el seno de la cual deberá velar por la protección de los datos personales.

Incluso, en los organismos públicos obligados a designar DPD, el artículo 37.3 del RGDPDP abre la posibilidad de que varios de esos organismos puedan "designar un único delegado de protección de datos para varias de esas autoridades u organismos, teniendo en cuenta su estructura organizativa y tamaño".

En el caso de las universidades públicas, ya se indicaron más arriba al inicio de este apartado las razones económicas que hacen preferible que se trate de un órgano interno, a las que habría que añadir ahora la razón jurídica del reconocimiento constitucional de la autonomía de las universidades (art. 27.10) y de su poder autoorganizativo reconocido en el artículo 2.2 a) de la Ley Orgánica 6/2001 de 21 de diciembre de Universidades.

En efecto, no cabe duda de que las Universidades en sus Estatutos podrán y deberán regular la figura del DPD, si tal vez no en cuanto a sus funciones esenciales que vienen prefiguradas por el artículo 39 del RGPD, si ciertamente en lo que atañe a su inserción en la estructura organizativa universitaria.

Siendo así, parece poco probable que se renuncie parcialmente a esa autonomía para aplicar el DPD compartido que posibilita el artículo 37.3 RGPD, ni a través de convenios interuniversitarios, ni a través de regulaciones estatales o autonómicas cuya compatibilidad con la constitucionalizada autonomía universitaria sería más que dudosa, por más que el tamaño y la homogeneidad de algunas universidades pudiese hacer factible compartir ese órgano.

En efecto, el carácter interno y exclusivo del DPD en las Universidades públicas implica que su designación debería de corresponder al máximo órgano colegiado, es decir, al Claustro Universitario. Y es que el artículo 38 del RGPD en su apartado 3 establece que "el responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos no reciba ninguna instrucción en lo que respecta al desempeño de dichas funciones. No será destituido ni sancionado por el responsable o el encargado por desempeñar sus funciones. El delegado de protección de datos rendirá cuentas directamente al más alto nivel jerárquico del responsable o encargado".

En fin, de la lectura de la LOU y especialmente de su artículo 16, parece deducirse que ese más alto nivel jerárquico en las Universidades públicas, es el Claustro, toda vez que el Rector es la más alta autoridad académica, aunque, por el momento, y a falta de otras disposiciones legales y estatutarias, el artículo 20.1 *in fine* de la LOU atribuye al Rector "cuantas competencias no sean expresamente atribuidas a otros órganos".

El artículo 38 del RGPD trata de garantizar en lo posible la más exquisita independencia del DPD en el ejercicio de sus funciones, lo que comporta que su rendición de cuentas[23] haya de ser ante el Claustro, ya que el Consejo de Gobierno tiene menor representatividad dada su procedimiento de designación, y el Consejo Social, aunque pudiera parecer en principio adecuado, por su parte acoge instancia sindicales y empresariales y administrativas externas.

[23] Alguna opinión pone en duda que se trate de una verdadera "rendición de cuentas", que sería contraria a la independencia del DPD, pero no parece un argumento muy atendible cuando se trata de un órgano colegiado y representativo como el Claustro Universitario, por más que se argumente sobre la versión inglesa del Reglamento, que utiliza el término *report* que podría apuntar a la simple exigencia de un informe anual de actividad, sin que tampoco esa interpretación sea muy aceptable, ya que según la jurisprudencia del TJUE hay que tener en cuenta todas las versiones a las lenguas oficiales de la UE a efectos de interpretación y *report en* inglés, y *faire rapport* en francés, también significan rendir cuentas. Ver B. DURÁN CARDO, *El Delegado de Protección de Datos en el RGPD y n la nueva LOPDGDD"*, La Ley Wolters-Kluwer, Madrid, 2019, págs. 677 a 72.

Por otra parte, la lógica aconseja que también su designación corra a cargo del órgano ante el que ha de rendir cuentas, por lo que es aconsejable una reforma de la LOU y de los estatutos de las Universidades públicas, que al igual que ocurrió con los defensores de universitarios o síndicos de quejas, pasen a contemplar esta figura que guarda cierta analogía con aquéllos.

Sin embargo, ese proceso puede sin duda prolongarse en el tiempo, de manera que, dada la urgencia de su designación, sólo puede llevarse a cabo, en tanto no haya reforma estatutaria, por el Rector en aplicación del artículo 20.1 *in fine* de la LOU, y habrá de regirse por un Reglamento aprobado por el Consejo de Gobierno que desarrolle los artículos 37 a 39 del RGPD, hasta que una reforma de Estatutos lo contemple. Tal reforma estatutaria, no tiene por qué ir precedida de reforma de la LOU necesariamente, puesto que es pura y simple aplicación de lo prescrito por el Derecho de la UE (RGPD) y por la LOPDGDD, establezca su designación por el Claustro y su rendición de cuentas anual ante el mismo órgano.

