RETOS Y DESAFÍOS EN LA PROTECCIÓN DE DATOS PERSONALES QUE REVELAN LAS CONVICCIONES RELIGIOSAS. PROPUESTAS EN UN NUEVO MARCO JURÍDICO

José Daniel Pelayo Olmedo
UNED

Resumen: En la actualidad la protección de los datos personales es un derecho en auge. La realidad en la que vivimos y el incremento de la capacidad informática para procesar información hace que nos cuestionemos hasta qué punto y cómo podemos proteger nuestra intimidad. Por otra parte, el uso e intercambio de información se está revelando como una de las piezas clave para facilitar la gestión de la diversidad religiosa, por un lado, y como instrumento imprescindible para combatir los casos de inseguridad donde se ha mezclado la violencia con el fundamentalismo y la radicalización. A pesar que desde los inicios de su consagración jurídica la mayoría de las normas internacionales y nacionales previeron la existencia de un régimen de protección reforzado para los datos sensibles, entre los que se encuentran los datos que revelan las creencias personales, de que la doctrina lo ha reivindicado y la jurisprudencia ha tenido que resolver casos específicos lo cierto es que hasta el momento su desarrollo ha sido meramente anecdótico. La promulgación de un nuevo régimen jurídico para las entidades religiosas en España, encabezado por el RD 594/2015, su referencia a la recogida y tratamiento de datos personales de sujetos vinculados con ellas, sumado a la adaptación del marco europeo sobre protección de datos con la aprobación del Reglamento General de Protección de Datos han impulsado la necesidad de abordar esta cuestión. En este trabajo, el autor presenta los motivos por los que se hace imprescindible la existencia de una normativa específica sobre esta cuestión y, al no existir un desarrollo específico salvo la remisión formal a la normativa general, ofrece un estudio actualizado del régimen general permitirían extraer y diseñar los criterios específicos para regular el uso y cesión de datos sensibles relativos a las creencias religiosas. Todo ello le permite ofrecer, en su último apartado, una propuesta sobre la regulación y las acciones que deberían desarrollarse en España.

Palabras clave: derecho a la protección de datos, datos que revelan las creencias personales, datos sensibles, elaboración de perfiles, intercambio de información, gestión de la diversidad religiosa.

Abstract: The right to personal data protection has reached a new height. Our social reality, increasingly digitalised, and the rise of computing capability to process information (personal data) make us question to what extent and how we can protect our privacy. Data revealing personal beliefs is a special category of personal data, which, by their nature, may cause a risk to data subjects when processed and needs enhanced protection. Data processing can provide better religious diversity management practices but also information exchange is revealing itself as an essential mechanism to prevent, prosecute, etc. cross borders incidents where violence and terrorism are merged with religious fundamentalism and radicalization. On the other hand, these operational practices also bring legal challenges (profiling, discrimination practices, private life damage, etc.). The question is can we balance all these benefits and risks with suitable protection of personal data, mainly for the special categories of personal data? Although most of the international and national legal standards on data protection foresaw the existence of enhanced protection for sensitive data, the scientific literature also has supported its importance and Spanish courts had to attend to specific cases, the fact is Spanish legal framework only have available an incidental development. A new legal framework brings us new opportunities. Throughout this paper, the author aims to present an updated study of the EU and national legal frame in order to extract and come up specific criteria to rule the processing of sensitive data. This will make possible to design and present his own proposal on the legal policies and the actions that in his opinion should be established in Spain.

Keywords: data protection right, data revealing personal beliefs, sensitive data, profiling, information exchange, religious diversity management.

originario europeo como punto de partida. 2.3.2 Las novedades introducidas por el nuevo Reglamento General de Protección de Datos y la Directiva 680/2016. 2.4 Elementos jurídicos propios para diseñar un sistema de protección de los datos religiosos extraíbles del desarrollo legislativo español. 3. 3 Reflexiones para construir un marco jurídico adecuado para el uso de datos personales en la gestión de la diversidad religiosa. 4. A modo de propuesta.

1. LA CRECIENTE IMPORTANCIA DEL DERECHO A LA PROTECCIÓN DE DATOS Y SU NECESARIA ATENCIÓN JURÍDICA

No hay duda de que gran parte de nuestra actividad diaria se encuentra notablemente imbuida en el uso de las nuevas tecnologías. Todo ha variado, desde la forma de relacionarnos (redes sociales, aplicaciones telefónicas de comunicación, etc.) hasta las herramientas con las que desarrollamos nuestra actividad profesional (e-mail, plataformas digitales, etc.). El ser humano actúa en un entorno cada vez más digitalizado que facilita y ofrece mejores oportunidades para participar en cualquier proceso ordinario pero que, a nivel jurídico, requiere prestar especial atención a los términos en los que estos procedimientos se desarrollan, a los requisitos en los que se concretan los protocolos de seguridad implantados para evitar fraudes y/o proteger los distintos intereses en juego y a los posibles efectos que todo ello pueda tener sobre la preservación de nuestra intimidad[1]. Y es que diariamente facilitamos información personal y generamos una cantidad ingente de datos disponibles, fundamentalmente, a través de internet que son tratados por distintas entidades, públicas y privadas[2]. La mayor parte de

[1] «El legislador ha sido consciente de la tremenda importancia de la información en su formato digital. El uso de las tecnologías de la información en los diferentes sectores de la actividad económica y social configura un nuevo orden que debe ser protegido por Ley», Cfr. MARTÍN SÁNCHEZ, María del Mar, «Tecnología informática y confidencialidad de los datos personales» en VV. AA. (Álvarez-Cienfuegos, J. M.ª –Dir.–) *La protección del derecho a la intimidad de las personas (fichero de datos)*, Consejo General del Poder Judicial, Madrid, 1997, pp. 153 a 193, *Vid.* p. 154. «(…) la difusión de las NT y las TIC en las sociedades actuales es un fenómeno ambivalente. En su reverso, plantea riesgos para las libertades que exigen renovadas formas de tutela procesal; pero, en su anverso, aportan nuevos mecanismos que refuerzan la operatividad de la documentación y la gestión judiciales y, por consiguiente, representan un aumento de la eficacia de las instancias procesales que garantizan los derechos humanos», Cfr. PÉREZ-LUÑO ROBLEDO, Enrique Cesar, «Las nuevas tecnologías y la garantía procesal de las libertades», *Revista de Derecho UNED*, n.º 11, 2012, pp. 1007 a 1020, *Vid.* p. 1018

[2] «Se estima que cada día se crean 2.5 Exabytes (2.5 × 1018 bytes) de datos, equivalente a 200 millones de DVDs de 5 Gb (IBM, 2013) y son añadidos a la ya enorme cantidad de "big data" disponible principalmente a través de internet. Estos datos pueden variar desde instantáneas de las

estos datos –nombre completo, número de identificación habitual, e-mail, código postal, etc.– se utilizan como requisitos de acceso o bien como información necesaria para habilitar un sistema de identificación y registro seguro. Es así como, en la mayor parte de las ocasiones, su utilidad es percibida por el sujeto concernido como una pieza clave para garantizar su propia seguridad y, por ello, el usuario no duda en consentir su uso. Sin embargo, la capacidad de procesamiento casi ilimitada que conlleva la nueva tecnología y esa aparente voluntariedad del sujeto concernido no exime de contar con los mecanismos y previsiones de control necesarias, especialmente por las implicaciones que la transmisión/cesión voluntaria o involuntaria de esos datos pudiera tener sobre los derechos de las personas. Y no solo eso, sino que, junto con ese potencial riesgo de vulnerabilidad sobre la persona y sus derechos, nuestra propia actividad en la red –participar en plataformas comerciales, resolver encuestas de calidad de servicios, usar aplicaciones para compartir opiniones y gustos o, incluso, nuestros propios hábitos de navegación– puede generar datos que, procesados, llegan a ser utilizados como fuente de información de nuestros (supuestos) intereses. De este forma, además de por su valor en el contexto comercial (mercadotecnia), debemos considerar que la información se puede utilizar para generar *perfiles personales* de comportamiento[3], con el consiguiente riesgo no solo de sufrir una injerencia sobre nuestra intimidad, teniendo acceso a datos personales, si no de generar situaciones discriminatorias basadas en decisiones tomadas de forma automatizada sobre esos perfiles de comportamiento que son utilizados para decidir el tratamiento que recibiremos en distintos ámbitos de nuestra vida ordinaria. Es por ello que, dentro de los retos que supone la intervención de las nuevas tecnologías sobre el ejercicio de los derechos humanos, la necesidad de contar con un sistema adecuado de protección de nuestra propia intimidad y, específicamente, del uso de nuestros datos personales ocupa una posición relevante.

---

vacaciones del Sr. y la Sra. Jones de Londres y los tweets diarios de su hija de 16 años Elsie hasta el conjunto de datos comerciales de Google y Experian, el conjunto de datos recogidos por el sector público, como los datos censales, mapas topográficos y de altitud o elevación», *Vid.* VAN LOENEN, Bastiaan; KULK, Stefan & PLOEGER, Hendrik, «Data protection legislation: A very hungry Caterpillar. The case of mapping data in the European Union», *Government Information Quarterly* 33 (2016) 338-345, *Vid.* p. 338 –la traducción es del autor–.

[3] «En el mundo de la vigilancia líquida cada uno de nuestros comentarios, acciones o intereses es susceptible de pasar a engrosar alguno de los muchos centros de datos personales que los Estados y las entidades privadas poseen y que en numerosas ocasiones constituyen su activo y objeto de negocio principal», Cfr. GARRIGA DOMÍNGUEZ, Ana, «La elaboración de perfiles y su impacto en los derechos fundamentales. Una primera aproximación a su regulación en el Reglamento General de Protección de Datos de la Unión Europea», *Derecho y Libertades*, n.º 38, 2018, pp. 107 a 139, *Vid.* p. 108. En el mismo sentido *Vid.* DIORIO, Samantha, «Data protection Laws: quilts versus blankets», *Syracuse Journal of International Law and Commerce*; Spring 2015, 42, 2, pp. 486 a 513, *Vid.* p. 500.

Consciente de esta situación, pero más aún de lo retos que supone el rápido avance de la tecnología y el incremento de los peligros y desventajas que acechan en el uso y transmisión de nuestros propios datos a través de las nuevas tecnologías, la Unión Europea ha renovado su marco normativo a través 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* (en adelante RGPD)[4]. Con esta normativa se ha tratado de unificar el régimen jurídico de protección de datos en un sistema común para todos los Estados miembros que, hasta el momento, estaba caracterizado por la existencia de una diversidad de normas nacionales[5] y un cierto margen de armonización asentado por la ahora derogada Directiva 95/46/EC. El nuevo modelo de protección instaurado por la UE se contiene en un Reglamento que, como tal, resulta directamente aplicable en los Estados miembros, reduce la fragmentación legal[6] y lo (re)configura teniendo en cuenta el crecimiento exponencial de la capacidad informática para procesar nuestros datos[7], sin olvidar el impacto y beneficio económico, político, social, etc. que, como el propio título sugiere, tiene la garantía de una libre circulación de estos datos en el contexto europeo. En definitiva, con esta nueva regulación se trata de adaptar la tradicional formulación y alcance del derecho de protección de datos a un contexto más acorde con la realidad actual, donde las posibilidades se incrementan, los riesgos aumentan y la volatilidad propia de las innovaciones tecnológicas es una característica que acompaña al constructo del derecho[8].

---

[4] Diario Oficial de la Unión Europea, L. 119/1, de 4 de mayo de 2016. Pero, sobre todo, el nuevo RGPD, ha sido considerado como una oportunidad para establecer un estándar mínimo y homogéneo de protección en todos los países europeos. *Vid.* Fernández Villazón, Luis Antonio, «El nuevo Reglamento Europeo de Protección de Datos», *Foro, Nueva época,* vol. 19, n.º 1 (2016), pp. 395 a 411; Rebollo Delgado, Lucrecio; Serrano Pérez, M.ª Mercedes, *Manual de Protección de datos*, 2.ª edición, Dykinson, Madrid, 2017, pp. 53 a 58; De Miguel Asensio, Pedro Alberto, «Competencia y derecho aplicable en el Reglamento General sobre Protección de Datos de la Unión Europea», *REDI*, Vol. 69/1, 2017, pp. 75 a 108.

[5] Como señala De Miguel Asensio el RGPD está llamado a sustituir las legislaciones nacionales, salvo en aquellos aspectos que el propio Reglamento «(…) prevé que sus normas pueden ser especificadas o restringidas por los Estados miembros, (…)», Cfr. De Miguel Asensio, Pedro Alberto, «Competencia y derecho aplicable …», *op. cit.*, *Vid.* p. 77.

[6] Reding, Viviane, «The European data protection framework for the twenty-first century», *International Data Privacy Law*, 2012, Vol. 2, n.º 3, pp. 119 a 129, *Vid.* p. 121.

[7] Rebollo Delgado, Lucrecio; Serrano Pérez, M.ª Mercedes, *Manual de Protección de datos*, *op. cit.*, *Vid.* p. 37.

[8] «Si una de las notas distintivas de los sistemas jurídicos actuales es la de su acelerada e incesante mutación, este rasgo se hace manifiesto con especial intensidad en un sector como el de las relaciones entre la Informática y el Derecho, en el que, constantemente, cada Feria tecnológica abre nuevas proyecciones informáticas al Derecho, o innova bienes informáticos que requieren nuevos

Esta necesidad de modulación y atención a las circunstancias cambiantes se plasmó, mejor que en ningún otro sitio, en la evolución seguida por la configuración definitiva de este derecho. No en vano, su contenido transitó desde el mero establecimiento de un *principio de no injerencia*, más propio del derecho a la intimidad, hasta la concreción de su actual contenido, *derecho de acceso y control de los datos personales*, integrado por un *haz de facultades de disposición* que van incrementándose incluso con las necesidades que surgen de la realidad práctica, por ejemplo la inclusión del más reciente y específico derecho al olvido[9]. Nos situamos, por lo tanto, ante un derecho que reivindica su propia virtualidad y relevancia, que a su vez está conectado al ritmo en que se producen los avances tecnológicos, pero que lo hace sin desprenderse de su carácter instrumental en el ejercicio de los demás derechos de la persona[10]. Un *derecho autónomo*[11], sí, pero no aislado, ya que como el resto de derechos fundamentales permanece anclado en el respeto a nuestra dignidad[12], al libre desarrollo de nuestra personalidad y a los demás derechos de la persona, donde, sin duda, cobra especial relevancia el derecho a ser respetado en nuestra intimidad (personal o familiar) y a la privacidad.

Esta conexión ente intimidad, identidad y protección de datos provocará que, no en pocas ocasiones, corramos el riesgo de que la información que se esté manejando incida directamente sobre aspectos realmente sensibles del nú-

---

procedimientos de tutela jurídica, o da a conocer dispositivos que condenan al anacronismo los medios de protección jurídica anteriormente existentes», Cfr. PEREZ LUÑO, Antonio Enrique, «La tutela de la libertad informática en la sociedad globalizada», *Isegoría*, n.º 22, 2000. pp. 59 a 68, *Vid.* p. 63

[9] Sobre el que el Tribunal Europeo se ha pronunció en el conocido Caso C-131/12, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos. Sobre la misma ÁLVAREZ CARO, María, «Reflexiones sobre la sentencia del TJUE en el asunto «Mario Costeja» (C-131/12) sobre derecho al olvido», *Revista Española de Derecho Europeo*, n.º 51, 2014, pp. 165 a 187; ARENAS RAMIRO, Mónica, «Unforgettable: a propósito de la STJUE de 13 de mayo de 2014. Caso Costeja (Google vs AEPD), *Teoría y realidad constitucional*, n.º 34, 2014, pp. 537 a 558; MARTÍNEZ OTERO, Juan María, «El derecho al olvido en Internet: debates cerrados y cuestiones abiertas tras la STJUE Google vs AEPD y Mario Costeja», *Revista de Derecho Político*, n.º 93, 2015, pp. 103 a 142; MINERO ALEJANDRE, Gemma, «A vueltas con el «derecho al olvido». Construcción normativa y jurisprudencial del derecho de protección de datos de carácter personal en el entorno digital», *Revista jurídica Universidad Autónoma de Madrid*, n.º 30, 2014, pp. 129 a 155.

[10] FERNÁNDEZ VILLAZÓN, Luis Antonio, «El nuevo Reglamento Europeo …», *op. cit.*, *Vid.* p. 395-396.

[11] STC 292/2000 FJ. 6.º, *Vid.* ARENAS RAMIRO, Mónica *El derecho fundamental a la protección de datos personales en Europa*, Tirant lo Blanch, Valencia, 2006, p. 445; FUENTETAJA PASTOR, Jesús, MEDINA GONZÁLEZ, Sara, *La protección de datos en la Administración local*, *Iustel*, Madrid, 2008, pp. 19 a 21; PLANAS ARNALDOS, M.ª Carmen, «El derecho fundamental a la protección de datos personales y los ficheros privados: el interés legítimo en el tratamiento de datos», *Comunitania. Revista Internacional de Trabajo Social y Ciencias Sociales*, n.º 7, enero 2014, pp. 69 a 89, *Vid.* p. 70.

[12] DIORIO, S., «Data protection Laws: …», *op. cit.*, *Vid.* p. 498.

cleo esencial de su persona, a su identidad y personalidad, o podrá ser el germen de posibles actitudes discriminatorias, basadas en decisiones adoptadas a consecuencia del tratamiento de datos que revelan las convicciones ideológicas y religiosas, entre otras características – raza, sexo, ideología, etc.–. Para evitar estos casos, el legislador ha optado tradicionalmente por incrementar el nivel de protección jurídica que se dispensa a aquellos datos considerados sensibles por estar vinculados más directamente con la identidad e integridad física (datos relativos al origen, etnia, a la salud, genéticos y biométricos) y la integridad moral y/o espiritual de la persona (ideología, orientación política, religión…)[13]. De esta forma, la mayoría de las regulaciones especificarán las condiciones para configurar un sistema de garantías cualificado para los datos considerados sensibles, dentro de un régimen ya de por sí fuertemente guarnecido con medidas de protección, y realzarán el grado responsabilidad que asume quien recoge, transmite y/o cede los datos[14].

En esta especialidad y régimen cualificado es donde se sitúa el principal objeto de nuestro trabajo: el tratamiento de los datos religiosos o que revelan la adscripción religiosa del individuo. Por ello, nuestro estudio se centrará en determinar cuál es la conexión entre ambos derechos y los nuevos retos que se plantean y en extraer los términos aplicables a la protección de estos datos, teniendo en cuenta las novedades que en esta materia se han promulgado en Europa y, específicamente, en España.

2. LA NECESIDAD DE CONCRETAR UN SISTEMA DE PROTECCIÓN DE DATOS PERSONALES QUE REVELAN LAS CREENCIAS RELIGIOSAS

A pesar de su relativa novedad y de la enorme especificidad que le confiere su vinculación con la libertad ideológica y religiosa, la preocupación por el sistema de garantía de los datos que revelan las convicciones personales no debe ser, en nuestra opinión, una cuestión residual. Varias razones nos llevan a sostener esta afirmación.

---

[13] Llamazares Fernández, Dionisio, *Derecho de libertad de conciencia II. Conciencia, identidad personal y solidaridad,* Civitas, Cizur la menor, Navarra, 2011, p. 27.

[14] Como responsables del tratamiento, en el sentido expresado por el artículo 4 del RGPD: «cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción».