3.3.Funciones del Delegado de Protección de Datos Personales.

El Reglamento (UE) 2016/679 dedica su artículo 39 a enumerar las funciones que, como mínimo, deberá desempeñar el DPD, que concreta en su apartado 1 en las siguientes:

a) “Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros;
b) supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o encargado del tratamiento en materia de protección de datos personales, incluida la

asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;

c) ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 5;
d) cooperar con la autoridad de control;
e) actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa, a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto."

El desempeño de estas funciones por parte del DPD, deberá hacerse prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, y teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento, tal y como prescribe el artículo 9.2 del RGPD.

Como se desprende de esta regulación, la figura del DPD resulta clave para la adecuada aplicación de las normas incidentes sobre la protección de datos en las organizaciones que han de contar necesariamente con él, y un enlace imprescindible de estas con la autoridad de control, es decir en con la Agencia Española de Protección de Datos, o con las entidades autonómicas que asuman competencias en la materia, y buena prueba de ello es que los datos de contacto del DPD han pasado a ser parte importante de la información que debe proporcionarse a los interesados[24].

La LOPDGDD por su parte, en su artículo 36.1 *in fine* añade que "el delegado podrá inspeccionar los procedimientos relacionados con el objeto de la presente ley orgánica y emitir recomendaciones en el ámbito de sus competencias".

Para el ejercicio de todas sus funciones, incluidas en su caso la función inspectora y de emisión de recomendaciones, el apartado 3 del mismo artículo 36 de la LOPDGDD le concede "acceso a los datos personales y procesos de tratamiento, no pudiendo oponer a este acceso el responsable o el encargado del tratamiento, la existencia de cualquier deber

[24] Ver en tal sentido A. Fernández-Tresguerres García, *El derecho privado europeo en la transformación digital*, Discurso leído el día 10 de diciembre de 2018 en el acto de su recepción como Académica de Número, Real Academia de Jurisprudencia y Legislación, Madrid, 2018, pág. 226

de confidencialidad o secreto, incluyendo el (deber de confidencialidad) previsto en el artículo 5 de esta ley orgánica".

Del mismo modo, el apartado 4 del artículo 36 de la LOPDGDD, impone al delegado cuando "aprecie la existencia de una vulneración relevante en materia de protección de datos", el deber de documentarlo y comunicarlo inmediatamente a los órganos de administración y dirección del responsable o el encargado del tratamiento.

Todo lo cual viene a complementar la caracterización de la figura, y a justificar la relevancia institucional de que habrá de revestirse en las Universidades públicas

Por último, en los casos de reclamación, el afectado, facultativamente, podría dirigirse previamente a la presentación de su reclamación ante la autoridad de control competente, al delegado de protección de datos de la entidad contra la que se reclame, en los términos que establece el artículo 37 de la LOPDGDD. Esa petición obligará al DPD a comunicar al afectado la decisión que se adopte, en el plazo máximo de dos meses a contar desde la presentación de la reclamación, lo que viene a convertir al DPD en receptor de una especie de primera instancia en reclamaciones contra presuntas infracciones de las normas de protección de datos personales.

El DPD, es, también facultativamente, destinatario de las reclamaciones presentadas directamente ante la AEPD o las autoridades autonómicas de protección de datos, porque de acuerdo con el apartado 2 del artículo 37 de la LOPDGDD, ya aquéllas podrán remitir la reclamación al DPD para que responda en el plazo de un mes, prosiguiendo en caso de falta de respuesta del DPD en ese plazo, la tramitación de la reclamación la AEPD o las autoridades autonómicas competentes el procedimiento de acuerdo con los establecido en el Título VIII (arts. 63 a 68 de la LOPDGDD).

Así pues, el DPD puede resultar clave en los procesos iniciados por reclamación de algún afectado, lo que en el caso de las Universidades Públicas, le sitúa a efectos de protección de datos personales como instancia competente *prima facie* y extrae del ámbito de competencias del defensor del universitario esta materia, por lo que si la reclamación se presenta por el afectado ante el defensor del universitario, este deberá inhibirse y dar traslado de la reclamación al DPD con el que necesariamente debe contar la Universidad.

Queda así meridianamente claro, que la figura del DPD en las universidades públicas debe insertarse en el organigrama con el rango institucional antes indicado, y que la Universidad, como "responsable", en la nomenclatura legal, de la protección de los datos personales de los integrantes de amplios colectivos deberá atender al amplio haz de funciones que la normativa europea y española atribuyen al DPD.

4. La diversidad de los datos personales posible objeto de tratamiento en las Universidades.

Merece alguna breve consideración, en relación con la figura del DPD, el que, a los efectos de confeccionar el registro de actividades de tratamiento al que se refieren los artículos 30 del RGD y 31 de la LOPDGDD la actividad de las universidades comporta la existencia de los ficheros de datos automatizados propios de cualquier organización, como los relativos al personal que, en las universidades públicas es el llamado personal docente e investigador por una parte (PDI) y el personal de administración y servicios (PAS) por otra parte, existiendo en cada uno de ellos una parte de personal funcionario y otra parte de personal contratado, bien en régimen administrativo, bien en régimen aboral.

Otro aspecto importante en todas las universidades radica en los ficheros de los alumnos de los títulos cuya docencia imparten en ellas, sean titulaciones oficiales, o sean los llamados títulos propios, en los que en todo en todo caso el colectivo de alumnos resulta ser el más numeroso.

La confección y el mantenimiento de tales registros está legalmente atribuida a los responsables y encargados, que deben comunicar al DPD "cualquier adición, modificación o exclusión del contenido del Registro".

También el artículo 31.3 de la LOPDGDD obliga a los responsables y encargados en determinados casos que contempla el artículo 77.1 de la LOPDP, entre los cuales bajo la letra i) se contempla a las universidades públicas, a hacer público un inventario de sus actividades de tratamiento, accesible por medios electrónicos en el que habrá de constar la información establecida en el artículo 30 del RGDP[25].

[25] El citado artículo enumera: a) Nombre y datos del responsable, y en su caso, del corresponsable, del representante del responsable y del delegado de protección de datos. b) fines del tratamiento. c) Descripción de las categorías de interesados y de las categorías de datos personales. d)
categorías der destinatarios a quienes se comunicaron o comunicarán los datos personales incluidos los destinatarios en terceros países u organizaciones internacionales. e) en su caso, las transferencias a terceros países u organizaciones internacionales. f) cuando sea posible, los plazos previstos para la supresión de las

Por último, también es preciso tener en cuenta que en relación con la actividad investigadora del PDI de las universidades públicas, en determinadas áreas de conocimiento, puede surgir alguna actividad de tratamiento de datos personales, cuyo responsable no será ninguna de las universidades o institutos a que estén adscritos los profesores investigadores, sino más bien el Investigador Principal del Proyecto en que se lleve a cabo ese tratamiento masivo y automatizado de datos personales, o que vaya a ser objeto de publicación con la difusión de los resultados de la investigación. Esto ocurre en investigaciones muy diversas, como las de ciencias de la salud, las sociológicas, económicas, e incluso las jurídicas e históricas, en las que se emplee parcialmente metodología que implique manejo de datos personales. La información que las Universidades públicas poseen en virtud de sus actividades docentes e investigadoras, entra de lleno en esa posible reutilización que requiere una especial atención a los datos personales

La cuestión que puede plantearse es si tales responsables y encargados, que no tienen por qué contar con delegado de protección de datos personales, podrán recabar el auxilio de los DPD de sus respectivas universidades, cuestión ésta que parece merecer respuesta afirmativa pese a no estar legalmente prevista.

Recientemente se ha publicado la Directiva (UE) 2019/1024 del Parlamento Europeo y del Consejo de 20 de junio relativa a los datos abiertos y la reutilización de la información del sector público que incide como es obvio en el régimen de la protección de datos en las universidades públicas. En esta norma que habrá de trasponer a los ordenamientos jurídicos de los Estados miembros, la definición de datos personales es la contenida en el artículo 4 del Reglamento (UE)2016/679 al que se remite expresamente la Directiva, y se ven afectadas en una doble dirección, ya que por una parte son depositarias de

---

distintas categorías de datos. g) cuando sea posible, descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 2.1.

En su aparatado segundo continua el citado artículo con la siguiente enumeración: a) nombre y datos del representante del encargado y de cada responsable, por cuenta del cual actúa y en su caso, del representante del responsable o del encargado y del delegado de protección de datos. b) categorías de tratamientos de datos efectuados por cuenta de cada responsable. c) en su caso las transferencias de datos a terceros países u organizaciones internacionales. d) cuando sea posible, descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 301.

Tales registros, continua el precepto, constarán por escrito, incluso en formato electrónico. Además, el responsable, el encargado, y, en su caso, sus representantes pondrán el registro a disposición de la autoridad de control que lo solicite, aunque estas obligaciones no se aplican a ninguna empresa u organización que emplee menos de 250 personas.

documentos reutilizables, y por otra parte son sujetos activos de actividades investigadoras.