Primero, desde una perspectiva general debemos partir del hecho antes esbozado de que el propio derecho de protección de datos se encuentra conectado al pleno ejercicio de los demás derechos de la persona. Desde sus orígenes, como tendremos la oportunidad de conocer más adelante, la garantía del derecho de protección de datos tiene un *carácter instrumental* respecto a otros derechos, extendiendo su alcance a aquellos supuestos en los que otros derechos, especialmente los vinculados con la personalidad del individuo, puedan verse afectados por el uso e intercambio de información (datos) personal. En el caso de la libertad ideológica y religiosa, la Agencia Española de Protección de Datos (en adelante AEPD) ha tenido que pronunciarse, desde hace ya algún un tiempo, sobre dudas que surgían en torno al régimen aplicable a la recogida, procesamiento y difusión de datos que incidían (o podrían incidir) sobre la condición religiosa de las personas. Esta Agencia tuvo que tratar, en sus informes jurídicos, conceptos como la propia consideración de datos religiosos, la naturaleza de archivos y registros de las comunidades religiosas[15] y otras cuestiones donde la libertad religiosa se conjugaban con la necesaria protección de datos personales. Pero donde más nítidamente se detecta esta interacción entre libertad ideológica y religiosa y el derecho de protección de datos fue cuando la AEPD tuvo que pronunciarse sobre casos en los que debía medirse las consecuencias que pudiera tener el tratamiento de cierta información vinculada el ejercicio de la libertad religiosa, como la elección de la enseñanza religiosa en los colegios públicos[16] y privados concertados[17] o del destino de la asignación tributaria en un impuesto personal[18], etc.[19], sobre el grado de revelación de sus creencias y la injerencia en su derecho a proteger esos datos. Pero además, como ya señalara el profesor Rallo Lombarte, el derecho de protección de datos se encuentra en *plena vis expansiva*[20], por lo que podemos constatar que está

[15] Informe jurídico 0000-2000; Informe jurídico 486/2005; Informe jurídico 0296/2008 y 0381/2008.

[16] Informe AEPD de 28 de febrero de 2003.

[17] Informe AEPD 0501/2005.

[18] Informe AEPD de 24 de enero de 2001, donde lo consideraba un dato que revelaba la adscripción ideológica o religiosa del individuo y, a posteriori, el Informe AEPD 158/2008 donde rectifica su opinión anterior y considera que ese dato no debe ser considerado sensible.

[19] Sobre estas cuestiones *Vid.* CANO RUIZ, Isabel, *Los datos religiosos en el marco del tratamiento jurídico de los datos de carácter personal*, Comares, Granada, 2011, pp. 105 a 11, ROCA, M.ª José, *La declaración de la propia religión o creencias en el Derecho español*, USC, Santiago de Compostela, 1992, *Vid.* p. 259; RODRÍGUEZ GARCÍA, José Antonio, «La protección de los datos personales y las confesiones religiosas», *Laicidad y Libertades. Escritos jurídicos*, n.º 7, 2007, pp. 354 a 356.

[20] RALLO LOMBARTE, Artemi, «La protección de datos en España. Análisis de la actualidad», *Anuario de la Facultad de Derecho*, Universidad de Alcalá, II, 2009, pp. 15 a 30, *Vid.* p. 16.

aumentando el número de supuestos en los que se produce la interacción con otros derechos fundamentales del individuo. No hay que descartar, por lo tanto, que los nuevos retos a los que se tenga que enfrentar la libertad ideológica y religiosa tengan relación directa con el tratamiento de datos personales asociados, en muchas ocasiones, por la aplicación de nuevas tecnologías en el procesamiento de información y más en el ámbito de la gestión y administración de la diversidad religiosa.

En segundo lugar, desde la perspectiva específica de la ciencia del Derecho eclesiástico del Estado, un importante sector de la doctrina viene apuntando la necesidad de atender a esta cuestión, especialmente cuando se planteaban el análisis de casos relacionados con el ejercicio del derecho de libertad religiosa en materia de abandono de la religión profesada, donde conocer el régimen de protección de datos era un elemento crítico para comprender los argumentos y el resultado alcanzado en importantes pronunciamientos jurisprudenciales[21]. En todo caso, su atención residual hasta el momento no está exenta de una cierta lógica, pues esta cuestión ha pasado tradicionalmente desapercibida para el legislador y el gestor público. Desde que se promulgó la *Ley Orgánica de Libertad Religiosa* de 1980 (en adelante LOLR) y los consiguientes decretos de desarrollo para concretar el régimen aplicable a determinadas cuestiones de tipo más funcional (Registro de entidades religiosas, Comisión Asesora de Libertad Religiosa, etc…) el establecimiento de medidas para garantizar el tratamiento de los datos religiosos como datos personales sensibles no ha formado parte de ninguna agenda pública de reforma, actualización, etc. de la legislación sobre el tratamiento de la diversidad religiosa en España, por lo menos en lo que se refiere a la legislación unilateral del Estado. Por su parte, en los

[21] Siendo los más importantes SAN 4728/2007, STS 383/2011y STS 7583/2011. En este caso nos referimos a la polémica suscitada a raíz de la pervivencia de datos en los libros bautismales que fue resuelta por el TS. Sobre esta cuestión pueden verse importantes trabajos. Sin ánimo de ser exhaustivos, pueden ahora citarse por su especial vinculación directa con el objeto señalado (la doctrina del TS): Arenas Ramiro, Mónica, «Protección de datos personales y apostasía: la sentencia del Tribunal Supremo de 19 de septiembre de 2008», en *Anuario de Derecho Eclesiástico del Estado*, vol. XXVI. (2010), pp. 684 a 702. Cano Ruiz, Isabel, *Los datos religioso …, op. cit., Vid.* p. 115 y ss; González Moreno, Beatriz, «Apostasía y protección de datos. Comentario a la Sentencia del Tribunal Supremo de 19 de septiembre de 2008», *Anuario de la Facultad de Derecho de Ourense*, n.º 1, 2008, pp. 227 a 246. Lopéz-Sidro Lopez, Ángel, «La apostasía como ejercicio de la libertad religiosa: Iglesia católica e Islam», en *Anuario de Derecho eclesiástico del Estado*, vol. XXIII (2007), pp. 177 a 210. Otaduy, Juan, «Iglesia católica y Ley española de protección de datos: falsos conflictos», *Ius Canonicum*, n.º 95, 2008, pp. 117 a 140. Pelayo Olmedo, José Daniel, «La adscripción religiosa como dato especialmente protegido. El caso del registro bautismal en España», *Revista de Derecho Político*, n.º 94, 2015, pp. 143 a 182; Rodríguez García, José Antonio, «La protección de los datos personales y…», *op. cit.*

Acuerdos de cooperación con las comunidades religiosas tan solo podemos encontrar algunas referencias a cuestiones tangenciales, como la inviolabilidad de los archivos y registros eclesiásticos, que sí han sido objeto de análisis cuando se ha tratado de resolver cuestiones vinculadas con el tratamiento de datos personales[22].

Sea como fuere, en nuestra opinión parece que el número de cuestiones vinculadas con el tratamiento de datos religiosos de los individuos seguirá creciendo, aunque solo sea como consecuencia de la aplicación de las nuevas tecnologías en los sistemas de gestión, almacenamiento y transmisión de datos de los órganos administrativos de gestión pública, tal y como se prevé en el nuevo RD 594/2015[23], o, de forma más genérica, a la misma implantación de la administración electrónica e, incluso, en la actividad jurisdiccional, como consecuencia de la extensión del uso de las TICs[24]. Pero sobre todo consideramos que en el futuro próximo será necesario reflexionar sobre dos aspectos en los que esta cuestión tendrá un gran transcendencia. Una más vinculada con la labor de gestión de la diversidad religiosa encomendada a los poderes públicos y otra a su labor de prevención y control en el ejercicio de los derechos fundamentales y, en concreto, de la libertad religiosa[25]. Nos explicaremos.

El punto de inflexión respecto a la *labor de gestión* se produce con la modificación del régimen jurídico de las entidades religiosas en España a consecuencia de la reciente publicación y entrada en vigor de dos Reales Decretos,

---

[22] ROCA FERNÁNDEZ, M.ª José «Interpretación del término 'inviolabilidad' en el Acuerdo entre el Estado español y la Santa Sede, sobre Asuntos Jurídicos, de 3-I-1979», *Revista General de Derecho Canónico y Derecho Eclesiástico del Estado* 29 (2012), pp. 1 a 14, *Vid.* pp. 7 a 13. Para profundizar sobre los archivos eclesiásticos *Vid.* ALDANONDO SALAVERRIA, Isabel, «Aspectos jurídicos de los archivos eclesiásticos», en VV. AA. *Dimensiones jurídicas del factor religioso: estudios en homenaje al profesor López Alarcón,* Universidad de Murcia, Murcia, 1987, pp. 19 a 52.

[23] *Vid.* Disposición adicional tercera. Gestión electrónica de los procedimientos administrativos y depósito de documentación.

«*En el plazo de dos años, desde la entrada en vigor de este real decreto, se habilitarán los recursos necesarios para la gestión electrónica de los procedimientos administrativos regulados. En tanto se completan los procesos necesarios para la presentación en formato y con firma electrónicos de la documentación que ha de acompañar a las solicitudes dirigidas al Registro, se presentarán en formato no electrónico.*

El Registro de Entidades Religiosas sustituirá la conservación material de documentación por su almacenamiento mediante medios electrónicos, dotados de garantías suficientes, conforme a lo dispuesto en la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos».

[24] PÉREZ-LUÑO ROBLEDO, Enrique Cesar, «Las nuevas tecnologías y…», *op. cit.*, *Vid.* pp. 1015 a 117.

[25] *Vid.* PELAYO OLMEDO, José Daniel, *Una nueva regulación del Registro de Entidades Religiosas. Entre el control y la gestión de la libertad en el tratamiento de la diversidad religiosa*, Tirant lo Blanch, 2017, *Vid.* pp. 152 y ss.

uno sobre la declaración de notorio arraigo[26] y otro sobre el Registro de entidades religiosas[27]. Sin duda no se nos escapa que el objeto principal de ambas

[26] Sobre el nuevo Real Decreto y sus características *Vid.* García García, Ricardo, «Real Decreto 593/2015, de 3 de julio, por el que se regula la declaración de notorio arraigo de las confesiones religiosas en España [*BOE* n.º 183, de 1-VIII-2015]. Declaración de notorio arraigo de las confesiones religiosas en España», en *Ars Iuris Salmanticensis*, Vol. 4, junio 2016, pp. 256-250; Suárez Pertierra, Gustavo, «La libertad ideológica, religiosa y de culto. Los principios informadores del Derecho eclesiástico del Estado», en VV. AA. *Derecho eclesiástico del Estado*, 2.º ed., Tirant lo Blanch, Valencia, 2016, pp. 119 a 137; Torres Gutiérrez, Alejandro, «Los retos del principio de Laicidad en España: una reflexión crítica a la luz de los preceptos constitucionales», *Anuario de Derecho Eclesiástico del Estado*, Vol. XXXII, 2016, pp. 663 a 722, *Vid.* especialmente p. 671. Para conocer la evolución del concepto de notorio arraigo y sus distintas implicaciones *Vid.* Fernández-Coronado, Ana, «Consideraciones sobre una interpretación amplia del concepto de notorio arraigo», *Laicidad y Libertades. Escritos jurídicos*, n.º 0, 2000, pp. 285 a 302; Fernández-Coronado, Ana, «Notorio arraigo de la Federación de Comunidades Budistas de España (Consideraciones jurídicas sobre la evolución del concepto de notorio arraigo)», *BANDUE*, n.º III, 2009, pp. 137 a 154.

[27] Para un comentario sobre la nueva regulación del Registro de entidades religiosas *Vid.* Alenda Salinas, Manuel, «Repercusión de la doctrina, científica y jurisprudencial, en la nueva regulación reglamentaria del registro de entidades religiosas», *Anuario de derecho eclesiástico del Estado*, n.º 32, 2016, pp. 1209-1248; García García, Ricardo, «Real Decreto 594/2015, de 3 de julio, por el que se regula el Registro de Entidades Religiosas [*BOE* n.º 183, de 1-VIII-2015]», *Ars Iuris Salmanticensis*, Vol. 4, junio 2016, pp. 261 a 265; Pelayo Olmedo, José Daniel, *Una nueva regulación del… op. cit.* Sobre el Registro de entidades religiosas y su función en el ámbito jurídico español de protección de la libertad religiosa puede consultarse un amplio elenco de aportaciones científicas publicadas por la doctrina eclesiásticista, entre otros: Aldanondo Salaverria, Isabel, «El Registro de Entidades Religiosas», *Anuario de Derecho Eclesiástico del Estado*, n.º 7, 1991, pp. 13 a 48; Alenda Salinas, Manuel, *El Registro de Entidades Religiosas. La praxis administrativa tras la STC 46/2001*, IUSTEL, Madrid, 2009; Camarero Suárez, M.ª Victoria, *Las confesiones religiosas y su inscripción en el registro de entidades religiosas*, Low Cost Books, Valencia 2016; Contreras Mazarío, José María, «Las confesiones religiosas y el registro de entidades religiosas», *Estudios jurídicos*, n.º 2010, 2010; Fernández-Coronado, Ana, «Reflexiones en torno a la función del Registro de Entidades Religiosas. (A propósito de la Sentencia de la Audiencia Nacional de 11 de octubre de 2007 sobre inscripción de la Iglesia de la Scientology)», *Revista Laicidad y Libertades. Escritos jurídicos*, no 7, 2007, pp. 389 a 402; Herrera Ceballos, Enrique «Hacia la construcción de un Registro el reflejo de la realidad. La reforma del Registro de Entidades Religiosas», *Revista General de Derecho Canónico y Derecho eclesiástico del Estado*, n.º 39 (2015), pp. 1 a 34; Herrera Ceballos, Enrique, *El Registro de Entidades Religiosas. Estudio global y sistemático*, EUNSA, Pamplona, 2012; IBÁN, Iván Carlos; Prieto Sanchis, Luís, Motilla, Agustín, *Manual de Derecho Eclesiástico*, Trotta, Madrid, 2016; López-Alarcón, Mariano, «La función calificadora en el Registro de Entidades Religiosas», *Anuario de Derecho eclesiástico del Estado*, n.º 14, 1998, pp. 433 a 462; Llamazares Calzadilla, M.ª Cruz, «Personalidad jurídica de las confesiones religiosas y concepto de religión. Estudio comparado de cinco ordenamientos: España, Alemania, Italia, Francia y Estados Unidos», *Boletín de la Sociedad de Ciencias de las Religiones*, n.º 14, 2000, pp. 7 a 27; Llamazares Fernández, Dionisio, «Derecho de libertad de conciencia II. Conciencia, identidad personal y solidaridad», Thomson Reuters, Madrid, 2011; Mantecón Sancho, Joaquín Mariano, «Confesiones religiosas y Registro» en VV. AA. *Libertad religiosa a los veinte años de su Ley Orgánica*, Ministerio de Justicia, Madrid, 1999, pp. 79 a 166; Motilla de la Calle, Agustín; «El reconocimiento estatal de las entidades religiosas. El Registro de Entidades Religiosas», en VV. AA. (Andrés Corsino Álvarez Cortina; Miguel Rodríguez Blanco, coord.) *La libertad religiosa en España: XXV años de vigencia*

disposiciones es el esclarecimiento de la *dimensión institucional* de la libertad religiosa, algo que *per se* quedaría fuera del ámbito del derecho a la protección de datos, pues está reservado a las personas físicas[28]. Pero también es cierto que, como consecuencia de las medidas adoptadas para disponer de la mayor información posible de la realidad estructural y orgánica de la entidad religiosa, o de su implantación en el territorio español, se ha incluido entre sus disposiciones la posibilidad de asociar datos personales con el expediente registral de la comunidad religiosa añadiendo, unas veces con carácter potestativo y otras reglamentario, los datos personales de sujetos vinculados con ellas desde una perspectiva funcional. Nos referimos a las disposiciones en las que se habilita la recogida de datos de personas vinculadas con la entidad, que van desde los *titulares de los órganos de representación* hasta los *ministros de culto,* pasando por aquellos individuos que voluntariamente quieren dejar constancia de su aval a la constitución y establecimiento de la entidad religiosa en España. La necesidad de desarrollar una interpretación conforme a la protección de datos se hizo patente desde la propia gestación del proyecto, cuando se solicitó informe a la AEPD sobre ello[29], facilitando en él importantes reflexiones y recomendaciones que se tuvieron en cuenta a la hora de elaborar el Real Decreto[30].

En cuanto a la segunda, más vinculada con la *labor de prevención y control* público para evitar la lesión de los derechos fundamentales y la comisión de actos delictivos, la protección de datos se conecta con la necesidad y cada vez

de la Ley Orgánica 7/1980, de 5 de julio (Comentarios a su articulado), Comares, Granada, 2006, pp. 145 a 176; MURILLO MUÑOZ, Mercedes, «El Registro de Entidades Religiosas», Observatorio del pluralismo religioso en España, 2013, http://www.observatorioreligion.es/upload/27/94/GuiaRER.pdf OLMOS ORTEGA, M.ª Elena «Personalidad jurídica civil de las entidades religiosas y Registro de Entidades Religiosas», *Revista General de Derecho Canónico y Derecho Eclesiástico del Estado*, n.º 19, 2009, pp. 1 a 43; PELAYO OLMEDO, José Daniel, *Las comunidades ideológicas y religiosas, la personalidad jurídica y la actividad registral*, Ministerio de Justicia, Secretaria General Técnica, 2007; POLO SABAU, José Ramón., *El estatuto de las confesiones religiosas en el derecho de la Unión Europea: entre el Universalismo y la peculiaridad nacional*, Dykinson, Madrid, 2014; RODRÍGUEZ BLANCO, Miguel, «Libertad religiosa y Registro de Entidades Religiosas», *Revista Española de Derecho Constitucional*, Año 23, n.º 68, 2003, pp. 337-354; SOUTO GALVÁN, Beatriz, *El reconocimiento estatal de las entidades religiosas*, Servicio de Publicaciones UCM, Madrid, 2000; VEGA GUTIÉRREZ, Ana, «El Registro de entidades religiosas y la promoción de la libertad religiosa colectiva (A propósito de la STC 46/2001, de 5 de febrero)», *Repertorio Aranzadi del Tribunal Constitucional*, n.º 3, 2001, pp. 1861-1908.

[28] Que queda fielmente reflejado en el art. 1 del RGPD, al delimitar el sujeto de aplicación en las personas físicas.

[29] De hecho, tuvo que informar tanto en los dos proyectos de reforma previos como el que finalmente dio lugar al actual reglamento, *Vid.* Informe jurídico 0363-2014.

[30] «En la elaboración de este real decreto se ha tenido en cuenta el informe del Pleno de la Comisión Asesora de Libertad Religiosa emitido en su reunión de 26 de noviembre de 2014 y el informe de la Agencia Española de Protección de Datos de 18 de marzo de 2015», *Vid.* preámbulo del RD 594/2015.

mayor utilidad del uso, tratamiento e intercambio de información en la lucha contra la radicalización y el terrorismo vinculado a circunstancias religiosas. Nos referimos a aquellos datos que son recogidos y tratados a través de sistemas diseñados para garantizar la seguridad y prevención de los delitos. En la mayor parte de las ocasiones, los procesos de cooperación entre las fuerzas y cuerpos de seguridad tiene como eje fundamental el manejo de esa información vinculada con datos personales. Por ejemplo, en su proyecto de informe de 2018 la *Comisión Especial sobre Terrorismo* del Parlamento Europeo ponía el acento sobre la retención de datos como parte esencial del proceso de investigación y, por ello, recordaban « (…) *que las autoridades policiales y judiciales suelen depender en gran medida de los datos de las comunicaciones para proceder con* éxito *con sus casos»* por lo que « (…) *para que la interoperabilidad de los sistemas de información alcance todo su potencial, es fundamental que existan regímenes de retención de datos armonizados en toda la Unión* (…)»[31]. Es así como en sus recomendaciones solicita a los Estados que diseñen y activen un conjunto de medidas basadas en el tratamiento de la información e insta a la Comisión para que presente una propuesta legislativa que armonice los 28 regímenes jurídicos diferentes para la retención de datos[32].

En todo caso, las limitaciones propias de esta aportación y la imposibilidad de jerarquizar la importancia de ambas cuestiones, nos obliga a relegar esta segunda cuestión, relativa a la seguridad, a un estudio específico que será publicado en otro marco y, en este caso, nos centraremos en tratar de dar respuesta a las cuestiones que surgen como consecuencia del incremento de acceso y cesión de información personal relativa a las personas que participan, de un modo u otro, en la estructura de una comunidad religiosa.