Desde el primer punto de vista, relativo a la actividad docente y de relaciones con terceros no estudiantes (proveedores, por ejemplo) el artículo 1.2 letra h) de la Directiva (UE)2019/1924, excluye de la obligación de proporcionar en abierto "los documentos cuyo acceso este excluido o limitado en virtud de regímenes de acceso por motivos de protección de datos personales, y las partes de documentos accesibles en virtud de dichos regímenes que contengan datos personales cuya reutilización se haya definido por ley como incompatible con la legislación relativa a la protección de las personas físicas con respecto al tratamiento de los datos personales o como un menoscabo de la protección de la intimidad y la integridad de las personas, en particular de conformidad con la legislación nacional o de la Unión europea sobre protección de datos personales".

Desde el segundo punto de vista relativo a la actividad investigadora, el artículo 10.1 de la Directiva (UE)2019/1024, establece que "Los Estados miembros apoyarán la disponibilidad de los datos de la investigación mediante políticas nacionales y actuaciones pertinentes destinadas a hacer que los datos de la investigación financiada públicamente sean plenamente accesibles ("políticas de acceso abierto") en aplicación del principio de apertura por defecto y de compatibilidad con los principios FAIR. En este contexto, deberán tenerse en cuenta las inquietudes relacionadas con los derechos de propiedad intelectual e industrial, la protección de datos personales y la confidencialidad, la seguridad y los intereses comerciales legítimos de conformidad con el principio "tan abiertos como sea posible, tan cerrados como sea necesario"".

Además, hay que tener en cuenta la exclusión contenida en el artículo 1.2 letra f) que afecta a los "documentos cuyo acceso esté limitado en virtud de regímenes de acceso de los Estados miembros, incluidos entre otros, aquellos casos en los que los ciudadanos o personas jurídicas tengan que demostrar un interés particular en obtener acceso a los documentos, como es el caso de los protocolos notariales o registros parroquiales a los que se acceda con finalidad investigadora.

III. Los Códigos de conducta y la resolución extrajudicial de conflictos.

La sección 5ª del Capítulo IV del Reglamento UE 2016/679 prevé la posible existencia de códigos de conducta que la LOPDGDD a su vez en su artículo 38.1 declara vinculantes para quienes se adhieran a los mismos, al tiempo que posibilita que tales Códigos permitan a los sujetos dotarse de mecanismos de resolución extrajudicial de conflictos[26].

Es pertinente, no obstante, preguntarse si esta posibilidad reviste interés en el caso de las universidades públicas y privadas, porque sin duda podría parecer redundante que entidades obligadas a disponer de DPD que aparece como un destinatario facultativo para los reclamantes, de cualquier reclamación en materia de protección de datos.

Pero lo cierto es que la resolución extrajudicial de conflictos puede ser otra pieza importante y conveniente, especialmente en el caso de las universidades públicas, cuyo sometimiento a la jurisdicción contencioso-administrativa ofrece a los reclamantes un cauce judicial tal vez poco apropiado y en todo caso a través procedimientos muy prolongados en el tiempo.

Ahora bien, la existencia de tales cauces extrajudiciales de resolución de conflictos está supeditada la concurrencia de los supuestos que enumera el artículo 38 LOPDGDD, es decir a que se incorporen a códigos de conducta, cuya existencia en este ámbito es una hipótesis lejana por el momento, al menos en las universidades públicas, y difícil de encajar con su sometimiento al procedimiento administrativo, de la mayor parte de sus relaciones internas y externas.

De modo que, por el momento, es precisamente el DPD, quien puede asumir un decisivo papel preventivo en ejercicio de su intervención facultativa para los reclamantes, en los procedimientos iniciados a instancias de tales reclamantes.

IV. Conclusiones sobre la excepción a la obligación de permitir la reutilización de la información del sector público que implique datos personales.

1. Criterios de admisión de la licitud de la publicación de datos personales: el consentimiento y el interés público

[26] Ver B. DURÄN CARDO, obra citada, págs. 443 y ss.

Llegado el momento de concluir, hay que comenzar por afirmar como punto de partida esa consideración que ha aflorado a lo largo de estas páginas que ha otorgado nuestra Constitución a la protección de los datos personales, y que como se ha puesto de relieve por algún autor[27], no es otra que dar carta de naturaleza la existencia de un nuevo derecho fundamental al control de los datos personales propios.

Como es lógico, no se puede predicar esta misma naturaleza de los datos de las personas fallecidas, cuya protección, de la que se ocupa también el RGPD, merece otras calificaciones.

Sentada esta premisa, parece que estamos ante un obstáculo formidable y difícil cuando no imposible de superar para la reutilización de materiales documentales o de otro tipo que tengan asociados esos datos personales.

Pero lo cierto es que la protección presenta algunas debilidades, provenientes de la propia noción de derecho en sentido subjetivo, que al entenderse como una facultad concedida al titular (*facultas agendi, agere licere*), éste puede ejercitar o no ejercitar a su arbitrio, de modo que la propia voluntad de la persona puede hacer lícitos tratamientos de esos datos por parte de terceros[28].