2.1 **Tratamiento jurídico actual del uso y recogida de datos personales para la gestión de la diversidad religiosa**

Entre las múltiples e importantes novedades que incluye la modificación legislativa operada por el RD 594/2015 destacamos un aspecto aparentemente sencillo, pero cuya importancia no se le escapa al propio Real Decreto. Nos

[31] *Vid.* Párrafo AL. del *Proyecto de Informe sobre las conclusiones y recomendaciones de la Comisión Especial sobre Terrorismo* (2018/2044(INI)), Ponentes: Hohlmeier, M.; Stevens, H., (en adelante Proyecto de Informe de la Comisión TERR) disponible en: http://www.europarl.europa.eu/sides/getDoc.do?type=COMPARL&reference=PE-621.073&format=PDF&language=ES&secondRef=01 (última visita 5 de noviembre de 2018).

[32] *Vid.* recomendación 37 del *Proyecto de informe de la Comisión TERR* (última visita 5 de noviembre de 2018).

referimos a la atención que presta en sus disposiciones a las condiciones en que ha de desenvolverse el tratamiento de datos personales relativos a un grupo de personas concretas que mantienen una relación específica con la comunidad religiosa que está o va a ser inscrita. En concreto, el Real Decreto prevé la posibilidad de que puedan incorporarse al expediente registral de la entidad los datos de: a) *personas que decidan avalar* el establecimiento o fundación de la entidad religiosa en España; b) los *titulares de los órganos de representación* y c) los *ministros de culto*.

Los trazos fundamentales que el Real Decreto dibuja sobre el régimen aplicable a estos datos se sitúan en dos disposiciones específicas: a) la Disposición adicional segunda del RD 594/2015, que se desarrolla bajo el título de «protección de datos de carácter personal»; b) el art. 30, que se refiere a «la publicidad del Registro». En la primera de ellas, la DA 2.ª, el legislador sostiene que toda actividad que sea llevada a cabo en materia de gestión y tratamiento de los datos contenidos en el Registro de entidades religiosas, sea de archivo, almacenamiento, difusión o intercambio, habrá de desarrollarse necesariamente de conformidad con lo dispuesto por la legislación española sobre protección de datos[33]. Pero esta disposición no solo actúa como enlace o remisión al marco jurídico general del derecho a la protección de datos sino que, además de este valor esencial, introduce una previsión específica sobre como desarrollar el procedimiento de acceso y recogida de los datos. Nos referimos a la solicitud de hacer constar en los formularios de inscripción o anotación, de forma expresa, el consentimiento de los *solicitantes* y de los *titulares de los órganos de representación* para incluir sus datos personales en el Registro que, a consecuencia de su función de instrumento para dotar de la necesaria publicidad, debemos tener en cuenta que podrían ser objeto de transmisión. Y aún más, ese consentimiento previsto para la generalidad de los casos quedará reforzado por la condición de ser *expreso* y *por escrito* cuando los datos que se manejen (colecten, traten, etc.) sean aquellos que revelan la condición de *ministro de culto* de la persona concernida.

Por su parte, el artículo 30 se refiere a la necesidad de proteger los datos recabados al regular expresamente «la publicidad del registro», un proceso que, conviene recordar, está más vinculado con la transmisión, cesión y difusión de los datos que con la mera recogida o almacenamiento. Aquí, el legislador detecta dos circunstancias en la que se requerirá adoptar medidas para generar una especial protección frente a su potencial difusión: primero, cuando alguien

[33] Haciendo mención expresa a la por aquel entonces aún vigente *Ley orgánica 15/1999, de Protección de Datos*.

quiere acceder/consultar los datos que obran en él y segundo cuando se concrete y dé traslado de esa información en las copias o certificaciones mediante las que, según el propio Real Decreto, se ha de efectuar la publicidad formal propia de este Registro.

Para entender las cautelas del primer momento, debemos tener en cuenta que el registro es público y, por ello, los ciudadanos tienen reconocido el derecho de acceder al mismo[34]. Este derecho de acceso, sin más cautelas, podría tener como consecuencia la revelación de los datos personales de aquellas personas que hubieran sido inscritas en el expediente de la comunidad religiosa al mantener una determinada vinculación con la entidad. Grosso modo, la principal garantía que mantiene el Real Decreto es la imposibilidad de presentar una solicitud de consulta genérica, lo que impide un acceso directo, abierto, libre e indiscriminado a todos los datos en él contenidos. Y en todo caso, según sostiene la propia norma, cuando se produzca la solicitud de consulta genérica solo se admitirá para su consideración con carácter potestativo por el responsable del Registro, que deberá adoptar una decisión ajustada «(…) a la normativa sobre protección de datos de carácter personal»[35]. En segundo lugar, el legislador tiene en cuenta la forma en que se produce la transmisión de la información, para ello protege las condiciones en las que se emitirán los documentos que contienen esos datos: certificaciones y/o copias de los contenidos de los asientos. En ambos casos, el legislador recuerda que deberán ajustarse a «(…) los requisitos establecidos en materia de protección de datos de carácter personal»[36], con la adición de una garantía específica: «(…) se hará constar a los destinatarios la prohibición de crear ficheros con la finalidad exclusiva de almacenar datos de carácter personal que revelen la religión o creencias, en los términos previstos en el artículo 7.4 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal»[37].

Esta forma de atender a la cuestión nos permite extraer dos cuestiones previas:

— la primera, que el RD 594/2015 se remite a las condiciones generales establecidas en el régimen de protección de datos aplicables en España, sin profundizar en un desarrollo más específico. Esto nos conduce a la necesidad de conocer el régimen de protección de datos y de ahí extraer los criterios que

[34] *Vid.* art. 30.1 RD 594/2015.
[35] *Vid.* art. 30.3 del RD 594/2015.
[36] *Vid.* art. 30.4 del RD 594/2015.
[37] *Vid.* art. 30.5 del RD 594/2015.

nos permitirán completar el contenido que habrá de tener y presentar las correspondientes propuestas de regulación;

— la segunda, cuando se detiene a especificar condiciones en que dichos datos deberán ser tratados, lo hace más desde la perspectiva de su posible transmisión que desde la propia recogida o almacenamiento. No en vano, las referencias que el Reglamento hace de esta cuestión se sitúan fundamentalmente en su Título IV, cuando trata sobre «la publicidad del Registro de entidades religiosas»[38]. Esto supone la necesidad de incrementar la protección cuando se trata de la cesión de datos.

En definitiva, para extraer criterios de interpretación válidos, para cubrir los vacíos y necesidades y aportar sugerencias que, desde nuestra perspectiva, permitirían construir las bases de un régimen aplicable por la Subdirección General para garantizar el derecho a la protección de datos de estas personas que sea acorde con el marco legislativo aplicable en España resulta imprescindible conocer los requisitos, procedimientos y mecanismos implantados en el marco normativo general del derecho a la protección de datos y, específicamente, las novedades prevista por el nuevo Reglamento adoptado en la UE y la legislación española.

2.2 **Elementos jurídicos generales extraíbles de la configuración básica del derecho a la protección de datos para diseñar un sistema de protección de los datos religiosos**

A pesar de que la doctrina no se pusiera de acuerdo sobre la necesidad de incluir un párrafo específico en el texto constitucional para salvaguardar la intimidad de la persona frente al impacto de la informática[39], el constituyente finalmente dedicó el párrafo 4.º del artículo 18 CE a sentar las bases sobre las que se construiría el sistema de garantía del *derecho a la protección de datos*. La *libertad informática*, como la denominó el propio Tribunal Constitucional en España[40], desplegaba inicialmente su ámbito de protección sobre una imprescindible *dimensión negativa*, que otorgaba a la persona concernida el derecho a no

[38] «El título IV contempla la «Publicidad del Registro de Entidades Religiosas» incorporando tanto el uso de las nuevas tecnologías y los medios electrónicos como las exigencias derivadas de la normativa sobre protección de datos de carácter personal y de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno», *Vid.* preámbulo del RD 594/2015.

[39] *Vid.* DE LA LLANA VICENTE, Mariano, «La protección de datos personales automatizados: distintos aspectos», *BFD: Boletín de la Facultad de Derecho*, n 14 (1999), pp. 381 a 410, *Vid.* p. 383

[40] Expresión que es utilizada en España por el Tribunal Constitucional en la STC 254/1993.

sufrir injerencias en su intimidad personal a través de los medios informáticos. Poco a poco, el objeto de protección se fue determinando hasta incluir en su contenido esencial una *dimensión positiva* que lo traslada a su consideración como *un derecho autónomo*, que no solo protege la intimidad/privacidad de la persona, sino que incluye en su contenido el *derecho de acceso y control de los datos personales*, *habeas data*[41] y lo perfila centrándose en permitir tan solo su tratamiento para *la finalidad para los que son recabados y* evitar, a su vez, que *sean utilizados para fines distintos de aquel que justificó su obtención*[42]. Se trata de una evolución en el fundamento de la protección y tutela que, como puso de manifiesto el profesor Pérez Luño, conlleva el rediseño de su alcance, inicialmente circunscrita a un factor estático, asegurar la *calidad* de los datos, para ser completada por un factor dinámico, su *uso* o *funcionalidad*[43].

Para comprender y analizar el alcance y sentido del precepto constitucional debemos atender, en nuestra opinión, a tres cuestiones esenciales:

Primero, en toda interpretación que hagamos del derecho a la protección de datos debemos tener en cuenta la tradición jurídica desarrollada por la comunidad internacional y, especialmente, la desarrollada en el ámbito europeo, tal y como sucede respecto a otros derechos fundamentales consagrados en la Constitución española. No es nuestra intención realizar una exposición detallada de todos los documentos jurídicos que con mayor o menor intensidad han influido en su configuración internacional, pues excedería con creces los objetivos formales y materiales de este estudio. Si bien, teniendo en cuenta los documentos sobre los que más ha incidido la doctrina que se ha encargado de

---

[41] *Vid.* STC 254/1993, FJ. 7.º y STC 290/2000, FJ 7.ª Sobre el *habeas data Vid.* Pérez Luño, Antonio Enrique, «Del habeas corpus al habeas data», *Informática y derecho: Revista iberoamericana de derecho informático*, 1 (1992), pp. 153 a 161, *Vid.* p.158. Pérez-Luño Robledo, Enrique César, «Las nuevas tecnologías y …», *op. cit.*, *Vid.* pp. 1008 y 1009.

[42] «(…). La garantía de la vida privada de la persona y de su reputación poseen hoy una dimensión positiva que excede el ámbito propio del derecho fundamental a la intimidad (art. 18.1 CE), y que se traduce en un derecho de control sobre los datos relativos a la propia persona. La llamada «libertad informática» es así derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención (SSTC 11/1998, FJ 5, 94/1998, FJ 4)», STC 292/200, FJ 5.º

[43] Perez Luño, Enrique Cesar, «La tutela de la libertad informática en la sociedad globalizada», *Isegoría*, n.º 22, 2000. pp. 59 a 68, *Vid.* p. 65. En otro estudio también aclara que «El habeas data constituye un cauce procesal para salvaguardar la libertad de la persona en la esfera informática, que cumple una función paralela, en el seno de los derechos humanos de la tercera generación, a los que la primera generación correspondió al habeas corpus respecto de la libertad física o de movimientos de la persona», *Vid.* Pérez Luño, Antonio Enrique, «El concepto de interesado en la Directiva Comunitaria 95/46» en VV. AA. (Álvarez-Cienfuegos, J. M.ª –Dir.–) *La protección del derecho a la intimidad de las personas (fichero de datos)*, Consejo General del Poder Judicial, 1997, pp. 15 a 37, *Vid.* p. 23.

analizar este derecho y, sobre todo, atendiendo a nuestro objetivo principal, poner de manifiesto la evolución y aportaciones que ofrece la nueva regulación propuesta por la UE para poder aplicarlo al desarrollo del contenido indeterminado en el que se pronuncia el RD 594/2015, tomaremos como referencia aquellos documentos jurídicos que en nuestra opinión son más significativos.

Así, con independencia de que no debemos olvidar que en la comunidad internacional podemos encontrarnos con otras disposiciones, resoluciones y/o documentos jurídicos que nos sitúen ante el sustrato del marco de protección de este derecho[44], es decir la intimidad o privacidad de la persona, el artículo 8 del *Convenio Europeo de Derechos Humanos* (en adelante CEDH)[45] es el primer documento que nos interesa recuperar para conocer su proceso de concreción. El primer párrafo del art. 8 del CEDH garantiza el *derecho de toda persona a que su vida privada y familiar, su domicilio y su correspondencia sean* respetados. En este precepto, más que establecer un *derecho autónomo* de protección de datos, se configura una garantía general referida a la intimidad y privacidad de la persona, las raíces de las que con posterioridad nacerá este derecho. En su segundo párrafo, el precepto del Convenio recuerda a las autoridades públicas la prohibición de *intervenir de ninguna forma en el ejercicio de este derecho*, salvo en aquellos casos en que esté expresamente *previsto por la Ley*.

Por lo tanto, el sustrato jurídico que da origen al derecho de protección de datos asienta tres criterios básicos que debemos tener en cuenta a la hora de perfilar su núcleo esencial:

a) la autodeterminación informativa, como derecho de la persona concernida orientado a salvaguardar su intimidad y privacidad;

b) el principio de no injerencia, especialmente por parte de la autoridades públicas, como principio general;

c) los términos y condiciones en los que esta regla general puede excepcionarse, que podemos agrupar en dos grandes apartados: primero, la necesidad de que sea una Ley la que prevea una posible *intervención* en este derecho y, segundo, las condiciones en que la excepción podrá justificarse, basadas fundamentalmente en que esa intervenc*ión suponga una medida que sea necesaria en una sociedad democrática para salvaguardar la seguridad nacional, la seguridad pública y el bien estar económico del país, la defensa del orden y la prevención del delito, proteger la salud o la moral o proteger los derechos y libertades de los demás*.

[44] Nos referimos especialmente el artículo 12 de la *Declaración Universal de Derechos Humanos*.
[45] Disponible en https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/005

Junto a estos elementos esenciales, directamente extraíbles de la norma, la *Agencia Europea para la Protección de los Derechos Fundamentales*, en su interpretación del artículo 8 del CEDH, nos recuerda que el propio *Tribunal Europeo de Derechos Humanos* sostuvo que este precepto no solo contiene la obligación de los Estados de abstenerse a realizar cualquier actividad que pueda violar el derecho (no hacer), sino que, en determinadas circunstancias, los poderes públicos deben adoptar una posición activa (un obligación de hacer) en la garantía efectiva de su respeto[46].

Además del CEDH otras normas irán dando forma al contenido del derecho, a los principios que deben guiar el tratamiento, al grado de responsabilidad y facultades de los sujetos intervinientes, etc. Quizá la más significativa en los países del entorno europeo sea el *Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal*[47] (en adelante *Convenio 108*), donde se preveía la necesidad de contar con un desarrollo legislativo nacional adecuado a sus disposiciones que fijaría las garantías apropiadas[48]. Además de ser el primero que, hasta ese momento, introduce directamente en su título el término *protección de datos* lo que conduce a su tratamiento como derecho autónomo, el *Convenio 108* resulta esencial porque refleja nítidamente que este derecho mantiene su *carácter instrumental* e interconexión con el ejercicio de otros derechos. Según su primer artículo el objeto del *Convenio 108* es *garantizar* a toda persona, con independencia de su nacionalidad o residencia, *el respeto a sus derechos y libertades* y, en concreto, a la vida privada, *con respecto al tratamiento de sus datos personales*[49]. Datos personales que son definidos como «(…) *cualquier información relativa la persona física identificada o identificable* (…)»[50].

Entre las cuestiones que han de ser más destacadas de esta regulación podemos señalar tres: a) este *Convenio 108* fija en su Capítulo II los *principios básicos para la protección de datos* que, a partir de entonces y como veremos, se irán manteniendo y perfilando en la normativa posterior; b) pone su atención

---

[46] *Vid. Handbook on European data protection law* – 2018 edition, p. 24, disponible en http://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law (última visita 11 de enero de 2019) donde hace alusión a ECtHR, I v. Finland, n.º 20511/03, 17 July 2008; ECtHR, K. U. v. Finland, n.º 2872/02, 2 December 2008.

[47] Firmado en Estrasburgo el 28 de enero de 1981 y Ratificado por España el 27 de enero de 1984. *BOE* n.º 274 de 15 de noviembre1985.

[48] Aunque la Unión Europea no forma parte de la Convención 108, todos los Estados miembro son parte, *Vid.* Bignami, F., «Privacy and Law Enforcement in the European Union: The Data Retention Directive», *Chicago Journal of International Law*, Vol. 8. (1), 2007, pp. 233 a 255, *Vid.* p. 242.

[49] *Vid.* art. 1 del Convenio 108.

[50] *Vid.* art. 2 del Convenio 108.

también sobre los flujos transfronterizos de datos, una cuestión que se ampliará en el año 2001 con el *Protocolo adicional sobre flujo transfronterizo de datos con terceros Estados*[51]; y c) crea un *Comité consultivo*.

Por otra parte, el *Convenio 108* sustenta la construcción de su protección sobre la necesaria garantía de la *calidad* de los datos *y su adecuación a los fines*, señalando que estos:

a) habrán de ser recogidos y tratados *de forma leal y legítima*;
b) serán almacenados para *finalidades legítimas y determinadas*;
c) *no podrán ser utilizados para fines incompatibles* a las finalidades legítimas;
d) serán *exactos y actualizados*;
e) se conservarán en una forma que *permita la identificación de la persona*;
f) *no serán almacenados más allá de lo estrictamente necesario* para cumplir con las finalidades legítimas[52].

De este modo, si tenemos en cuenta lo establecido en estos seis apartados, quedan garantizados los *principios de proporcionalidad y de legitimidad* que debe regir todo tratamiento de los datos personales, al recordar que los datos habrán de ser *adecuados, relevantes* y *no excesivos para cumplir las finalidades legítimas por las que fueron tratados*.

Más adelante, el art. 8 del *Convenio 108* concreta el conjunto de facultades asignadas al sujeto concernido, que integran su núcleo esencial y le garantizan que dispondrá de un control efectivo sobre sus datos:

a) *conocer la existencia de un fichero*, *sus finalidades principales*, *su identidad*, *su residencia habitual o el establecimiento principal de la autoridad controladora*[53];
b) *obtener* a intervalos razonables *la confirmación de los datos y su permanencia* o no en el fichero;
c) *poder rectificar o borrar* dichos datos en caso necesario.

---

[51] *Vid.* art. 2 del *Protocolo Adicional del Convenio n.º 108 para la Protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y relativo a transferencias de datos*. Instrumento de ratificación publicado en el *BOE* n.º 228, de 20 de septiembre de 2010, pp. 79619 a 79624.

[52] *Vid.* art. 5 del Convenio 108.

[53] Autoridad controladora a efectos del art. 2 c) del Convenio 108 se refiere a «la persona física o jurídica, la autoridad pública, el servicio o cualquier otro organismo que sea competente con arreglo a la ley nacional para decidir cuál será la finalidad del fichero automatizado, cuáles categorías de datos de carácter personal deberán registrarse y cuáles operaciones se les aplicarán»,

Pero, sin duda, resulta especialmente interesante para nuestro objeto la previsión que hace de una *categoría especial de datos*. El *Convenio 108* los denomina *datos particulares* y en ellos se incluye *los datos que revelan las convicciones religiosas u otras creencias* (junto a los que revelan el origen racial y las opiniones políticas). Los datos que revelan la adscripción religiosa de la persona no podrán tratarse *salvo que la legislación interna del Estado firmante que lo vaya a permitir prevea las garantías jurídicas apropiadas*. Una regla que también se extenderá al tratamiento de los datos referidos a condenas penales[54]. Queda así dibujado, como mínimo imprescindible, un régimen donde no está permitido la recogida y uso de datos religiosos. Una regla general que solo se podrá excepcionar mediante una Ley donde se prevean las garantías necesarias para evitar que este tratamiento resulte en actitudes lesivas de derechos o discriminatorias.

Todas las garantías que concreta el *Convenio 108* antes vistas, es decir, la necesidad de cumplir los requisitos fijados para asegurar la *calidad* de los datos, la prohibición del tratamiento de las categorías especiales de datos como regla general y la indisponibilidad de los derechos reconocidos al sujeto para asegurar el control de sus datos no se podrán excepcionar salvo que, como prevé el propio Convenio recogiendo la tradición establecida en el CEDH, *esté previsto en la Ley del Estado parte que lo vaya a hacer* y *constituya una medida necesaria* en una sociedad democrática *para la protección de la seguridad nacional y la seguridad pública, los intereses monetarios del Estado, la represión de infracciones penales, la protección de la persona concernida y los derechos y libertades de otras personas*. Por último, sí que se contempla una posible restricción de los derechos previstos en el artículo 8 y solo de ellos cuando el uso, tratamiento o conservación de los datos se realice con *fines estadísticos o de investigación científica*[55].

Segundo, es cierto que el precepto constitucional no contiene, de forma literal, una mención expresa al *derecho a la protección de datos*, sin embargo su existencia y autonomía respecto al derecho a la intimidad ha sido constatado por la jurisprudencia del Tribunal Constitucional[56] en los siguientes términos:

— Su singularidad se deduce de la distinta función o finalidad que tiene asignada cada derecho: mientras el derecho a la intimidad busca proteger la vida

[54] *Vid.* art. 6 del Convenio 108.

[55] *Vid.* art. 9 del Convenio 108.

[56] *Vid.* especialmente las Sentencias del Tribunal Constitucional 290/2000 y 292/2000. Planas Arnaldos, M.ª Carmen, «El derecho fundamental a la protección de datos…», *op. cit.*, *Vid.* p. 70; Arenas Ramiro, Mónica, *El derecho fundamental a…», op. cit.*, *Vid.* p. 445.

personal y familiar del individuo ante cualquier injerencia externa, el derecho a la protección de datos aumenta la garantía concretando un *poder de disposición y control* del individuo sobre sus datos, que abarca desde su uso y destino hasta la disposición de una serie de facultades para evitar su trafico ilícito y lesivo para su dignidad y derechos[57]. Ese poder de *disposición y control*, afirma el Tribunal Constitucional, «(…) 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»[58].

— A consecuencia de ello ambos derechos se diferencian por su contenido. En el caso del derecho de protección de datos se ha concretado en un haz de facultades que integran ese poder de uso y disposición, a saber: a) el derecho a saber y estar informado sobre el destino y uso de estos datos; b) el derecho a acceder, modificar o rectificar y cancelar estos datos[59]. Un conjunto de facultades que en correspondencia «(…) *consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos*»[60]. De este modo el conjunto de derechos que integra su contenido esencial se corresponde con un conjunto correlativo de *obligaciones de hacer*[61] por parte de los terceros que intervienen en el tratamiento de esos datos: a) la obligación de recabar el consentimiento del interesado; b) de informar sobre el uso y destino de esos datos; c) facilitar el acceso a la consulta de dichos datos, su rectificación y borrado o cancelación. Obligaciones y responsabilidades que, como veremos, en el nuevo Reglamento europeo se han visto detalladas.

— Por último, ambos derechos se diferencian por el objeto sobre el que se proyectan, siendo más amplia la información protegida por el *derecho de protección de datos* que aquellos datos referidos exclusivamente a la intimidad de la persona. En palabras del Tribunal Constitucional la protección de datos se refiere a: *todos aquellos datos que sean relevantes o tengan incidencia para el ejercicio de cualesquiera de los derechos de las personas, sean o no constitucionales y sean o no relativos al honor, ideología, intimidad personal y familiar*[62]. La protección abarca así cualesquiera datos que pueden tener relación

[57] STC 292/2000, FJ 6.º
[58] STC 292/2000, FJ 7.º
[59] STC 292/2000, FJ 7.º
[60] STC 292/2000, FJ 5.º
[61] MARTÍNEZ MARTÍNEZ, Ricard, «El derecho fundamental a la protección de datos: perspectivas», en *Revista de Internet, Dret I Política. UOC*, n.º 5 (2007), pp. 47 a 61, *Vid.* p. 50.
[62] Argumento suficiente para que se establezca un párrafo independiente para enunciar este derecho, PÉREZ-LUÑO, Antonio Enrique, «Informática y Libertad. Comentario al artículo 18.4 de la Constitución española», en *Revista de Estudios Políticos*, n.º 24 (1981), pp. 31 a 53, *Vid.* p. 44.

con todas las facetas de la vida de una persona que, aunque no formen parte de su intimidad, no desea que sean conocidas[63]. En definitiva, dice el Tribunal Constitucional, la cobertura del derecho a la protección de datos se proyecta sobre *toda aquella información que identifique o permita identificar al sujeto y, especialmente, sobre aquellos datos que permitan elaborar un perfil ideológico, racial, sexual, económico del individuo*[64].

Tercero, no debemos olvidar que, a pesar de constituirse como un *derecho autónomo*, el marco de protección que se deriva de la redacción del precepto se refiere un grupo de derechos interconectados, el respeto *al honor, a la intimidad personal y familiar, a la propia imagen, la inviolabilidad del domicilio*, *el secreto de las comunicaciones*, etc. o, más específicamente los enumerados en el párrafo 4.º cuando señala que: «*la Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos* (…)». En todo caso, es una cláusula abierta, por la que el alcance del derecho se extiende por la referencia expresa que realiza el precepto al «(…) *pleno ejercicio de sus derechos*». De este modo, el *derecho a la protección de datos* presenta un *carácter instrumental* y de garantía de otros derechos donde, sin duda, se encuentra el derecho a la libertad ideológica y religiosa. Tomando literalmente las palabras de la profesora Garriga: «[e]n el artículo 18.4 se establecen limitaciones al uso de la informática para garantizar el pleno ejercicio de los derechos de las personas. Se mencionan expresamente dos de los derechos que podrían verse amenazados por un uso abusivo e ilegítimo de las tecnologías de la información: los derechos al honor y a la intimidad personal y familiar; pero *otros como la libertad ideológica o religiosa, la libertad sindical, el derecho a no ser discriminado, la presunción de inocencia o el derecho a acceder en condiciones de igualdad a la función pública, por ejemplo, podrían resultar igualmente amenazados*»[65].

Este *carácter instrumental* sin embargo no significa, como señala Polčák, que la normativa minimice su principal objetivo: ordenar una adecuada pro-

---

[63] Trascendiendo la protección de la privacidad más allá de la mera intimidad, entendida como soledad, para protegerla incluso en las relaciones sociales, *Vid.* Pérez Luño, A. «La protección de los datos personales del menor en Internet», en *Anuario de la Facultad de Derecho* (Universidad de Alcalá II), 2009, pp. 143 a 175, *Vid.* pp. 145 y ss.

[64] STC 292/2000, FJ 6.ª: «(…) el que los datos sean de carácter personal no significa que solo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo».

[65] Garriga Domínguez, Ana, *Tratamiento de datos personales y derechos fundamentales,* Dykinson, p. 99. La cursiva es del autor.

tección de los datos personales, sino que a la hora de configurar su tutela jurídica supone la necesidad de tener en cuenta los efectos que el uso de la información (datos) tendrá sobre el resto de los derechos, más que los datos en si mismos considerados. Por lo tanto, resulta evidente que el objetivo de la Ley no será la regulación de todos los derechos de la persona, que en la mayor parte de las ocasiones ya tendrá su propia legislación, si no de aquellos aspectos de su ejercicio que sufrirán un impacto por el tratamiento de sus datos. Por ello, el régimen de protección de los datos está basada principalmente en una comprensión procedimental de su alcance y utilidad, enfocada a los efectos del uso de la información sobre la vida privada y los intereses sociales de la persona, más que una protección meramente estática de los datos que, de por si, podrían tener distinto valor: disponer de los datos genéticos de una persona –ADN– puede ser útil para la investigación y sus aplicaciones en la salud pero, en otras ocasiones y bajo otras circunstancias, puede resultar inútil o incluso dañino para el sujeto concernido[66].

Como veremos, al analizar la nueva regulación, esta nueva formulación coincide con la evolución del fundamento estático, garantía de la *calidad* de los datos, al dinámico, la legitimidad de su uso. Para ello, será útil conocer la nueva formulación de este derecho en el ámbito europeo y español.

2.3 **Un nuevo impulso al derecho de protección de datos en el marco de la Unión Europea**

2.3.1 *Las referencias al derecho a la protección de datos en el Derecho originario europeo como punto de partida*

La Unión Europea asienta su estrategia sobre protección de datos con importantes referencias en su Derecho original o primario. Su protección, como la del resto de los derechos fundamentales de la persona, es un objetivo inexcusable de la UE pues, como nos recuerda el art. 2 del *Tratado de la Unión Europea* (en adelante TUE), la UE se funda sobre los *valores de respeto a la dignidad humana, libertad, democracia, igualdad, Estado de Derecho y respeto de los derechos humanos* (…). El reconocimiento de esos derechos fundamentales se hará, según el art. 6 del mismo Tratado, de acuerdo con la *Carta de los Derechos fundamentales de la Unión Europea de 7 de diciembre de 2000*

[66] POLČÁK, Radim, «Getting European data protection off the ground», *International Data Privacy Law*, 2014, Vol. 4, n.º 4, pp. 282 a 289, *Vid.* pp. 283 y 284.

(en adelante *Carta*), el CEDH y las tradiciones constitucionales comunes[67]. Dado que el CEDH ya se ha analizado con anterioridad y la diversidad de tradiciones constitucionales requeriría un estudio de mayores dimensiones que no solo sobrepasaría el objeto formal de este estudio[68] sino también el material, ya que su realidad debería ceder ante la reciente aplicación del Reglamento que instaura un marco general directamente aplicable en todos los países y genera un proceso de actualización de la normativa interna de cada Estado para adecuarla al marco común de la UE, nos centraremos en el análisis de la *Carta* para, a continuación, pasar al apartado que nos permita desarrollar los términos previstos en la nueva normativa.

Superando la formulación del CEDH, la *Carta* regula de forma expresa el *derecho a la protección de datos*[69]. Para ello le dedica su propio artículo situado, eso sí, justo a continuación de consagrar en su artículo 7 el respeto a la vida privada y familiar. Esta formulación, en nuestra opinión, realza el *carácter autónomo* del derecho a la protección de datos sin dejar de preserva su *carácter instrumental* e interconexión con el resto de derechos, en especial, con el derecho a la intimidad y vida personal. Centrándonos ya en los términos en los que se desarrolló su proclamación, según el art. 8 de *la Carta* toda persona tiene reconocido el derecho a la protección de sus datos personales y reafirma el *principio de legitimidad,* establecido en el *Convenio 108*, al señalar que *los datos habrán de ser tratados para fines específicos*. Del mismo modo, este ar-

---

[67] *Vid.* art. 6 del TUE: 1. La Unión reconoce los derechos, libertades y principios enunciados en la Carta de los Derechos Fundamentales de la Unión Europea de 7 de diciembre de 2000, tal como fue adaptada el 12 de diciembre de 2007 en Estrasburgo, la cual tendrá el mismo valor jurídico que los Tratados.

Las disposiciones de la Carta no ampliarán en modo alguno las competencias de la Unión tal como se definen en los Tratados.

Los derechos, libertades y principios enunciados en la Carta se interpretarán con arreglo a las disposiciones generales del título VII de la Carta por las que se rige su interpretación y aplicación y teniendo debidamente en cuenta las explicaciones a que se hace referencia en la Carta, que indican las fuentes de dichas disposiciones.

2. La Unión se adherirá al Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales. Esta adhesión no modificará las competencias de la Unión que se definen en los Tratados.

3. Los derechos fundamentales que garantiza el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales y los que son fruto de las tradiciones constitucionales comunes a los Estados miembros formarán parte del Derecho de la Unión como principios generales».

[68] Para lo que resulta absolutamente recomendable el estudio Arenas Ramiro, Mónica, *El derecho fundamental a…», op. cit.*

[69] «En efecto, (…), la Carta Europea de Derechos Fundamentales incorpora de modo expreso el derecho a la protección de datos», Cfr. Martínez Martínez, Ricard, «El derecho fundamental a la protección…», *op. cit.*

tículo 8 de *la Carta* incluye de forma expresa una cuestión esencial en el sistema de protección de este derecho: solo el consentimiento de la persona o una causa legítima legalmente establecida permitirá el tratamiento de los datos. Concluye el sistema adoptado por *la Carta* recordando las funciones que, como parte de su contenido esencial, este derecho otorga al sujeto concernido, especialmente el *derecho al acceso a los datos* y *el derecho de rectificación*.

Bajo este mínimo común, el artículo 39 TUE se remite a la potestad del Consejo para concretar su desarrollo normativo y adoptar una decisión orientada a fijar las reglas *relativas a la protección de los individuos respecto al tratamiento de sus datos personales, así como las relativas a la libre circulación de dichos datos*[70], que dictará de conformidad con lo dispuesto en el art. 16 del *Tratado de Funcionamiento de la Unión Europea* (en adelante TFUE). Este art. 16 del TFUE, tras garantizar el derecho de todos a la protección de los datos personales, se refiere también al mandato del *Parlamento* y *el Consejo para establecer las reglas relativas a la protección de datos personales por las Instituciones, cuerpos, oficinas y agencias europeas y los Estados miembros*, así como *las relativas a la libertad de movimiento de dichos datos*. En ambos casos, ambos Tratados prevén la necesidad de que el cumplimiento de ambas reglas se sujete al control de una autoridad independiente.

Nos situamos así frente al necesario desarrollo normativo que ahora se concreta, en términos generales[71], en un conjunto de disposiciones normativas: el anteriormente mencionado RGPD[72], en el Reglamento (CE) n.º 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, *relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos*[73] (en adelante Reglamento 45/2001) y en la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, *relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones*

[70] *Vid.* art. 39 del TUE.

[71] Ciertamente existen otras normas pero que, por su referencia a cuestiones específicas consideramos innecesario tratar en este estudio, por ejemplo, *Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas* (Directiva sobre la privacidad y las comunicaciones electrónicas), publicada en Diario Oficial n.º L 201 de 31/07/2002, y

[72] Que deja totalmente sin efecto la Directiva 95/46 desde el 24 de mayo de 2018.

[73] Publicado en el Diario Oficial n.º L 008 de 12/01/2001.

penales o de ejecución de sanciones penales y a la libre circulación de dichos datos (en adelante *Directiva 680/2016*)[74].

No todos ellos tienen la misma incidencia en el objeto de nuestro estudio, especialmente el referido a las instituciones y órganos comunitarios, por lo que nosotros analizaremos en profundidad el RGPD apoyado en referencias expresas a la Directiva 680/2016, ya que ambos forman el paquete de actualización del marco normativo europeo en esta materia.

2.3.2 *Las novedades introducidas por el nuevo Reglamento General de Protección de Datos y la Directiva 680/2016*

Una de las grandes virtudes que se han puesto de manifiesto sobre el nuevo RGPD es el incremento del nivel de garantía sobre los derechos/facultades en los que tradicionalmente se descomponen el derecho de acceso y control de los datos, pero, sobre todo, la inclusión y enumeración de otros nuevos, como por ejemplo el derecho a la portabilidad, el derecho al olvido y el derecho a conocer cuando se ha producido una violación de la seguridad de sus datos, etc. Un conjunto de nuevas facultades que proporcionan al ciudadano europeo un grado de eficiencia y control más alto sobre el ejercicio de su *autodeterminación informativa*[75]. Por su parte, la *Directiva 680/2016*, referida específicamente al ámbito de la investigación, persecución, detección, etc. de ofensas criminales[76], procura actualizar las debidas garantías en la protección de los datos personales cuando estos vayan a ser manejados por las autoridades y fuerzas y cuerpos de seguridad del Estado *con la finalidad de prevenir y perseguir la comisión de delitos*. Para ello adopta medidas muy clarificadoras y útiles como, por ejemplo, la delimitación del diferente tratamiento que podrá darse a los datos recogidos según pertenezcan a cada una de las partes que pueden verse implicadas en estos procedimientos. Y es que, con toda lógica, no tiene porque coincidir ni el grado de tratamiento ni el nivel de seguridad que requiere el uso y cesión de los datos pertenecientes a las víctimas y potenciales testigos de un proceso que los relativos a los sospechosos y autores del delito[77]. Así mismo, esta *Directiva 680/2016* considera necesario impulsar medidas adecuadas para la cooperación en la lucha contra el terrorismo y el

[74] Por la que se deroga la Decisión Marco 2008/977/JAI del Consejo. Publicada en el Diario Oficial n.º L119/89, el 4 de mayo de 2016.

[75] Fernández Villazón, Luis Antonio, «El nuevo Reglamento Europeo …», *op. cit.*, *Vid.* p. 398.

[76] *Vid.* art. 1 de la Directiva 680/2016.

[77] *Vid.* art. 6 de la Directiva 680/2016.

crimen transfronterizo permitiendo a los cuerpos policiales y de justicia de los Estados miembro intercambiar información necesaria para las investigaciones de forma más efectiva y eficiente[78].

Pues bien, el RGPD y la Directiva 680/2016, cada una en su ámbito de actuación, nos ofrecen elementos jurídicos básicos que son transversales y, en nuestra opinión, necesarios para interpretar como se desarrollan las garantías generales del modelo de protección de los datos. Antes de pasar a su desarrollo consideramos útil tener en cuenta algunas cuestiones:

Primero, desde sus primeros preceptos ambas normas se sitúan como un marco legal que supera la antigua posición de la Directiva 95/46/CE, más centrada en la disposición de normas y obligaciones procedimentales[79], y el derecho se regula con un indudable *carácter instrumental*, que permite intensificar el respeto al conjunto de derechos y libertades de las personas concernidas, entre los que se encuentra la libertad ideológica y religiosa[80]. Bajo esta lógica la normativa trata de proteger a la persona de la vulneración o interferencias que pudieran suponer sobre sus derechos, en nuestro caso sobre la libertad religiosa, el uso y disposición de cierta información personal.

Segundo, el sujeto de la protección siguen siendo las personas físicas, sin que pueda extenderse a las personas jurídicas, por lo que todo lo que tenga que ver con el diseño de políticas legislativas orientadas a la protección del derecho de libertad ideológica y religiosa, en lo que se refiera a las posibles interferencias que el uso y disposición de sus datos personales tenga sobre las personas, habrá de focalizarse en el establecimiento de garantías personales,

[78] «La Directiva de policía establece normas comunes relativas al tratamiento de los datos personales de las personas físicas implicadas en procesos penales, ya sea en calidad de sospechosos, víctimas o testigos, teniendo en cuenta el carácter específico del ámbito policial y de la justicia penal. La armonización de las normas de protección de datos en el ámbito de la aplicación de la ley, incluidas las relativas a las transferencias internacionales, facilitará la cooperación transfronteriza entre las autoridades policiales y judiciales, tanto dentro de la UE como con los socios internacionales y, de este modo, propiciará una mayor eficacia en la lucha contra la delincuencia. Se trata de una importante contribución a la Agenda Europea de Seguridad», *Vid.* la Comunicación de la Comisión al Parlamento Europeo y al Consejo, *Intercambio y protección de los datos personales en un mundo globalizado*, COM(2017) 7 final, Bruselas, 10.1.2017, p. 4 disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52017DC0007&from=EN (última visita el 9 de noviembre de 2018).

[79] MCDERMOTT, Yvonne, «Conceptualising the right to data protection in an era of Big Data», *Big Data & Society*, January-June 2017, pp. 1-7, *Vid.* p. 1.

[80] Esta afirmación se concreta desde los primeros preceptos en la identificación de su objeto: *la protección de los derechos y libertades fundamentales de las personas físicas*, en general, y *de su derecho a la protección de datos*, en particular, vid art. 1 del RGPD y 1.2. a) de la Directiva 680/2016.

no institucionales, sobre aquellas actividades y medidas que implique el tratamiento de sus datos personales.