En consecuencia, la primera excepción al carácter absoluto de la protección de los datos personales, viene dada por la licitud que el consentimiento informado y prestado por persona capaz y de modo libre, expreso e inequívoco, atribuye a su tratamiento por terceros (arts. 6 y 7 LOPDGDD).

La LOPD, al igual que sus antecedentes, establece una edad especial para la prestación de ese consentimiento que se cifra en catorce años, al tiempo que guarda silencio sobre el consentimiento de los incapaces con capacidad modificada por resolución judicial firme, o carentes de capacidad de entender y querer sin modificación judicial de la capacidad y

[27] Ver A. OLLERO TASSARA, obras citadas en nota 1 *supra*,

[28] Aparece así una característica de la protección de los datos personales que asemeja este derecho fundamental al derecho a la intimidad personal y familiar, en el que de acuerdo con la L.O. 1/1982 de 5 de mayo, no habrá intromisión ilícita de los terceros si media consentimiento del interesado. En tal sentido, F. DE CASTRO afirmaba que "el término derecho subjetivo, salvado de su variedad de sentidos y utilizado como concepto técnico, no se le puede aplicar de modo general a los "llamados derechos de la personalidad". Ver "Los llamados derechos de la personalidad", ahora en *Estudios jurídicos del Profesor Federico de Castro"*, ed. Colegio de Registradores de la Propiedad y Mercantiles de España, tomo II, pág. 888.

consiguiente constitución de representación legal o sistemas alternativos de protección, por lo que habrá que estar a las reglas generales.

Surge en todo caso la duda de la eficacia de una protección de los datos personales sensible a la evolución de una regulación de la persona en la que retroceden permanentemente las llamadas incapacidades y nulidades de protección, ya que este retroceso puede ser deletéreo para los niveles de protección que se pretenden

. En efecto, la amenaza tecnológica que refleja el artículo 18.4 de la Constitución española, al prometer la limitación del uso de la informática, había sido prevista mucho tiempo atrás[29], en momentos de menor desarrollo tecnológico, y hoy cabe preguntarse si ese reto a los juristas está siendo adecuadamente respondido en el mundo digitalizado, o la excepción del consentimiento del interesado es una posición replegada, más que un adecuado baluarte defensivo, ya que la protección es indisponible únicamente en los datos personales especialmente protegidos del artículo 9.1 del Reglamento para cuyo tratamiento el consentimiento del afectado no tiene virtualidad habilitante.

En todo caso la cuestión afecta solo tangencialmente al tema que aquí nos ocupa, que es el relativo a los datos abiertos en las Universidades en las que se trata de datos por lo general de personas mayores de edad, a diferencia de lo ocurre con el interés general, que sería la segunda gran excepción al carácter absoluto de la protección de los datos personales, cuya definición está lejos de perfilarse por el momento, incluso respecto de los datos personales especialmente protegidos.

En efecto, la reciente sentencia del Tribunal Constitucional nº 76/2019 de 22 de mayo, al resolver el recurso de inconstitucionalidad presentado por el Defensor del Pueblo en que solicitaba la anulación de la Disposición final tercera apartado 2 de la Ley Orgánica

[29] Así el citado texto de F. DE CASTRO Y BRAVO sobre "Los llamados derechos de la personalidad", que fue una ponencia en el homenaje a Filippo Vassalli (fallecido en el año 1955), se terminaba por el autor con las siguientes consideraciones: "un compatriota nuestro, pues lo es mío y vuestro, Lucius Anneus Seneca, andaluz, *hispanus et romanus*, menciona los bienes sin los cuales, ciertamente, se puede vivir, pero sin los cuales es preferible la muerte (*sine quibus possumus vivere, sed mors potius est*). En este mundo moderno, lleno de maravillas técnicas, cunde ya el temor de que esos bienes *libertas, pudicitia, et mens bona* (*De benef.* I y II), y la *tranquillitas animi* están en peligro, y tan grave que se ha llegado a pensar seriamente si la persona puede sustituirse por el autómata humano. La expansión creciente de los poderes de la Administración que lleva a la masificación de la sociedad, la radio, la televisión, la prensa gráfica y sensacionalista, la cinta magnetofónica, los micrófonos, la interferencia en teléfonos, la telefotografía, etc., pueden fácilmente ser mal utilizadas y emplearse en daño de los valores personales.
He aquí una importante misión de los juristas…". Así pues, a mediados de los años cincuenta del pasado siglo era previsible la creciente amenaza a la que sale hoy al paso la LOPD 3/2018 de 5 de diciembre, e incluso lo que ha dado en llamarse el transhumanismo.