Tercero, tanto en el RGPD[81] como en la Directiva 680/2016[82] la UE trata de cubrir una doble faceta con este sistema: por un lado actuar como protector de los derechos de la persona y, por otro, como garante del *intercambio de información* o la *libre circulación de datos* en el territorio de la Unión. Por lo tanto, la nueva legislación europea busca asentar una base equilibrada entre la protección de los derechos de la persona y el legítimo tratamiento y libre circulación de los datos, es decir entre los intereses del individuo y de quienes tratan los datos. Esto permite señalar que el derecho a la protección de datos no implica una ausencia total de tratamiento, sino la posibilidad de concretar un adecuado intercambio de información atemperado por el cuidadoso establecimiento de las garantías necesarias para proteger a la persona concernida de los efectos indeseados de su uso[83]. Estas garantías generales que establezca el marco europeo podrán incrementarse en la legislación de cada Estado[84].

Cuarto, el ámbito de aplicación material del RGPD incluye cualquier forma de tratamiento de los datos personales, sea o no automatizada, excepto cuando se lleven a cabo por las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o su ejecución «(…) *incluida la de protección frente a amenazas a la seguridad pública y su prevención*»[85]. En este caso, los procedimientos y garantías, como ya sabemos, quedarán asentados por la *Directiva 680/2016*[86].

Quinto, en la determinación de su alcance, el RGPD opta por aplicar una fórmula que extiende sus garantías a todas aquellas situaciones o actividades en las que una de las dos partes esté en territorio europeo. En los términos en los que se expresa la norma, su protección se aplicará cuando el establecimien-

---

[81] *Vid.* art. 1 del *RGPD.*

[82] *Vid.* art. 1.2 a) y b) de la Directiva 680/2016.

[83] «This would also mean that the physical existence of personal data should not be problematic, as the primary concern would then be about forms of their use, or better said, rights to use them», Polčák, R., «Getting European data protection…», *op. cit.*, *Vid.* p. 284.

[84] *Vid.* art. 1.3 de la Directiva 680/2016.

[85] *Vid.* art. 2 del *RGPD*.

[86] Esta a su vez excluye de su ámbito aplicación, junto con aquellas que se desarrollen en el desempeño de actividades que no estén comprendidas en el ámbito de aplicación del Derecho de la Unión, el tratamiento de datos que se realice por las instituciones y organismos de la Unión, lo que nos lleva a la necesaria aplicación del Reglamento 45/2001 identificado al inicio entre la terna de disposiciones a tener en cuenta para conocer el contexto normativo general europeo. *Vid.* art. 2.3 a) y b) de la Directiva 680/2016.

to principal[87] del responsable del tratamiento[88] esté en la Unión o cuando la persona concernida resida en la Unión, con independencia de que el tratamiento de los datos tenga lugar en la UE o no, en el primer caso, o que el responsable del tratamiento no este establecido en la UE, en el segundo[89]. Esta fórmula permite a los Estados ejercer su jurisdicción de forma eficiente sobre aquellos datos (información) que de alguna manera están vinculados con su territorio, ciudadanos, o intereses generales[90]. Esta forma de concretar su alcance, por ejemplo, nos resultará útil a la hora de valorar la aplicación de estas garantías a los casos en que el RD 594/2015 solicita información adicional para certificar la fundación y establecimiento en España de las entidades de origen extranjero o que operan internacionalmente, donde se pueden recabar datos personales de sujetos relacionados con estas confesiones en sus países de origen.

A continuación analizaremos los términos en los que se concreta el desarrollo que el nuevo marco normativo europeo realiza sobre la regulación de ciertos elementos esenciales para la protección de este derecho.

a) El concepto general de datos personales y algunas nuevas categorías

La determinación del concepto «datos» es un elemento nuclear en la configuración del sistema de protección, ya que se trata del objeto material sobre el que se

---

[87] El propio RGPD nos ofrece un concepto de ««establecimiento principal»: a) en lo que se refiere a un responsable del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión, salvo que las decisiones sobre los fines y los medios del tratamiento se tomen en otro establecimiento del responsable en la Unión y este último establecimiento tenga el poder de hacer aplicar tales decisiones, en cuyo caso el establecimiento que haya adoptado tales decisiones se considerará establecimiento principal; b) en lo que se refiere a un encargado del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión o, si careciera de esta, el establecimiento del encargado en la Unión en el que se realicen las principales actividades de tratamiento en el contexto de las actividades de un establecimiento del encargado en la medida en que el encargado esté sujeto a obligaciones específicas con arreglo al presente Reglamento», *Vid.* art. 4 del *RGPD*.

[88] Será responsable del tratamiento: «la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros», *Vid.* art. 4. 7) del *RGPD*.

[89] *Vid.* art. 3 del *RGPD*. Para un estudio más pormenorizado de las consecuencias de este precepto *Vid.* DE HERT, Paul, and CZERNIAWSKI, Michal, «Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context», International Data Privacy Law, 2016, Vol. 6, n.º 3, pp. 230-243.

[90] Conocida como estrategia de «Top-down» en contraposición a la de «Bottom-up», todo ello en POLČÁK, Radim, «Getting European data protection…», *op. cit.*, *Vid.* p. 287 –la traducción es del autor–.

proyecta el sistema de protección establecido. La preocupación por este tema se remonta incluso a los orígenes de su armonización en el ámbito europeo[91]. Desde un punto de vista general, lo más lógico sería considerar que el concepto de datos personales queda destinado a definir todo aquello que pueda ser considerado un «dato» en un sentido estricto o literal: nombres, direcciones, números de identificación personal o, desde un punto de vista más técnico, direcciones de correo electrónicos, IPs, etc. Sin embargo, en la actualidad se ha optado por utilizar un concepto más amplio, donde cada vez son más los elementos susceptibles de ser incluidos dentro de esta categoría, no solo por su condición estricta de dato sino también por las consecuencias que su uso pueda tener. Atender a esta realidad y a la verdadera capacidad de procesamiento de datos actual que incrementa los riesgos, se alinea con la necesidad de complementar su fundamento una dimensión más dinámica –orientada a asegurar la finalidad y legitimidad de su uso–. Van Loenen et. alia nos recuerdan el énfasis con el que el Grupo de Trabajo del art. 29 recomendaba que fueran tenidas en cuenta la finalidad y los resultados del uso de esos datos para determinar cuándo nos encontramos ante datos personales o no. Según la opinión que fue vertida por el Grupo de Trabajo en su informe de 2007 los datos pueden ser considerados personales, y por lo tanto objeto de la protección del derecho, no solo por su mero carácter de datos sino por que su uso probablemente tendrá impacto sobre los derechos e intereses de una persona, para lo que habrá que tener en cuenta todas las circunstancias que rodean el caso concreto. Ni si quiera se precisa que el resultado potencial de su uso deba tener un gran impacto, basta simplemente con que, como resultado de su procesamiento, el individuo pueda llegar a ser tratado de forma distinta a otras personas[92].

---

[91] Se trata de un concepto que ya tuvo que ser definido por el Grupo de Trabajo del artículo 29, creado en el contexto de la Directiva 95/46/CE. Este Grupo se trataba de «(…) un organismo europeo de carácter consultivo e independiente, formado por un representante de la autoridad o autoridades de control de cada uno de los Estados miembros y un representante de la Comisión. (…) Tiene como finalidad específica (…)»: a) estudiar la aplicación de las disposiciones nacionales para la aplicación de la Directiva para contribuir a su aplicación homogénea; b) emitir dictamen sobre el nivel de protección existente; c) asesorar a la Comisión sobre cualquier proyecto de modificación de la Directiva, de medidas adicionales o específicas que deban adoptarse para salvaguardar los derechos y libertades de las personas en lo que se refiere al tratamiento de sus datos personales, así como cualquier otro proyecto de medidas comunitarias que afecte a esos derechos; d) emitir dictamen sobre los códigos de conducta elaborados a escala comunitaria, *Vid.* Rebollo Delgado, Lucrecio, *Vida privada y protección de datos en la Unión Europea*, Dykinson, 2008, p. 156.

[92] Todo lo anterior en Van Loenen, Bastiaan; Kulk, Stefan & Ploeger, Hendrik, «Data protection legislation: A very hungry Caterpillar. The case of mapping data in the European Union», *Government Information Quarterly* 33 (2016) 338–345, *Vid.* p. 339. Sobre el Informe del Grupo de Trabajo *Vid. Dictamen 4/2007 sobre el concepto de datos personales*, adoptado el 20 de junio, 01248/07/ES WP13, disponible en http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_es.pdf pp. 11 y 12.

Tanto en la interpretación del concepto de datos personales, como en la determinación del conjunto de principios que deben guiar su tratamiento la nueva regulación se mantiene en términos sustancialmente similares[93]. Es así como tanto el RGPD como la *Directiva 680/2016* dedican uno de sus preceptos iniciales a definir de forma amplia el concepto de *datos personales*, considerados como «toda información sobre una persona física identificada o identificable». Quizá la mayor duda que se pueda plantear del tenor de este precepto será como determinar cuando una persona puede ser considerada identificable. El propio precepto afirma que una persona resulta *identificable* cuando pueda determinarse, directa o indirectamente, su identidad utilizando un «identificador», por ejemplo, el nombre, el número de identificación, la localización o varios elementos de su «(…) *identidad física, fisiológica, genética, psíquica, económica, cultural o social* (…)»[94]. La forma en que se expresa el Reglamento y el conjunto abierto de características a las que hace referencia nos permite concluir que nos situamos ante una normativa que tiene en cuenta la posibilidad de que sean incluidos dentro de la categoría muchos de los datos que, aunque disgregados pudieran resultar inútiles, al tratarlos de forma conjunta puedan dar como resultado la identificación de la persona. Por eso la lista no es exhaustiva, sino que cualquier información puede ser objeto de la misma protección, si da como resultado la identificación del sujeto. Esta vis expansiva, por ejemplo, puede comprobarse en la nueva regulación cuando junto a esta definición general del elemento «datos», el Reglamento introduce nuevas categorías: a) los *datos genéticos*: que califica como aquellos relativos a las características genéticas heredadas o adquiridas que proporciona información sobre la fisiología de una persona o su salud y que son extraídos de una muestra biológica[95]; b) los *datos biométricos*: «(…) *relativos a las características físicas, fisiológicas o conductuales de la persona* (…)» que permiten la identificación única de la persona y son obtenidos mediante un sistema técnico específico, como la captura de imágenes faciales o datos dactiloscópicos[96]. Ambos conceptos no solo interesan porque se refieren a elementos que cada vez están siendo más utilizados para identificar a los sujetos, sino porque incluso se han incluido dentro de las categorías de datos especiales[97].

---

[93] VAN LOENEN, Bastiaan; KULK, Stefan & PLOEGER, Hendrik, «Data protection legislation:…», *op. cit.*, *Vid.* p. 343.

[94] *Vid.* art. 4. 1) del RGPD y 3. 1 de la Directiva 680/2016.

[95] *Vid.* art. 4. 13) del RGPD.

[96] *Vid.* art. 4. 14) del RGPD y artículo 3. 13) de la Directiva 680/2016.

[97] *Vid.* art. 10 del RGPD y de la Directiva 680/2016.

En definitiva, esta forma de entender el concepto de datos nos permite asegurar que la protección no solo incluye aquellos que afectan a la esfera íntima de la persona, si no todos aquellos que el individuo no quiera que sean conocidos, ampliando la dimensión de protección de la mera intimidad, concebida como aquella esfera que el individuo se desenvuelve en soledad o asilamiento, a la intimidad como un espectro de información, datos, características, etc. que la persona desea conservar auto determinado incluso en sus relaciones sociales[98]. De manera específica en ellos se incluyen aquellos datos que pudieran servir para confeccionar el perfil ideológico y religioso, racial, sexual, etc. de la persona o que según la utilidad a la que fueran destinados pudieran suponer, bajo determinadas circunstancias, una amenaza para la persona y sus derechos[99].

b) La protección específica de datos que revelan las convicciones ideológicas y religiosas de la persona

El artículo 9 del nuevo RGPD considera datos sensibles aquellos que revelen las convicciones ideológicas y religiosas del individuo, junto con otra información sensible, como aquella que pueda revelar su origen étnico o racial, las opiniones políticas, la afiliación sindical, la vida y orientación sexual, los datos genéticos o biométricos, los relativos a la salud, etc. Como principio general se establece la prohibición expresa de tratar estos datos. Esta regla general supone que el sistema de protección por el que opta la legislación es aplicar el principio de autonomía y no injerencia. Si bien, siguiendo a la profesora Cano, debemos tener en cuenta que este derecho no solo se compone de una *dimensión negativa* o *faceta estática* –el derecho a excluir del conocimiento ajeno cuanto se refiere a la persona–, sino también de un *aspecto dinámico* o *dimensión positivo*: el acceso y control por el titular de sus datos e información[100]. Por lo tanto, la prohibición general de tratamiento no solo asegura una efectiva aplicación del principio de no injerencia por parte de terceros, sino que solo podrá excepcionarse cuando medie consentimiento explícito del interesa-

[98] Pérez Luño, Antonio Enrique, «La protección de los datos personales del menor…», op. cit, *Vid.* pp. 145 y ss. En este sentido se distingue entre intimidad y privacidad, como una esfera en el que se desarrollan facetas del individuo que no siempre son íntimas pero desea que no sean conocidas, *Vid.* De la Llana Vicente, Mariano, «La protección de datos personales automatizados:…», *op. cit.*, *Vid.* p. 386 y 387

[99] Fuentetaja Pastor, Jesús, Medina González, Sara, *La protección de datos…, op. cit.,* p. 21.

[100] Cano Ruiz, Isabel, *Los datos religiosos…, op. cit.,* p. 8.

do en ejercicio de su derecho de control sobre los datos o concurra una de las causas legalmente establecidas:

a) el tratamiento sea necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, siempre que lo autorice el Derecho de la Unión o un convenio colectivo que establezca las garantía adecuadas del respeto de los derechos fundamentales e intereses del sujeto concernido;

b) el tratamiento es necesario para proteger los intereses vitales de la persona, cuando no este capacitado física o jurídicamente para emitir el consentimiento;

c) Cuando el tratamiento sea desarrollado por una entidad –asociación, fundación u organismo sin ánimo de lucro– c*uyos fines sean políticos, filosóficos, religiosos, sindicales, etc.*, lo realice en el desarrollo de sus actividades legítimas, con las debidas garantías y los datos sean relativos a sus miembros actuales o antiguos o personas que mantengan contactos regulares con ellas en relación con sus fines. En todo caso, los datos no podrán ser cedidos o comunicados salvo que cuenten con el consentimiento del interesado;

e) los datos tratados ya se han hecho *manifiestamente públicos* por el interesado;

f) sea necesario para formular, ejercer o defender reclamaciones o cuando «(…) los tribunales actúen en ejercicio de su función judicial».

g) como señala literalmente el precepto «el tratamiento es necesario por razones de interés público esencial, (…) que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado»;

h) «el tratamiento es necesario con fines de archivo de interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, (…)»[101];

Por su parte, cuando se trate de usar los datos en caso de investigación, detención, prevención de delitos, etc., el art. 10 de la *Directiva 680/2016* también señala que los datos personales relativos a la adscripción religiosa del individuo solo serán tratados cuando sea estrictamente necesario, estén sujetos a las adecuadas garantías para la protección de los derechos y libertad de la persona concernida, lo haya au-

[101] Además, el precepto incluye otras dos opciones: h) «el tratamiento es necesario para fines de medicina preventiva o laboral (…)»; i) «el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, (…); En ambos casos, los datos podrán ser tratados para los fines previstos en el apartado h) e i) bajo el deber del secreto profesional –según establece el propio apartado h) o el párrafo 3.º del art. 9–.

torizado la Unión europea o un Estado miembro, se protejan los intereses vitales de la persona concernida u otra persona física o cuando el tratamiento se refiera a datos que han sido hechos públicos de manera manifiesta por el sujeto. Será responsabilidad de las autoridades nacionales adoptar las medidas técnicas y organizativas necesarias para asegurar que el nivel de seguridad de la protección de datos es apropiado al riesgo que entraña su uso. Específicamente, cuando el tratamiento de los datos se realice de forma automática (automatizada), deben adoptarse un importante número de medidas, entre las que se deben incluir: a) denegar el acceso al equipamiento técnico utilizado para realizar el tratamiento a toda persona no autorizada; b) prevenir la lectura, la copia el remoción o modificación de los datos; c) prevenir la introducción no autorizada de datos personales o el acceso, modificación o borrado no autorizado de datos personales almacenados.

c) Los principios que deben guiar el tratamiento de datos.

Aunque ciertamente evolucionados y con alguna ampliación, existe una serie de principios que la legislación viene manteniendo para configurar el sistema jurídico sobre protección de datos[102]. Grosso modo, los principios establecidos por el RGPD son: a) el *principio de legalidad*, *legitimidad y transparencia*; b) el *principio de limitación de la finalidad*; c) *el principio de minimización de los datos*; d) el *principio de exactitud de los datos*; e) el *principio de limitación del almacenado*; f) el *principio de seguridad de los datos* y g) el *principio de responsabilidad*[103].

1. Para cumplir con el *principio de legalidad, legitimidad y transparencia*, se requiere:

a) que su posible tratamiento se habilite por el consentimiento del sujeto concernido o en su defecto por cumplir[104] cualquiera de las causas previstas en el artículo 6 del RGPD[105] –*legalidad*– entre las que se incluye:

— el cumplimiento de las obligaciones previstas en un contrato del que el sujeto sea parte;

---

[102] En ellos se recoge desde la necesidad de contar con la información necesaria para tomar una decisión formada, hasta la calidad, la finalidad y su compatibilidad con los objetivos perseguidos, la veracidad, etc., pasando por el punto de bóveda del sistema, el consentimiento del sujeto concernido. Sobre su concreción desde las regulaciones anteriores *Vid.* Pérez Luño, Antonio Enrique, «El concepto de interesado…, *op. cit.*, *Vid.* pp. 27 y 28; Fuentetaja Pastor, Jesús, Medina González, Sara, La protección de datos…, *op. cit.*, *Vid.* pp. 27 a 37.

[103] *Vid. Handbook on European data protection law*, *op. cit.*, *Vid.* pp. 115 a 138.

[104] Bajo responsabilidad quien desarrolla el tratamiento, que deberá se capaz de demostrar su cumplimiento, *Vid.* art. 5 del RGPD.

[105] *Handbook on European data protection law*, *op. cit.*, *Vid.* p. 117.

— el cumplimiento de una obligación legal;

— proteger el interés vital del sujeto o una tercera persona;

— *llevar a cabo una tarea desarrollada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento*;

— satisfacer los intereses legítimos del responsable del tratamiento o un tercero siempre que sobre ellos no prevalezcan los intereses o los derechos y libertades del interesado, especialmente si se trata de un menor.

b) la relación entre el responsable del tratamiento y el sujeto concernido estará presidida por el principio de *legitimidad*[106]. Los datos serán recabados y tratados para el cumplimiento de *fines legítimos*, lo que requiere que el sujeto esté informado de los riesgos posibles que entraña el proceso, de tal manera su tratamiento no pueda suponer efectos negativos no previstos.

c) la *transparencia* se consigue aportando toda la información necesaria sobre el tratamiento, es decir su propósito o fines y sus consecuencias, la identidad y domicilio del responsable del tratamiento, la información sobre las actividades de procesamiento que se llevarán a cabo, de forma clara y comprensible para que el sujeto comprenda las reglas, los riesgos, las garantías y los derechos involucrados. Por último, la transparencia se asegura garantizando el derecho de acceso del sujeto a los datos que están siendo tratados[107].

2. El *principio de finalidad limitada o específica*, requiere que todo tratamiento de datos sea realizado para un fin específico y bien definido, que solo podrá extenderse a otros objetivos adicionales siempre que sean compatibles con el principal[108]. A estos efectos, para valorar cuando un tratamiento ulterior es compatible «(…) el responsable deberá tener en cuenta (entre otras cuestiones): cualquier relación entre estos fines y los fines del tratamiento posterior previsto, el contexto en el que se recogieron esos datos, las expectativas razonables del interesado fundadas en su relación con el responsable del tratamiento, la naturaleza de los datos, las consecuencias de ese tratamiento ulterior para los interesados y la existencia de garantías, tanto para el tratamiento previsto para el fin original como el ulterior, lo que puede ser desarrollado aplicando medidas de encriptación de los datos y/o de *seudonimización»*[109].

3. El *principio de minimización* supone que solo serán tratados los datos que sean adecuados, relevantes y no excesivos para el cumplimiento del propósito principal por el que han sido recogidos o tratados. El tratamiento de los

[106] *Vid. Handbook on European data protection law*, *op. cit.*, *Vid.* pp. 118.
[107] *Vid. ibidem* p. 117.
[108] *Ibidem* p. 122.
[109] *Ibidem* pp. 123 y 124.

datos solo tendrá lugar cuando el fin para el que son tratados no pueda ser alcanzado por ningún otro medio y, en todo caso, el tratamiento no podrá interferir de manera desproporcionada en los intereses, derechos y libertades en riesgo[110].

4. El *principio de exactitud de los datos*, requiere comprobar regularmente los datos y mantenerlos actualizados. De esta forma, los datos inexactos o desactualizados habrán de ser borrados y/o rectificados sin dilación[111].

5. El *principio de limitación del almacenado*, implica que los datos deberán ser borrados o convertidos en anónimos para impedir la identificación del sujeto cuando ya no sean necesarios para los fines para los que fueron recogidos. Sólo en el caso de que sean conservados para un interés público, para fines históricos, científicos o estadísticos podrá ampliarse el tiempo[112].

6. El *principio de seguridad de los datos* evita efectos adversos para los interesados. Para ello habrá de adoptarse medidas de naturaleza técnica u organizativa que permitan garantizar la seguridad. Para asegurar que las medidas adoptadas sean las apropiadas, la nueva regulación considera que deberán concretarse teniendo en cuenta las circunstancias de cada caso, optando por el diseño de medidas específicas para hacer frente a las distintas eventualidades que puedan surgir según el tipo de datos, sus fines, etc. Aunque en términos generales la *seudonimización* se considera un proceso técnico genérico que pueda garantizar la seguridad de los datos en la mayoría de los casos[113].

7. El *principio de responsabilidad* supone desarrollar una actitud proactiva del responsable y el encargado del tratamiento implantando medidas para promover y garantizar la protección de los datos en sus actividades de tratamiento. Los responsables deberán ser capaces de demostrar el cumplimiento de la normativa[114].

El RGPD concreta todos estos principios en su redacción al regular expresamente las condiciones en las que los datos habrán de ser tratados, señalando que deberán ser:

a) Tratados de manera lícita, leal y transparente en relación con el interesado.

b) Recogidos con fines determinados, explícitos y legítimos y no podrán ser tratados posteriormente para otros fines incompatibles con aquellos. En este caso, los fines de archivo en interés público, de investigación científica e histórica y fines estadísticos no se considerará incompatibles en virtud del art. 89 RGP.

---

[110] *Ibidem* p. 125.
[111] *Ibidem* p. 127.
[112] *Ibidem* p. 129.
[113] *Ibidem* p. 131.
[114] *Ibidem* p. 134.

c) Adecuados, pertinentes y limitados a lo necesario para los fines por los que son tratados (minimización de datos)

d) Exactos y actualizados, adoptando las medidas razonables para que se supriman o rectifiquen los inexactos.

e) Conservados por un plazo limitado de forma que permita la identificación de la persona por un tiempo no superior al necesario para los fines de tratamiento.

f) Conservados íntegros y de forma confidencial evitando el tratamiento no autorizado o ilícito, su perdida, destrucción o daño accidental[115].

d) Tratamientos de datos con un especial impacto sobre los datos sensibles: la elaboración de perfiles y la seudonimización

Como punto de partida debemos señalar que tanto el RGPD y la Directiva 680/2016 siguen considerando tratamiento «*cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción*»[116]. En todo caso, como viene sucediendo desde la Directiva 95/46/CE, la protección se extiende sobre cualquier tratamiento sea o no automatizado. Ahora bien, dentro del conjunto de acciones posibles la nueva legislación se refiere de forma explícita a dos nuevas formas de tratamiento, cuyo análisis resulta muy útil en nuestra opinión. Nos referimos a:

a) elaboración de perfiles de comportamiento, un concepto que se refiere a las operaciones automatizadas de tratamiento de datos utilizados para evaluar determinados aspectos personales del individuo, «(…) en particular *para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física*»[117].

De este modo, se garantiza el derecho del sujeto concernido a no ser objeto de una decisión fundada en el mero tratamiento automatizado de los datos, salvo que «a) sea necesario para el cumplimiento de un contrato; b) esté autorizado por el Derecho de la Unión o de un Estado miembro (…); c) se base en

[115] *Vid.* art. 5 del RGPD y art. 4 de la Directiva 680/2016.
[116] *Vid.* art. 4. 2) del RGPD y 3. 2) de la Directiva.
[117] *Vid.* art. 4. 4) del RGPD y 3. 4) de la Directiva 680/2016.

el consentimiento explícito del interesado». Su aplicación en los supuestos recogidos en el apartado a) y b) está sujeta a la necesidad de que el responsable del tratamiento adopte las medidas necesarias para proteger los derechos, libertades e intereses legítimos del sujeto, lo que se concreta jurídicamente en la previsión «(…) como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión»[118]. Se trata de garantizar, de este modo, un mínimo[119].

El riesgo intrínseco de este tipo de tratamiento de datos se ve más claramente en el contexto de la prevención y seguimiento de los delitos. Por ello, el art. 11 de la Directiva 680/2016 dispone que los Estados deben contemplar la prohibición de adoptar toda decisión basada exclusivamente en el resultado de una acción de tratamiento automático de los datos, como pueda ser la *elaboración de perfiles*, cuando produzca efectos legales adversos al sujeto. Como mínimo, mantiene el precepto, deberá preverse el derecho del sujeto a que haya intervención humana por parte del responsable del tratamiento y/o el derecho a impugnar la decisión. En ningún caso, continua el precepto, estas decisiones no podrán basarse en las *categorías especiales de datos*, entre las que se encuentran los datos religiosos. Sólo se admite excepciones a esta regla general cuando «(…) *se hayan tomado las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado*». Por que, concluye el párrafo 3, la *elaboración de perfiles* basada en categorías especiales de datos que dé lugar a una discriminación de las personas físicas quedará proscrita por el Derecho de la Unión[120], salvo que el interesado preste su consentimiento, no exista la prohibición de dicha actividad en el Derecho de la Unión o nacional y se hayan tomado las medidas adecuadas para salvaguardar los derechos, libertades e intereses legítimos de la persona.

Para garantizar los derechos de las personas en el tratamiento que supone la elaboración de perfiles resulta imprescindible, señala Garriga, que se aplique de forma escrupulosa el *principio de calidad de los datos* y el *principio de transparencia*, facilitando siempre al interesado una información sencilla, en lenguaje claro y accesible del tratamiento que se va a desarrollar y las consecuencias que este supone[121].

b) seudonimización: supone el tratamiento de los datos de una persona de tal manera que no puedan atribuirse al interesado sin utilizar información adicional. Para ello, la información adicional debe figurar por separado y debe estar sujeta a

---

[118] *Vid.* art. 22 del RGPD.

[119] Fernández Villazón, Luis Antonio, «El nuevo Reglamento Europeo…», *op. cit.*, *Vid.* p. 400.

[120] *Vid.* art. 11 de la Directiva 680/2016.

[121] Garriga Domínguez, Ana, «La elaboración de perfiles y…», *op. cit.*, *Vid.* p. 133 y 134.

las medidas técnicas y organizativas adecuadas para garantizar que esos datos no se puedan atribuir a una persona identificada o que pueda ser identificable[122].

Estos datos, aunque *seudonimizados*, pueden llegar a considerarse información sobre una persona identificable, ya que aplicando los medios y técnicas adecuados podría revelarse la identidad de la persona. Para determinar el grado y alcance de que esa posibilidad sea real deberá valorarse los medios y procedimientos que se puedan utilizar para identificar al titular de esos datos, como por ejemplo la singularización, y para comprobar la viabilidad de esos medios debe tenerse en cuenta factores como el costo y tiempo necesario para concretar la identificación, especialmente teniendo en cuenta la tecnología disponible en el momento del tratamiento[123].

e) El consentimiento: la pieza clave del sistema

Según las definiciones ofrecidas por la normativa, el consentimiento será «*toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen*»[124]. Para considerar que el sujeto tiene la capacidad para emitirlo será necesario que tenga, como mínimo, 16 años de edad y en el caso de que el sujeto concernido sea menor de esta edad, el consentimiento solo se considerará lícito cuando lo emita el titular de la patria potestad o tutela del menor «y solo en la medida en que se dio o autorizó»[125].

Formal y materialmente tanto los términos en los que se solícita como la totalidad del procedimiento por el que se requiere el consentimiento habrán de ser claro y sencillo. Para ello la solicitud habrá de ser concisa y tratando de evitar que su complejidad suponga la innecesaria perturbación del uso del servicio para el que dicho consentimiento es requerido[126]. Teniendo en cuanto las capacidades y uso de las nuevas tecnologías, el propio RGPD prevé que el consentimiento pueda ser emitido electrónicamente a través de «tick box» o «casillas» y, desde su preámbulo, el RGPD avisa que el responsable del tratamiento no puede utilizar el silencio, casillas preseleccionadas o la misma inactividad para probar la existencia de consentimiento[127]. Este elemento puede resultarnos útil para nuestro objeto ya que, dadas las circunstancias actuales como la im-

[122] *Vid.* art. 4. 5) del RGPD y 3. 5) de la Directiva 680/2016.
[123] *Vid.* párrafo 26 del preámbulo del RGPD.
[124] *Vid.* art. 4. 11) del RGPD.
[125] *Vid.* art. 8 del RGPD.
[126] *Vid.* apartado 32 del preámbulo del RGPD.
[127] *Vid.* apartado 32 del preámbulo del RGPD.

plantación de la administración electrónica y la necesaria digitalización del RER según las propias previsiones del RD 594/2015, debemos tener en cuenta que el consentimiento podrá ser requerido y prestado a través de formularios electrónicos. En todo caso, a diferencia de la anterior Directiva 95/46/EC que permitía el consentimiento implícito y la emisión opcional bajo determinadas circunstancias, el tratamiento no podrá continuar a menos que el sujeto concernido haya emitido el consentimiento expresamente y para cada una de las acciones que se vayan a llevar a cabo. Por último, como pudimos ver en los derechos otorgados por el RGPD, el consentimiento puede ser retirado por el sujeto interesado, para lo que el RGPD exige al responsable del tratamiento que se realice a través de un procedimiento tan sencillo como el establecido para prestarlo[128].

La existencia y solicitud de consentimiento válido e inequívoco como requisito imprescindible para el tratamiento de los datos requiere la participación del sujeto concernido y del responsable del tratamiento[129]. Aunque solo fuera desde una perspectiva general, la interposición de una solicitud de consentimiento expresa la voluntariedad del sujeto, garantiza su derecho de uso y control y como señala la doctrina, facilita al sujeto tiempo, como mínimo, para tomar la decisión y pensar activamente sobre las consecuencias de su emisión[130]. Por lo que se refiere al responsable del tratamiento la solicitud de consentimiento le permite informar al sujeto concernido de todas las circunstancias necesarias (finalidades, derechos, garantías, etc.). Pero además debemos tener en cuenta que el responsable debe ser capaz de demostrar que el sujeto concernido lo ha prestado, por lo que le supone adoptar una posición activa. Esta obligación será la que impida que algunas prácticas aceptadas hasta el momento se mantengan, como por ejemplo entender que la mera inactividad del sujeto supone que consiente, siendo ahora necesario que en todos los casos la emisión del consentimiento sea explícita[131].

La importancia de esta nueva característica –ser explícito– es sustancial. Desde la misma propuesta de Reglamento la doctrina ponía de manifiesto la importancia y consecuencias de optar por la condición de explícito como elemento que caracterice al consentimiento en esta nueva regulación, evitando que se faciliten diversas interpretaciones sobre la ambigüedad del consentimiento en cada uno de los Estados y afianzar la responsabilidad del encargado del trata-

[128] *Vid.* art. 7. 3 del RGPD.

[129] *Vid.* art. 7 del RGPD.

[130] Schermer, Bart W.; Custers, Bart & Van Der Hof, Simone, «The crisis of consent: how stronger legal protection may lead to weaker consent in data protection», *Ethics Inf Technol* (2014) 16, pp. 171 a 182, *Vid.* p. 172.

[131] Fernández Villazón, Luis Antonio, «El nuevo Reglamento Europeo…», *op. cit.*, *Vid.* p. 399.

miento[132]. Y es que, como sostienen Schermer, Custers y Van Der Hof, la diferencia entre consentimiento explícito y la anterior condición –inequívoco– será el hecho de que su necesaria explicitación hará que el acto de consentir se concentre en manifestar/explicitar el consentimiento, para lo que el responsable del tratamiento deberá cumplir con sus obligaciones y presentar a los sujetos concernidos un modo de prestarlo, una propuesta sobre cuál será el uso o finalidad de la revelación particular que se hará de su información personal, teniendo la obligación los sujetos concernidos de responder activamente aceptando o rechazando esa solicitud, para lo que tendrán en cuenta todos esos datos. Bajo está idea subyace la necesidad y procedencia de adoptar y plasmar la decisión de forma más activa y afirmativa cuando se requiera el consentimiento para tratar aquellas categorías especiales de datos, como son los que revelan la ideología o religión.

Es por ello que, siguiendo a los autores citados, resulta conveniente proponer que la existencia de consentimiento explícito se conecte con la necesidad de firmar y presentar un formulario de consentimiento en el que se determinará los diferentes objetivos y fines del tratamiento, así como los datos personales que vayan a ser tratados[133].

f) La condición de sujeto, de responsable y de encargado del tratamiento: derechos y obligaciones

Los sujetos intervinientes básicos en el proceso de tratamiento de los datos son: el sujeto concernido, el responsable y el encargado del tratamiento, pues serán ellos los que ostentarán los derechos y asumirán las obligaciones fijadas por el RGPD para garantizar un ejercicio pleno del derecho. En cuanto a los conceptos que maneja la nueva regulación encontramos las siguientes definiciones:

a) el *sujeto de los datos* podrá serlo toda persona natural identificada o identificable, sin restricciones en cuanto a la nacionalidad pero, en este caso, quedando excluidas las personas jurídicas[134].

b) el *responsable del tratamiento* no solo será toda persona natural, sino que también incluye a las personas jurídicas, autoridad pública o agencia que,

---

[132] *Vid.* Reding, Viviane, «The European data protection framework for the twenty-first century», *International Data Privacy Law*, 2012, Vol. 2, n.º 3, pp. 119 a 129, *Vid.* p. 124.

[133] Schermer, Bart W.; Custers, Bart & Van Der Hof, Simone, «The crisis of consent: how stronger legal protection may lead to weaker consent in data protection», Ethics Inf Technol (2014) 16, pp.171-182, *Vid.* p. 175.

[134] *Vid.* art. 4. 13) del RGPD y art. 3. 12) de la Directiva 680/2016.

de manera individual o junto con otros, *determine los fines y los medios para llevar a cabo el procesamiento* de los datos[135].

c) en el mismo sentido el *encargado del tratamiento* incluye toda persona física o jurídica, autoridad pública, agencia u órgano que procesa la información y datos en nombre del responsable del tratamiento[136].

d) por último, parece interesante describir el concepto de *destinatario*, que se identifica en el contexto de la Directiva 680/2016 y se refiere a la persona física, jurídica, autoridad pública, servicio o cualquier otro organismo al que se comunican los datos. De este rango de sujeto quedarán excluidas aquellas autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta[137].

Por lo tanto, la persona física a la que se refieran los datos recogidos y tratados será el sujeto y, como tal, asume la posición de titular de los derechos garantizados por ambas normativas para facilitar su poder de uso y control. Por su parte, el responsable y el encargado del tratamiento serán los que desarrollarán las actividades propias del tratamiento o procesamiento de los datos y, como parte de las garantías activas, deberán cumplir con las correlativas obligaciones que implican los derechos concedidos al sujeto, para de este modo garantizar que el ejercicio de estos derechos es pleno. La nueva regulación las determina en el Capítulo IV del RGPD. Para conocer el contenido de ambas cuestiones comenzaremos por el haz de facultades (derechos) en el que el nuevo RGPD concreta *el derecho de acceso y control a los datos* y que confiere al sujeto concernido. Estos son:

— Primero, *el derecho de acceso*, según el cual podemos asegurar que el sujeto tiene *derecho a recibir confirmación, por parte del responsable del tratamiento, de si sus datos personales están siendo procesados o no* y, en el caso de que tal tratamiento se esté llevando a cabo, el sujeto *tiene derecho a ser informado de*:

a) la finalidad y base jurídica de su tratamiento;

b) las categorías de datos personales que están siendo tratados y cualquier información sobre su origen;

---

[135] *Vid.* art. 4. 7) del RGPD y el art. 3. 8) de la Directiva 680/2016. En el caso de la *Directiva 680/2016*, además, se utiliza el término *autoridad competente*, con el que se refiere a toda autoridad pública que tenga la competencia para la prevención, investigación, detección y enjuiciamiento de delitos o ejecución de penas o cualquier otra entidad a la que el ordenamiento jurídico del Estado miembro otorgue la competencia y los poderes para realizar esas actividades, *Vid.* el art. 3. 7) de la Directiva 680/2016.

[136] *Vid.* art. 4. 8) del RGPD y art. 3. 9) de la Directiva 680/2016.

[137] *Vid.* art. 3. 10) de la Directiva 680/2016.

c) a quienes han sido comunicados/transmitidos sus datos, especialmente cuando los destinatarios sean o estén establecidos en terceros Estados o en organizaciones internacionales;

d) el plazo de conservación de los datos y los criterios utilizados para determinar ese plazo;

e) el derecho a solicitar del responsable la rectificación o supresión de los datos, la limitación de sus tratamiento u oponerse a su tratamiento;

f) su derecho a presentar una reclamación ante la autoridad de control;

g) su derecho a recibir cualquier información sobre el origen de los datos cuando estos no hayan sido obtenidos del interesado;

h) si se han adoptado decisiones automatizadas, incluida la elaboración de los perfiles, la lógica aplicada para adoptar esa decisión, así como la importancia y consecuencias previstas de dicho tratamiento[138]. Respecto a este último elemento, como previsión general garantizada por el art. 22 del RGPD, recordemos que «(…) el interesado tiene derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, (…)» salvo cuando:

> «*a)* es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento;
>
> *b)* está autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o
>
> *c)* se basa en el consentimiento explicito del interesado.»

En los casos a) y c) el responsable adoptará las medidas adecuadas para proteger los derechos, libertades e intereses legítimos del interesado, que incluirá como mínimo el derecho a obtener intervención humana, a expresar su punto de vista e impugnar la decisión[139].

En el mismo sentido se pronuncia la Directiva 680/2016 poniendo el foco en las categorías especiales de datos personales, que no podrán ser el fundamento de una decisión de este tipo «(…) salvo que se hayan tomado las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado». La Directiva prohíbe, en todo caso, la elaboración de perfiles que dé lugar a una discriminación de la persona basándose en las cate-

[138] *Vid.* art. 14 de la Directiva 680/2016 y art. 15 del RGPD.
[139] Todo ello en art. 22 del RGPD.

gorías especiales de datos personales[140] reconociendo, de este modo, la posibilidad de que tal «tratamiento de la información» puede tener efectos discriminatorios inherentes. Así la garantía de la protección que concede el derecho no solo se extiende al momento en el que se produce la recogida y uso de esos datos, sino que se proyecta *a posteriori* frente el potencial riesgo que esta práctica puede tener en la elaboración de perfiles genéricos o de evaluaciones de personas o grupos de personas que comparten esas características[141].

La Ley podrá (deberá) prever las excepciones que permiten la restricción de este *derecho de acceso* y, como se viene repitiendo desde los primeros textos internacionales, habrán de ser medidas necesarias en toda sociedad democrática, que respeten los derechos y libertades de la persona concernida y dirigidas a evitar:

a) que se obstruya una investigación, procedimientos oficiales o judiciales o indagaciones;

b) que se cause un perjuicio a la prevención, detección, investigación o enjuiciamiento de infracciones penales;

c) que se vea afectada la seguridad nacional, la seguridad pública y los derechos y libertades de terceras personas[142].