3/2018 de 5 de diciembre de Protección de Datos Personales y garantía de los derechos digitales, de la que ha sido Ponente Cándido Conde-Pumpido Tourón. Tal sentencia, pese a que se refiere a datos especialmente protegidos de los que contempla el artículo 9.1 de la LO 3/2018, dado que se trata de autorización a los Partidos Políticos para identificar la ideología de las personas llevando a cabo perfiles, lo que se justifica acudiendo al Considerando 56 del Reglamento 2017/679/UE que se refería a la permisión del tratamiento de las opiniones políticas personales con base en el interés público, no presta especial atención a este aspecto que era el primer fundamento de inconstitucionalidad que esgrimió el recurso del Defensor del Pueblo, al entender que la "genérica mención del interés público sin especificarlo no basta para fundamental la intromisión que en el derecho a la protección de datos de carácter personal implica el amparo que se otorga al tratamiento relativo a los datos relativos a opiniones políticas a favor de los partidos políticos".

En efecto, la fundamentación jurídica de la sentencia afirma que "el Reglamento General de Protección de datos no excluye de antemano que los Estados miembros puedan autorizar la recopilación de datos personales sobre las opiniones políticas en el marco de actividades electorales, si bien esa autorización está expresamente condicionada al establecimiento de "garantías adecuadas", como se desprende de su considerando 56".

Queda, así, sin respuesta expresa el primero de los motivos del recurso del Defensor del Pueblo, toda vez que la cuestión se remite a la existencia de "garantías adecuadas", todo con aplicación de un considerando de un Reglamento de la UE, es decir de un texto que está destinado a la interpretación en su caso del Reglamento, como los Preámbulos y Exposiciones de Motivos de nuestros textos legales, pero que en sí mismo no es una norma jurídica de directa aplicación en el Reino de España.

La cuestión ha perdido relevancia, ya que la STC 76/2019 declara la nulidad de la norma legal recurrida por absoluta falta de concreción de las "garantías adecuadas", con infracción de la reserva de ley existente, pero lo cierto es que para enjuiciar en su caso "las garantías adecuadas" que consagre una ley, será necesario calibrar si el tratamiento de datos personales especialmente protegidos que se permite está materialmente amparado por ese "interés público" en que se fundamenta la excepción al carácter absoluto de la protección, aspecto éste que debería haber puesto de relieve la sentencia, ya que la sentencia parece darlo por supuesto en ulteriores intervenciones del Legislador.

En efecto el interés público debe estar pormenorizadamente referido en la norma legal a todos los supuestos de tratamiento de ese dato personal especialmente protegido, porque de lo contrario, no será tampoco posible valorar la existencia de "garantías adecuadas" en la futura norma legal sobre esta materia.

Tal vez, la voluntad de dar pronta respuesta (se ha resuelto en el inusual plazo de dos meses) al recurso del Defensor del Pueblo contra la Ley Orgánica 3/2018, explique esta notoria insuficiencia de la fundamentación de la sentencia del TC 76/2019, pero desde luego no la justifica.

2. Le efectividad de la protección de los datos personales ante las exigencias de transparencia y de datos abiertos.

Como ha podido comprobarse la indisponibilidad de los datos personales constantes en la documentación obrante en las Universidades o embebidos en los datos utilizados en las tareas de investigación, es la regla general, que impone un cuidadoso proceder a responsables y encargados de su tratamiento.

La LOPDGDD 3/2018 de 5 de diciembre en su Disposición Final Undécima ha modificado el artículo 15 de la Ley de Transparencia, acceso a la información pública y buen gobierno 19/2013 de 9 de diciembre que permite el acceso a los datos personales no especialmente protegidos previa ponderación de forma "suficientemente razonada del interés público en la divulgación de la información y los derechos de los afectados cuyos datos aparezcan en la información solicitada y en particular su derecho fundamental a la protección de datos de carácter personal", para lo que proporciona una serie de criterios a tomar, entre otros posibles en consideración: a) El menor perjuicio de los afectados derivado del transcurso de los plazos establecidos en el artículo 57 de la Ley 16/1985, de 25 de junio del Patrimonio Histórico español. b) La justificación por los solicitantes de su petición en el ejercicio de un derecho o el hecho de que tengan la condición de investigadores y motiven el acceso en fines históricos, científicos o estadísticos". c) El menor perjuicio de los derechos de los afectados en caso de los documentos únicamente contuviesen datos identificativos de aquéllos. d) La mayor garantía de los derechos de los afectados en el caso de que los datos pudieran afectar a su intimidad o seguridad, o se refieran amenores de edad.

Los datos personales especialmente protegidos sólo se pueden divulgar previo consentimiento por escrito, o estuviese amparado por una norma con rango de ley.

En conclusión, puede afirmarse que "transparencia y protección de datos no son realidades radicalmente opuesta ni mucho menos excluyentes; su problemática reside en las dificultades para delimitar el correcto equilibrio entre transparencia y protección de datos"[30], afirmación especialmente aplicable a las Universidades Públicas, en las que están depositados numerosos datos personales, de los sólo pueden considerarse en principio excluidos de divulgación sin consentimiento expreso los datos especialmente protegidos, lo que implica una especial vigilancia preventiva de posibles conculcaciones del derecho fundamental que nos ocupa.

En lo que podría calificarse como tarea preventiva de violaciones de este derecho fundamental, resultará clave la figura del Delegado de Protección de Datos cuyas funciones de información y asesoramiento a responsables y encargados, así como de supervisión del cumplimiento de las mencionadas obligaciones, y asesoramiento sobre evaluación de impacto relativa a la protección de datos establece el artículo 39.1 del RGDPD en sus apartados a), b) y c).

También compete al DPD la cooperación con la autoridad de control, y la actuación como punto de contacto de tal autoridad de control de conformidad con lo previsto en las letras d), y e) del mismo precepto, incluidas las tareas de consulta previa.

Para ello puede el DPD inspeccionar los procedimientos relacionados con la protección de datos personales, y emitir en su caso recomendaciones.

Pero no se agota su función en esta faceta preventiva, sino que se extiende a los casos en que se hayan producido violaciones del derecho protegido sobre los datos personales, puesto que el que reclame frente a una violación de la protección de sus datos personales, puede hacerlo facultativamente, de acuerdo con el artículo 37.1 de la LOPDGDD, directamente ante el DPD que habrá de resolver en plazo de dos meses, y aunque lo haga directamente ente el organismo de control (AEPD u órganos de las CC.AA.) estos podrán facultativamente remitir la reclamación al DPD, quien habrá de resolver en tal caso en el plazo de un mes, lo que excluye esta materia de las competencias del defensor

[30] Ver D. TERRÓN Santos y J.L. DOMINGUEZ ALVAREZ, *Nueva regulación de la protección de datos*, ed. Comares, Granada, 2019, pág. 227.

universitario tanto en caso de reclamación directa ante el DPD, como en caso de remisión a éste por parte del organismo de control estatal o bien de la comunidad autónoma.

Hay, por lo tanto, una vía de defensa frente a posibles vulneraciones de la normativa de protección de datos, mediante los procedimientos regulados en el Título VIII de la LOPDGDD (art. 63 a 69 y futuras normas de desarrollo), que se inician a instancia de parte en los casos de falta de atención de una solicitud de ejercicio de los derechos establecidos en los artículos 15 a 22 del RGPD que ha de resolverse en el plazo de seis meses, y que en los casos de posible vulneración de las normas tanto se inicia a instancia de parte como si se inicia de oficio, habrá de resolverse el plazo de nueve meses contados desde el acuerdo de inicio del procedimiento.

3. Tutela judicial efectiva.

En todo caso, el RGPD dedica sus artículos 77 a 82 a los recursos y la responsabilidad, dejando a salvo en el artículo 78 el derecho a la tutela judicial efectiva contra una autoridad de control en los siguientes términos: "1. Sin perjuicio de cualquier otro recurso administrativo o extrajudicial, toda persona física o jurídica tendrá derecho a la tutela judicial efectiva contra una decisión jurídica vinculante de una autoridad de control que le concierna".

Como se puede deducir se trata no sólo de la defensa de las personas físicas titulares de los datos, sino también de las personas jurídicas que resulten afectadas por actos de las autoridades de control, y ello "sin perjuicio de cualquier otro recurso administrativo o extrajudicial" (art. 78.2 RGPD), así como en los casos en que no se dé curso a una reclamación "o no se informe al (reclamante) interesado en plazo de tres meses".

Las acciones contra una autoridad de control "deberán ejercitarse ante los Tribunales del Estado miembro en que esté establecida la autoridad de control" (art. 78.3 RGPD), lo que conduce sin duda a la jurisdicción contencioso administrativa[31], aunque no excluye la jurisdicción civil.

[31] Los interesados que denuncian y dan lugar a un procedimiento sancionador, estableció el TS en sentencia 531/2018 de 20 de febrero de 2018, carecen de legitimación activa para combatir la resolución de la autoridad de control que decide archivar el procedimiento sancionador.

Por otra parte, solo los interesados (personas físicas), disfrutarán de tutela judicial efectiva, "sin perjuicio de los recursos administrativos o extrajudiciales disponibles", tendrán "derecho a tutela judicial efectiva cuando considere que sus derechos en virtud del presente reglamento han sido vulnerados como consecuencia de un tratamiento de sus datos personales" (art. 79.1 RGPD).