— Segundo, el *derecho de rectificación* consiste en el derecho del interesado a obtener sin dilación indebida la rectificación por parte del responsable del tratamiento de los datos personales que resulten inexactos. Cuando estos datos sean incompletos, el interesado tendrá derecho, en virtud del RGPD, a que se completen, incluso mediante una declaración adicional. En el caso de las actividades de tratamiento realizadas con el fin de prevenir, perseguir, etc. actividades delictivas, incluidas dentro del ámbito de protección de la Directiva 680/2016, el responsable del tratamiento podrá restringir su tratamiento en lugar de borrarlos, cuando: a) no pueda determinarse la exactitud o inexactitud de los datos puesta en duda por el sujeto; b) cuando estos datos deban conservarse a efectos probatorios[143].

En todo caso, este *derecho de rectificación* podrá ser limitado a través de una Ley, siempre y cuando las medidas adoptadas sean necesarias en todo sociedad democrática, respeten los derechos y libertades de la persona concernida y estén dirigidas a evitar: a) que se obstruya una investigación, procedimien-

[140] *Vid.* art. 11 de la Directiva 680/2016.
[141] Mcdermott, Yvonne, «Conceptualising the right to data protection…», *op. cit.*, *Vid.* p. 4.
[142] *Vid.* art. 15 de la Directiva 680/2016.
[143] *Vid.* arts. 16 del RGPD y de la Directiva 680/2016.

tos oficiales o judiciales o indagaciones; b) que se cause un perjuicio a la prevención, detección, investigación o enjuiciamiento de infracciones penales; c) que se vea afectada la seguridad nacional, la seguridad pública y los derechos y libertades de terceras personas[144].

— Tercero, el *derecho de supresión o derecho de olvido*[145]: que concede al sujeto el derecho a que el responsable borre sus datos cuando:

a) ya no sean necesarios para los fines que fueron recabados;

b) el sujeto haya retirado su consentimiento o se oponga al tratamiento y no existan otros motivos que justifiquen su mantenimiento;

c) hayan sido tratados ilícitamente;

d) deban suprimirse para el cumplimiento de una obligación legal[146].

En todo caso, este derecho y sus condiciones no se aplicará cuando la finalidad del tratamiento sea:

a) el ejercicio de la libertad de expresión o información;

b) el cumplimento de una obligación legal impuesta por el Derecho de la Unión o de los Estados miembro que lo requiera;

c) razones de interés público en el ámbito de la salud pública;

d) para fines de archivo en interés público, de investigación científica, histórica o fines estadísticos;

e) para la formulación, el ejercicio o la defensa de reclamaciones[147].

Teniendo en cuenta lo dicho, resulta interesante concluir con Polčák que «mientras las razones para justificar el borrado se basan completamente en factores personales (por ejemplo, la voluntad de la persona respectiva, antes referida como sujeto de los datos) los motivos para la persistencia de los datos personales están relacionados con consideraciones generales como la necesidad de procesar los datos con fines históricos, la libertad de información o el tratamiento de los datos en el área de la salud pública»[148].

---

[144] *Vid.* art. 16.4 de la Directiva 680/2016.

[145] *Vid.* Case C-131/12, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos. *Vid.* KROPF, J. W., «Personal data –protection of individual privacy– right to be forgoten –responsibility of Internet search engine operators– European data protection Directive 95/46/C», *The American Journal of International Law*, Vol. 108, 2014, pp. 502 a 509.

[146] *Vid.* art. 17 del RGPD.

[147] *Vid.* art. 17. 3 del RGPD.

[148] POLČÁK, Radim, «Getting European data protection…», *op. cit.*, *Vid.* p. 284 –la traducción es del autor–.

— Cuarto, el *derecho a la limitación en el tratamiento de los datos*, que concede el derecho de la persona concernida a que se límite por parte del responsable el tratamiento de los datos cuando se cumpla alguna de estas condiciones:

a) el sujeto haya impugnado la exactitud de los datos. Esta limitación se extenderá durante el plazo en el que se realice la verificación por parte del responsable del tratamiento;

b) el tratamiento sea ilícito y el sujeto en lugar de optar por la supresión de los datos solicite la limitación de su uso;

c) ya no sean necesarios para los fines del tratamiento pero el sujeto interesado los necesite para formular, ejercer o defender sus reclamaciones;

d) cuando se haya ejercido el derecho de oposición y solo durante el plazo en el que se verifica si los intereses legítimos del responsable prevalecen sobre los del sujeto concernido[149].

Tanto en la rectificación como en la supresión o limitación del uso de los datos, el responsable del tratamiento será el responsable de comunicarlo a los destinatarios de su cesión o comunicación para que el tratamiento se adecue a las consecuencias del ejercicio de esos derechos, «(…) salvo que sea imposible o exija un esfuerzo desproporcionado». Por su parte, también está obligado a informar al interesado de quienes son esos destinatarios, «(…) si este así lo solicita»[150].

— Quinto, el *derecho a la portabilidad de los datos* que incluye el derecho del sujeto a recibir, del responsable que los estuviera tratando, sus datos personales en un formato estructurado, de uso común y lectura mecánica para poder transmitirlos a otro responsable. Al ejercer la portabilidad, el interesado también tendrá el derecho a que los datos sean transmitidos de responsable a responsable del tratamiento, sin necesidad de que sea él el encargado de realizar la transacción. Este derecho podrá ejercerse sin que afecte negativamente a los derechos y libertades de otros[151].

— Sexto, el *derecho de oposición*, según el cual el sujeto concernido, por motivos relacionados con su situación personal, podrá oponerse al tratamiento

[149] *Vid.* art. 18 del RGPD.

[150] *Vid.* art. 19 del RGPD.

[151] *Vid.* art. 20 del RGPD. Sobre el *derecho portabilidad Vid.* Fernández Villazón, Luis Antonio., «El nuevo Reglamento Europeo…», *op. cit.*, *Vid.* p. 401.

de sus datos, incluida la elaboración de perfiles y, dentro de ellos, cuando estos perfiles se compongan con objeto de mercadotecnia directa[152].

Además de las expresamente previstas para los *derechos de acceso* y *rectificación* en el marco de las actividades desarrolladas para la prevención, persecución, etc. de acciones penales, que hemos visto con anterioridad, todos los derechos que hemos analizado están sujetos a las limitaciones previstas de forma genérica para todos ello en el RGPD. Todas ellas habrán de cumplir con las condiciones previstas al determinar los límites: deberán estar contenidas en la Ley, deben respetar los derechos y libertades del sujeto y deben ser necesarias y proporcionales en una sociedad democrática para salvaguardar: «a) la seguridad del Estado; b) la defensa; c) la seguridad pública; d) la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluida la protección frente a amenazas a la seguridad pública y su prevención; e) otros objetivos importantes de interés público general de la Unión o de un Estado miembro, en particular un interés económico o financiero importante de la Unión o de un Estado miembro, inclusive en los ámbitos fiscal, presupuestario y monetario, la sanidad pública y la seguridad social; f) la protección de la independencia judicial y de los procedimientos judiciales; g) la prevención, la investigación, la detección y el enjuiciamiento de infracciones de normas deontológicas en las profesiones reguladas; h) una función de supervisión, inspección o reglamentación vinculada, incluso ocasionalmente, con el ejercicio de la autoridad pública en los casos contemplados en las letras a) a e) y g); i) la protección del interesado o de los derechos y libertades de otros; j) la ejecución de demandas civiles»[153].

Este conjunto de derechos supone una serie de obligaciones correlativas que recaen sobre el responsable y encargado del tratamiento. Tanto el RGPD como de la Directiva 680/2016 consideran necesario implementar las medidas técnicas y organizativas adecuadas que permitan asegurar y demostrar que el tratamiento es adecuado conforme a la normativa[154]. Tradicionalmente, este concepto de medidas de seguridad apropiadas ha sido considerado abierto e indefinido por la normativa para la protección de los datos personales, de tal modo que a través de ellas pudieran incluirse todo tipo de reglas y actuaciones que fueran dirigidas a evitar la perdida accidental, la alteración, la difusión o el

[152] *Vid.* art. 21 del RGPD.
[153] *Vid.* art. 23 del RGPD.
[154] *Vid.* art. 24. 1 del RGPD y art. 19 de la Directiva 680/2016.

acceso no autorizado de los datos[155]. En la actualidad, tanto el RGPD como la Directiva 680/2016 han concretado un conjunto de medidas que pueden servir de orientación. Por ejemplo, cuando la Directiva 680/2016 se refiere a las obligaciones en las que se puede materializar la responsabilidad asumida por responsable y encargado del tratamiento prevé:

a) Implementar medidas técnicas y organizativas, como la *seudonimización* y *minimización* de manera eficiente y con las garantías suficientes para cumplir los requisitos de la Directiva y proteger los derechos de la persona concernida[156].

b) Utilizar solo *encargados del tratamiento* que proporcionen las garantías suficientes de que implementarán las medidas técnicas adecuadas para que el tratamiento cumpla con los requisitos establecidos en la Directiva y no involucrar a otros *encargados del tratamiento* sin contar con la autorización por escrito previa, específica o general, del responsable del tratamiento[157].

c) Mantener un registro (archivo) de todas las categorías de actividades de tratamiento desarrolladas bajo su responsabilidad[158].

d) Cooperar con la autoridad supervisora en el desempeño de sus tareas[159].

e) Llevar a cabo una evaluación previa al tratamiento del impacto que las operaciones de tratamiento previstas puedan tener sobre el derecho de las personas, cuando el tratamiento suponga probablemente un elevado riesgo para los derechos de las personas[160].

f) Comunicar la violación de la seguridad los datos personales[161], tanto a la autoridad supervisora[162] como a los sujetos concernidos[163]. Esta autoridad supervisora será[164] una autoridad pública independiente establecida por el Estado miembro de acuerdo con las previsiones correspondientes[165].

---

[155] Martín Sánchez, María del Mar, «Tecnología informática y confidencialidad …», *op. cit.*, *Vid.* p. 156.

[156] *Vid.* art. 20 de la Directiva 680/2016.

[157] *Vid.* art. 22 de la Directiva 680/2016.

[158] *Vid.* art. 24 de la Directiva 680/2016.

[159] *Vid.* art. 24 de la Directiva 680/2016.

[160] *Vid.* art. 27 de la Directiva 680/2016.

[161] Con ella la normativa se refiera a «toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita, o la comunicación o acceso no autorizados a datos personales transmitidos, conservados o tratados de otra forma», *Vid.* art. 4. 12) del RGPD y art. 3. 11) de la Directiva 680/2016.

[162] *Vid.* art. 30 de la Directiva 680/2016.

[163] *Vid.* art. 31 de la Directiva 680/2016.

[164] *Vid.* art. 3. 15) de la Directiva 680/2016.

[165] En este caso art. 51 del RGPD y 41 de la Directiva 680/2016.

e) que los Estados dispongan en sus legislaciones la obligación de que el responsable y el encargado del tratamiento implementen medidas técnicas y organizativas adecuadas para garantizar un nivel de seguridad adecuado al riesgo, especialmente para el tratamiento de categorías especiales de datos. Por ejemplo, en el caso del tratamiento automatizado se prevé la necesidad de asegurar un adecuado control del acceso a los equipamientos, a los soportes de los datos, a su almacenamiento, a usuarios no autorizados, a datos no autorizados, a su transmisión y introducción, al tiempo que medidas para asegurar la integridad de los datos (para evitar que sean degradados por fallos en el sistema)[166].

Sin perjuicio de que las referidas específicamente en el RGPD serán tratadas de forma más pormenorizada al definir el sistema establecido por la actual legislación promulgada en España, podemos afirmar, tras lo visto hasta ahora y siguiendo a Fernández Villazón, que partimos de un sistema en el que la actuación de los responsables y controladores de los datos se desarrolla bajo el principio de *responsabilidad proactiva*, por lo que «los encargados y responsables del tratamiento asumen un mayor control y capacidad de decisión sobre la protección de los datos personales que tratan, pero esa libertad se compensa con la obligación de acreditar todas las medidas de protección y control que adopten (para probar que se han hecho) y con una fuerte responsabilidad»[167]. Esta es la razón por la que, en su opinión, el RGPD diseña un sistema de protección que realza la conveniencia de elaborar códigos de conducta supervisados y, por otro lado, en un *sistema de certificación, sellos y marca*[168] que permitan acreditar la viabilidad y funcionamiento de las medidas adoptadas.

Junto a este cambio de orientación conviene destacar, también en el contexto del RGPD, que se ha introducido un elemento de carácter preventivo que asegura la puesta en marcha de esa responsabilidad proactiva por parte de quien llevará a cabo el tratamiento: el *principio de protección de datos desde el diseño y por defecto* que supone la obligación para el responsable del tratamiento de diseñar las estrategias de actuación para garantizar el tratamiento desde el inicio mismo del proceso[169].

---

[166] *Vid.* art. 29 de la Directiva 680/2016.
[167] FERNÁNDEZ VILLAZÓN, Luís Antonio, «El nuevo Reglamento Europeo…», *op. cit.*, *Vid.* p. 402.
[168] *Ibídem Vid.* p. 403.
[169] *Ibídem.*

2.4 Elementos jurídicos propios para diseñar un sistema de protección de los datos religiosos extraíbles del desarrollo legislativo español

Gran parte del desarrollo normativo de este derecho en España se ha enfocado en concretar la dimensión pasiva y activa del derecho: la primera, fijando las medidas y garantías necesarias para evitar la injerencia de terceros en la privacidad de la persona, su autonomía y el resto de sus derechos, en lo que se refiere a las consecuencias que sobre ellos pueda suponer la tenencia y uso de sus datos y, la segunda, definiendo aquellas garantías que preservan su capacidad de disposición plena, tanto las que se refieren a las facultades que corresponden al sujeto concernido como las correlativas responsabilidades de quienes tratan los datos, ambas como dos caras de una misma moneda imprescindible para asegurar el pleno disfrute del derecho.

La primera Ley que desarrolló el art. 18.4 CE fue la *Ley 5/1992 de regulación del tratamiento automatizado de datos de carácter personal*[170] (en adelante LORTAD)[171]. Sus previsiones muestran la notable influencia que tuvo sobre su redacción el *Convenio 108* del que, además de asumir los aspectos generales, utilizó como referencia para concretar la regulación de los datos sensibles. Antes de analizar su contenido nos interesa poner de manifiesto un elemento que puede resultar útil a nuestros efectos. Al delimitar los campos de aplicación, el *Convenio 108* recoge la posibilidad de que los Estados parte puedan extender sus garantías a personas jurídicas, lo cual requiere una declaración dirigida al Secretario General del Consejo de Europa, donde se deje constancia de que «(…) *aplicará el presente Convenio, asimismo, a informaciones relativas a agrupaciones, asociaciones, fundaciones, sociedades, compañías o cualquier otro organismo compuesto directa o indirectamente de personas físicas, tengan o no personalidad jurídica*»[172]. Esta posibilidad no pasó desapercibida para el legislador español. No en vano, como ya pusiera de manifiesto el profesor Pérez Luño, el proyecto de LORTAD preveía la posibilidad de extender su régimen de protección a las personas jurídicas. En palabras del autor «(…) a medida que el proceso de datos se proyecta a las empresas, a las instituciones y asociaciones, se hace cada vez más evidente la conveniencia de no excluir a las personas jurídicas del régimen de protección que impida o repare los daños causados por la utilización indebida de informaciones que les conciernen. En efecto, la defensa de la intimidad y los demás derechos fundamentales no es privativa de los indi-

[170] Publicada en el *BOE* n.º 262, de 31 de octubre de 1992.

[171] Para un mayor desarrollo de la LORTAD *Vid.* Pérez Luño, Antonio Enrique, *Manual de informática y Derecho*, Ariel,1996, *Vid.* pp.47 y ss.

[172] *Vid.* art. 3. 2 b) del *Convenio 108*.

viduos, sino que debe proyectarse a las formaciones sociales en las que los seres humanos desarrollan plenamente su personalidad»[173]. A pesar de ello, finalmente no se llevó a cabo, más bien se optó por la posición contraria, excluir a las personas jurídicas, posición que fue refrendada por la Directiva 46/95/CE[174] y se mantiene en la actualidad, como hemos podido comprobar al analizar el RGPD y veremos en la nueva legislación española.

Pues bien, la propia LORTAD ya diseñaba un modelo de protección que debía desplegarse desde una perspectiva dinámica o funcional, no solo estática. Es así como la tutela que desplegaba esta Ley trascendió el mero depósito y conservación de los datos y, como señalaba su exposición de motivos, se extendió sobre todos aquellos procesos o aplicaciones de los datos que si se llegaban a conectar entre sí seran susceptibles de configurar *un perfil personal* del sujeto concernido que, incluso, podría ser utilizado para valorar actividades públicas o privadas en las que participara. De este modo, concluye el profesor Pérez Luño, la LORTAD se propuso «tutelar la calidad de los datos, pero no en sí mismos, sino en función de evitar que su informatización permita o propicie actividades discriminatorias»[175].

Los datos que revelan las convicciones ideológicas y religiosas de la persona –entre otras cuestiones– eran tratados por el art. 7 de la LORTAD como *datos especialmente protegidos*. Tomando como referencia la previsión constitucional contenida en el art. 16.2 CE sobre la protección de la libertad ideológica y religiosa, este precepto recordaba que *nadie podría estar obligado a declarar sobre sus convicciones religiosas,* siendo el sujeto concernido libre para optar entre facilitar o no esos datos. Desde esa voluntariedad inicial, alineada con el contenido esencial de la libertad religiosa, se construye un régimen de protección especial cuyas características esenciales se mantendrán desde ese momento en casi todas las regulaciones posteriores, a veces con algunas matizaciones. Grosso modo esas características son: a) la determinación de la forma en que la voluntad –consentimiento– debe ser emitida: de forma clara y nítida o, en los términos en los que aparece expresado en la norma, el consentimiento habrá de ser *expreso y por escrito;* b) la obligación de quien trate los datos de recordar al sujeto su derecho a no prestarlo y, en todo caso, la responsabilidad de poder probar que dispone del consentimiento. Se completa

[173] PÉREZ LUÑO, Antonio Enrique, «El concepto de interesado…», *op. cit.*, *Vid.* p. 19.

[174] Incluso a pesar de las reformas penales efectuadas en España en materia de protección del derecho de honor de las personas jurídicas, que parecían constituir un fundamento para corregir esta carencia. Sobre todo ello *ibídem*, *Vid.* p. 19 y 20.

[175] Todo en PEREZ LUÑO, Antonio Enrique, «La tutela de la libertad informática…», *op. cit.*, *Vid.* p. 65.

este régimen específico diseñado por la LORTAD para proteger los datos religiosos con la prohibición expresa de crear ficheros con la *finalidad exclusiva de almacenar datos personales que revelen la ideología, religión, creencias*.

Algo muy específico de esta norma fue que su artículo 2 excluía de su ámbito de aplicación los *ficheros mantenidos por iglesias, confesiones y comunidades religiosas* (junto con los partidos políticos y sindicatos), cuando los datos que en ellos obraran se refirieran a sus *miembros* o *exmiembros*. Este exclusión queda matizada cuando se refiera a la cesión de estos datos, que según el mismo precepto deberá ajustarse a los términos prescritos en el art. 11 de la LORTAD. En este último artículo se prevé que solo podrán ser cedidos para el *cumplimiento de los fines directamente relacionados con las funciones legítimas del cedente y del cesionario* e incluso podrá omitirse la necesidad de consentimiento expreso cuando: a) una Ley que estableciera las garantías necesarias previera otra cosa; b) estos hubieran sido obtenidos de fuentes accesibles al público; c) el establecimiento del fichero respondiera a una libre y legítima aceptación de una relación jurídica que implique la conexión con otro fichero. En todo caso, *el consentimiento para la cesión de los datos era revocable y el cesionario se obligaba a observar las disposiciones previstas en la Ley*. Cierto es que esta exclusión desaparece en las normas sucesivas, pero en nuestra opinión su fundamento tiene una notable importancia que perdura en las sucesivas legislaciones: existe una relación específica entre la persona y la entidad basada en los elementos que configuran su identidad y que se construye sobre la base de la autonomía tanto de la persona como de las propias entidades religiosas, esta relación implica su voluntad de pertenecer a ella y presupone la de ceder sus datos. Por ello se considera que la voluntad de pertenecer a una confesión conlleva la existencia de un consentimiento tácito para que sus datos sean incluidos dentro de los ficheros internos y de organización de la entidad. En las siguientes leyes veremos como dicha característica se transforma y de ser una cláusula de exclusión se convertirá en una circunstancia que permite minorar la rigidez de las condiciones que debe reunir el consentimiento del sujeto para la recogida de los datos sensibles, pero no excluye la necesidad de mantener una adecuada garantía de los datos. En todo caso, esta disminución del rigor no se aplica de la misma forma en el caso de intercambio o cesión, en los que el consentimiento mantiene la misma necesidad de cumplir con las condiciones generales establecidas[176].