Las acciones, en tal caso, habrán de ejercitarse ante los Tribunales del Estado en el que el responsable o encargado tenga un establecimiento" (art. 79.2 RGPD)[32].

4. Datos abiertos.

Por último, respecto la futura regulación de datos abiertos en transposición de la Directiva UE 2019/1924, serán de aplicación las reglas generales que ofrecen suficiente salvaguarda de los datos personales, por los distintos cauces y procedimientos hasta aquí estudiados, que viene a constituirse en una excepción de importancia a la obligación de autorizar la reutilización de la información del sector público.

5. Cauces y procedimientos de aplicación de la protección de los datos personales.

El Reglamento General y la LOPDGDD el pasado año 2018, ofrecieron un esquema de aplicación que viene siendo ya usual en las materias de derecho público y privado reguladas por la UE, toda vez que contienen un vigoroso derecho sancionador, de aplicación por los órganos de control, al que acompaña como garantía de la tutela judicial efectiva, el sistema de recursos contencioso-administrativos de cada Estado miembro.

En segundo lugar, se contempla la coexistencia de Códigos de conducta de adhesión voluntaria, y la posibilidad de establecer mecanismos de resolución de conflictos alternativos a la jurisdicción, cuyo desarrollo e implantación se hará esperar algún tiempo, y por último, como es lógico, la tutela judicial efectiva mediante acciones civiles de resarcimiento de daños frente a responsables, corresponsables y encargados de la protección de datos, a ejercitar ante los órganos jurisdiccionales del Estado en que el responsable o encargado tenga establecimiento, lo que ofrece al interesado una

[32] Ver E. TORRALBA MENDIOLA, "Los litigios civiles en materia de protección de datos: criterios de competencia judicial internacional", *GA_P*, 29-09-2018, artículo de análisis en el que la autora aprecia una cierta contradicción entre este precepto del Reglamento y el Reglamento Bruselas 1, y se inclina por la inconveniencia de su aplicación conjunta y la conveniencia de aplicar el art. 79.2 del RGPD.

amplia panoplia en el momento presente, y hace previsible su incremento en lo sucesivo.

6. Desarrollos legislativos previsibles.

A la fecha de cierre de este trabajo se ha conocido la existencia de un grupo de trabajo constituido en la Unión Europea para formular propuestas legislativas relativas a fortalecer la protección de los datos biométricos frente las amenazas que posibilita la combinación de las técnicas de identificación facial con la inteligencia artificial a este aspecto de la protección de datos personales incluido entre los llamados datos biométricos.

Se trata de una iniciativa todavía en unja fase muy incipiente de la que se han hecho eco diversos medios de comunicación tras la aparición de una información en una revista británica[33], que podría desembocar en alguna modificación de la actual regulación tendente a mantener el control de las personas sobre este dato personal especialmente protegido y relacionado estrechamente con la intimidad personal, frente al tratamiento de imágenes obtenidas en espacios públicos o privados, por empresas o administraciones públicas.

Se trata por lo tanto de buscar medios que permitan asegurar el consentimiento informado y verificable de las personas físicas para su identificación automática mediante inteligencia artificial o técnicas similares.

En consecuencia, parece que es posible alguna iniciativa legislativa al respecto, ya que ha surgido alguna aplicación del Reglamento General de Protección de datos en Estados miembros (Suecia[34]) sobre la utilización de tales técnicas de identificación en escuelas, cuyo potencial resulta cada vez más inquietante para los derechos fundamentales que nos ocupan, aunque en todo caso se desconoce la existencia de recomendaciones concretas a formular por el grupo de trabajo mencionado para

[33] Se trata de reportaje datado por MEHREEN KHAN en Bruselas a 22 de agosto de 2019 bajo el título "EU plans sweeping regulation of facial recognition", aparecido en *Financial Times* de la indicada fecha.
[34] Se trata de una primera sanción de 18.760 Coronas impuesta por la Agencia de Protección de Datos de Suecia a una escuela que confiaba el control de asistencia diaria de los alumnos a la técnica del reconocimiento facial, por vulnerar el derecho a la privacidad de los estudiantes mediante una cámara de videovigilancia.

permitir que las personas físicas tengan los derechos que el RGPD les reconoce sobre sus datos personales.

Abreviaturas:

AEPD: Agencia Estatal de Protección de Datos

DPD: Delegado de Protección de Datos

LOPD: Ley Orgánica de Protección de Datos 15/1999 de 13 de diciembre.

LOPDGDD: Ley Orgánica de Protección de Datos Personales y Gestión de los Derechos Digitales, 3/2018 de 5 de diciembre.

LOU: Ley Orgánica de Universidades 6/2001 de 21 de diciembre.

PAS: Personal de Administración y Servicios.

PDI: Personal Docente e Investigador.

RGPD: Reglamento General de Protección de Datos (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016.