[176] En ese sentido, el legislador no rehuía las posibles necesidades adicionales de protección que pudieran derivarse del tráfico de estos datos y advertía que a pesar de la exclusión de este tipo de archivos de su ámbito de aplicación su cesión debía ajustarse a la aplicación de lo dispuesto en sus artículos 7 y 11, *Vid.* artículo 2 LORTAD: «*2. El régimen de protección de los datos de carác-*

Siete años después, el legislador español modifica su régimen interno sustituyendo la LORTAD por *Ley Orgánica* 15/1999, de 13 de diciembre, *de Protección de Datos*[177] (en adelante LOPD 1999), encargada de trasponer la Directiva 95/46/CE al ordenamiento jurídico español. Esta Ley fue desarrollada por el *Real Decreto 1720/2007*, de 21 de diciembre[178]. Como consecuencia de su necesaria adhesión a los requisitos jurídicos establecidos por la Directiva, la LOPD ofrece un modelo de protección que se extiende más allá del tratamiento automatizado, al que por su denominación y los términos en los que se expresaba en la redacción de la mayoría de sus preceptos (utilizando el término automatizado), parecía circunscribirse la LORTAD[179]. La *calidad de los datos*[180] se sitúa como principio clave del tratamiento de los datos –sean o no sensibles–. Para alcanzarlo, los datos deben ser exactos y actualizados, de tal modo que respondan a la realidad del afectado[181]. Cuando se considere que son inexactos o incompletos deberán ser cancelados, sustituidos, modificados o completados de oficio o por el afectado, en los términos previstos en el art. 16 LOPD 1999[182]. Y, salvo que sean cancelados, serán conservados de forma que permitan el ejercicio del derecho de acceso por parte del sujeto concernido[183]. Pero la caracterización del régimen previsto en este norma no se detiene ahí. La norma conjuga el *principio de calidad* con el de *legitimidad*, basado en la aceptación del tratamiento según su adecuación a los fines a los que se destina su recogida y tratamiento. Por ese motivo el precepto advierte que los datos solo podrán ser recogidos cuando sean pertinentes y no excesivos para el ámbito y fines para los que fueron recabados[184] y serán cancelados cuando hayan dejado de ser necesarios o pertinentes para esa finalidad[185]. Los datos que resulten cancelados, o que sean cancelables, no habrán de conservarse de forma que permitan la identificación del interesado más allá del periodo necesario para el cumplimiento de los fines por los que hubieran sido recabados[186]. Finalmente, la LOPD 1999 mantiene la garantía prevista des-

---

ter personal que se establece en la presente Ley no será de aplicación: (…) A los ficheros mantenidos por los partidos políticos, sindicatos e Iglesias, confesiones y comunidades religiosas en cuanto los datos se refieran a sus asociados o miembros y ex miembros, sin perjuicio de la cesión de los datos que queda sometida a lo dispuesto en el artículo 11 de esta Ley, salvo que resultara de aplicación el artículo 7 por tratarse de los datos personales en él contenidos».

177 Publicado en *BOE* n.º 298 de 14 de diciembre de 1999.

178 Publicado en *BOE* n.º 17 de 19 de enero de 2008.

179 *Vid.* ARENAS RAMIRO, Mónica, *El derecho fundamental a la protección…, op. cit., Vid.* p. 475.

180 *Vid.* art. 4 de la LOPD 1999.

181 *Vid.* art. 4.3 de la LOPD 1999.

182 *Vid.* art. 4.4 de la LOPD 1999.

183 *Vid.* art. 4.6 de la LOPD 1999.

184 *Vid.* art. 4.1 de la LOPD 1999.

185 *Vid.* art. 4.5 de la LOPD 1999.

186 *Vid.* art. 4.5 segundo párrafo de la LOPD 1999.

de el *Convenio 108* que impide el uso de esos datos para finalidades incompatibles con las que motivan su recogida, considerando compatibles fundamentalmente los fines históricos, estadísticos o científicos entre otros[187]. Aunque esta excepción en el mantenimiento íntegro de determinados datos justificada por su valor histórico, estadístico o científico se deberá desarrollar, de acuerdo con la legislación específica, a través de un Reglamento[188].

LOPD 1999 sitúa el consentimiento en el eje del tratamiento de los datos. Según el precepto de la norma este habrá de ser *inequívoco* y solo no será necesario cuando: a) una Ley disponga otra cosa; b) los datos se recojan por las Administraciones públicas para el ejercicio de sus funciones y en el marco de sus competencias; c) «(…) *se refieran a partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento*»; d) el tratamiento «*(…) tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley*»; e) « (…) los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos». Todas estas excepciones serán aplicables «(…) *siempre que no se vulneren los derechos y libertades fundamentales del interesado*»[189].

Este mínimo general en materia de consentimiento se ve reforzado, como en el caso de su antecesora, por su artículo 7, donde se desarrolla el régimen especial previsto para los datos especialmente protegidos, en nuestro caso los datos ideológicos y religiosos. Tomando en consideración lo allí dispuesto y lo que desaparece de las previsiones anteriores, el régimen puede resumirse en 3 puntos:

1. Para tratar estos datos, la norma mantiene la obligación de que la emisión del consentimiento reúna, además de los requisitos generales previstos en el art. 6 de la LOPD que acabamos de ver, dos características específicas: *ser expreso y por escrito*[190]. El artículo comienza recordando la garantía prevista en el art. 16.2 de la CE –nadie podrá ser obligado a declarar sobre su religión– y su correlativa obligación por parte del responsable del tratamiento de advertirle que tendrá derecho a no prestarlo. Se configura así un sistema específico para el tratamiento de los datos sensibles religiosos basado en el refuerzo del consentimiento, donde la autonomía y voluntad que supone el consentimiento para la protección de datos se refuerza con la garantía que forman parte del contenido esencial

[187] *Vid.* art. 4.2 de la LOPD 1999.
[188] *Vid.* art. 4.5 tercer párrafo de la LOPD 1999.
[189] *Vid.* art. 6 de la LOPD.
[190] *Vid.* art. 7.2 LOPD.

de su libertad religiosa, más concretamente el derecho a no declarar sobre sus convicciones. Para cumplir con este refuerzo resulta imprescindible que la persona concernida esté convenientemente informada de su derecho a no manifestar sus creencias religiosas y, en segundo lugar, que la emisión de su consentimiento *sea expresa y por escrito*, a lo que se acumula el deber genérico de mantener el secreto por parte del responsable del tratamiento previsto en el art. 10.

2. Esta será la regla general y solo cabrá una excepción: cuando los datos sean recogidos y almacenados en los ficheros mantenidos por las Iglesias, confesiones y comunidades religiosas, con finalidad religiosa y referidos a los datos de sus asociados o miembros. Con la LOPD 1999 desaparece la exclusión de su ámbito de aplicación de los ficheros y archivos de las comunidades religiosas, pero no cae en el olvido y, como también hemos adelantado, sirve de fundamento para rebajar las condiciones en las que debe prestarse el consentimiento por el sujeto concernido y el grado de elevación de las garantías adoptadas por parte del responsable del tratamiento. En este caso, se admite la existencia de *un consentimiento tácito* que se desprende del alta voluntaria en la comunidad[191] y, en todo caso, se recupera la necesidad de contar con el consentimiento expreso para la cesión. Es así como en ambas normas se mantienen dos vías para la definitiva caracterización del consentimiento, dependiendo de si se trata de: a) recogida y tenencia de datos, donde se rebaja las condiciones previstas para la emisión del consentimiento y se admite la existencia de un consentimiento tácito derivado del alta de la persona en la entidad o comunidad; b) trafico y cesión, es decir en el intercambio de la información, donde se recupera la idea de que es necesario contar con un refuerzo del consentimiento exigiendo que su emisión sea por expreso y por escrito. Por lo tanto, esto nos permite concluir que no serán las mismas las implicaciones que supone la recopilación y almacenamiento de datos religiosos que la cesión e intercambio de la información, lo que requerirá distintos niveles de garantías, requisitos, medida de seguridad, etc.

3. En todo caso quedan prohibidos los ficheros que tengan por finalidad almacenar datos que revelen la ideología, religión, afiliación sindical, etc. (art. 7.4 LOPD). Por lo tanto, la Administración no podrá disponer de un registro que almacene esta categoría de datos salvo que el interesado consienta, la finalidad para la que han sido recogidos y almacenados sea una de las excepciones previstas en la normativa o se adhiera una finalidad de interés general, por ejemplo aquellas vinculadas con la gestión de la diversidad religiosa[192].

[191] RODRÍGUEZ GARCÍA, José Antonio, «La protección de los datos personales…», *op. cit., Vid.* p. 341.
[192] *Ibidem* p. 341.

Compartimos plenamente la opinión de la profesora CANO cuando al analizar la situación de los datos religiosos en el marco de la LOPD consideraba adecuado concluir que el sistema de protección se construye sobre «(…) una conceptualización de datos sensibles por su propia naturaleza o per se, si bien acogiendo un carácter dinámico de los mismos (…) en atención, no solo a las características jurídicas y sociológicas de nuestro país –como recomiendo la normativa comunitaria–, sino también al contexto en el que van a ser utilizados»[193]. Opinión que se ha visto confirmada por la tendencia que marca la regulación europea y nacional actual.

En conclusión, ambas normas pueden ser consideradas como «*Leyes de protección de datos de tercera generación*», en la terminología empleada por Pérez Luño, ya que trascienden del mero factor estático –*calidad de los datos*– como fundamento de su tutela, principalmente en el caso de los datos especialmente sensibles, hasta incluir como fundamento de su protección un factor dinámico: los fines para los que fueron recabados y tratados, y consolidando el *principio de legitimidad*. Ambas disposiciones comparten el mismo propósito para evitar actividades discriminatorias basadas en el uso de los datos personales: asegurar la calidad y legitimidad en el uso de los datos que sobre todo evite las «decisiones individuales automatizadas» y sus posibles consecuencias discriminatorias derivadas de los resultados obtenidos en procesos realizadas con aplicaciones informáticas que tratan de elaborar perfiles personales[194]. Este elemento se consolidará en el nuevo Reglamento europeo y en la norma dictada por el legislador español, pero con mayor fuerza cuando se trate de datos especialmente protegidos, como es el caso de los que revelan las convicciones personales del individuo.

Con la promulgación del nuevo RGPD se modifica y renueva lo visto hasta ahora. Aunque la promulgación de una nueva legislación interna no resulta totalmente obligatoria[195], sí resulta aconsejable, especialmente para despejar la inaplicación de la LOPD 1999. Y es que el nuevo Reglamento, como los demás emitidos por la UE, resulta directamente aplicable en los Estados miembro haciendo innecesario mayor desarrollo, pero siempre se parte de la posibilidad de promulgar una normativa interna en cada Estado miembro a la que, en la mayor parte de las ocasiones, se le asigna la tarea de desarrollar cuestiones muy específicas (como, por ejemplo, la determinación de las condiciones generales

[193] Cano Ruiz, Isabel, *Los datos religiosos..., op. cit.*, *Vid.* p. 22.

[194] Todo lo anterior en Pérez Luño, Antonio Enrique, «La tutela de la libertad informática…», *op. cit.*, *Vid.* p. 66 y del mismo autor «El concepto de interesado…», *op. cit.*, *Vid.* pp. 25 y 26.

[195] Así lo afirma Fernández Villazón, Luis Antonio, «El nuevo Reglamento Europeo…», *op. cit.*, *Vid.* p. 410.

para la imposición de sanciones administrativas) [196]. Es así como, con el objeto de adaptar el ordenamiento jurídico español a esta realidad, se aprobó el 5 de diciembre de 2018 la Ley Orgánica 3/2018 de *Protección de Datos Personales y garantía de los derechos digitales*[197] (en adelante, LOPD 2018). Esta nueva Ley, por lo tanto, tiene dos objetivos: a) adaptar el ejercicio del derecho fundamental a la protección de datos previsto en el art. 18.4 CE al régimen previsto en el RGPD y b) garantizar los derechos digitales de la ciudadanía[198].

El Título II de la LOPD 2018 asienta los *principios* que deben sostener el régimen de protección de datos, desarrollando con detalle los términos en los que se garantizará *la exactitud de los datos*, el *deber de confidencialidad* de los sujetos que intervienen en el tratamiento, *el necesario consentimiento del sujeto* concernido, la especial protección a los *datos sensibles* y de naturaleza penal. Así, del conjunto de disposiciones podemos concluir que:

— *Los datos deben ser exactos y actualizados*. La inexactitud con respecto a los fines para los que se tratan no será imputable al responsable del tratamiento cuando:

a) hayan sido obtenidos directamente del afectado;

b) hubiesen sido obtenidos de un intermediario, en el caso de que las normas que regulen el sector al que se dedique el responsable del tratamiento establecieran la posible intervención de ese intermediario para recoger y transmitir al responsable los datos del sujeto. «El mediador o intermediario asumirá las responsabilidades que pudieran derivarse en el supuesto de comunicación al responsable de datos que no se correspondan con los facilitados por el afectado».

c) provengan de otro responsable en ejercicio del derecho de portabilidad del sujeto concernido;

d) provengan de un registro público[199].

— *Los responsables, encargados y demás sujetos* que intervengan en cualquier fase del tratamiento *están sujetos al deber de confidencialidad*. Se trata de una obligación general complementada con el *deber de secreto profesional* y que se prolongará en el tiempo aún cuando la relación del obligado con el responsable hubiera finalizado[200].

---

[196] *Ibidem.*
[197] Publicada en el *BOE* n.º 294, de 6 de diciembre de 2018.
[198] *Vid.* art. 1 de la LOPD 2018.
[199] Todo en art. 4 de la LOPD 2018.
[200] *Vid.* art. 5 de la LOPD 2018.

— El *consentimiento* se define en los mismos términos que vimos según el art. 4. 11 del RGPD: *manifestación de la voluntad del sujeto libre, específica, informada e inequívoca por la que se acepta el tratamiento de los datos*. Cuando ese consentimiento se pretenda utilizar para fundamentar el tratamiento de los datos por una pluralidad de finalidades «(…) será preciso que conste de manera específica e inequívoca que dicho consentimiento se otorga para todas ellas»[201].

— Solo podrá considerarse que el *tratamiento* de los datos está legítimamente *fundado* en el cumplimiento de una *misión realizada en interés público o en el ejercicio de los poderes públicos conferidos al responsable*, cuando «(…) derive de una competencia atribuida por una norma con rango de Ley».

— En cuanto al *tratamiento de los datos sensibles*, entre ellos los que revelan las convicciones ideológicas y religiosas del individuo, la LOPD 2018 considera que la prohibición general de tratamiento no puede ser levantada por el simple hecho de contar con el consentimiento del interesado[202], pero si que considera factible justificar la excepción a la prohibición general en el resto de los supuestos previstos en el RGPD[203], entre los que recordemos se encuentra:

a) el tratamiento para el *cumplimiento de obligaciones específicas del responsable y ejercicio de derechos del interesado en el ámbito laboral, seguridad y protección social*;

b) el tratamiento para *proteger intereses vitales del sujeto concernido u otra persona*;

c) el tratamiento de los *miembros actuales o antiguos y de personas que mantengan contacto regulares en relación a sus fines con fundaciones, asociaciones u organismos sin ánimo de lucro que tengan fines políticos, religiosos, etc.*, teniendo en cuenta en todo caso que la cesión de los datos está sujeta a la necesidad de contar con su consentimiento expreso;

d) el tratamiento se refiera a *datos manifiestamente públicos*;

e) el tratamiento se realice en cumplimiento de un *interés público esencial* que habrá de ser proporcional al objetivo perseguido, respetar en lo esencial el derecho de protección de datos y establecer las medidas adecuadas y específicas para proteger los intereses y derecho fundamentales del sujeto concernido; etc. Todas ellas, excepto la b) y la c) que se refieren a supuestos gene-

[201] *Vid.* art. 6 de la LOPD 2018.

[202] De conformidad con lo establecido en la parte final del art. 9.2 a) del RGPD: «(…) excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado», Cfr. art. 9.2 a) del RGPD.

[203] *Vid.* art. 9 de la LOPD 2018.

rales, podrían tener un gran interés para fijar los motivos por los que los datos personales son tratados en el RER.

Segundo. La norma reafirma los derechos del sujeto concernido[204] y cuando se trata de concretar el *deber de transparencia e información* que debe cumplir el responsable del tratamiento para asegurar y facilitar el ejercicio pleno de esos derechos[205], el responsable tiene la obligación inexcusable de facilitarle una información básica y una dirección electrónica, u otro medio, en el que pueda obtener el resto de información que exista en su caso. Respecto a la *información básica* que debe ofrecer el responsable del tratamiento contendrá:

a) la identidad del responsable y, en su caso, su representante;
b) la finalidad del tratamiento;
c) la posibilidad de ejercer los derechos establecidos en los artículo 15 a 22 del RGP
d) pero, además, si la información fuera a ser tratada *para elaborar perfiles*, el interesado deberá ser informado de su derecho a oponerse a la adopción de decisiones individuales automatizadas que le produzcan efectos jurídicos o le afecten significativamente.
e) Cuando los datos no hayan sido obtenidos directamente del interesado, la información básica incluirá las categorías de datos objeto de tratamiento y la fuente de la que proceden esos datos [206].

Tercero. Siguiendo lo que hemos dicho con anterioridad, la norma fija unas *medidas de responsabilidad activa* para el responsable y encargado del tratamiento. Son ellos los encargados de adoptar las medidas técnicas y organizativas apropiadas para garantizar y acreditar que el tratamiento se realiza conforme al RGPD[207]. En la adopción de estas medidas, el legislador avisa al responsable y encargado del tratamiento que deberán extremar la precaución en aquellos supuestos donde pueden producirse los mayores riesgos, entre los que incluye:

a) los casos en que el tratamiento pueda generar, entre otras, situaciones de discriminación, usurpación de la identidad, daños en la reputación, perdida de confidencialidad de datos sujetos al deber de secreto profesional, reversión no autorizada de la *seudonimización* o cualquier otro perjuicio moral y social;

[204] *Vid.* arts. 13 a 18 de la LOPD 2018.
[205] Según lo establecido en el art. 13 del RGPD.
[206] *Vid.* art. 11 de la LOPD 2018.
[207] *Vid.* art. 28.1 de la LOPD 2018.

b) cuando el tratamiento pudiera privar a los sujetos de sus derechos y libertades o el control sobre sus datos;

c) cuando se produzca el tratamiento de los datos especiales o sensibles que no sea meramente incidental o accesorio;

d) cuando el tratamiento suponga una evaluación de aspectos personales del sujeto para crear o utilizar perfiles personales de comportamiento;

e) cuando los datos tratados se refieran a grupos de afectados por una situación especial de vulnerabilidad y, en particular, menores y personas con discapacidad;

f) cuando se produzcan tratamientos masivos de datos[208];

El responsable tiene la obligación de *mantener un registro de las actividades de tratamiento* en los términos previstos por el art. 30 del RGPD. Este registro deberá contener: a) el nombre y datos de contacto del responsable, corresponsable, del representante del responsable y del delegado de protección de datos; b) los fines del tratamiento; c) una descripción de categorías de interesados y de los datos personales; c) las categorías de destinatarios incluidos los de terceros países y organizaciones internacionales; d) el plazo previsto para la supresión de los datos, cuando sea posible; e) una descripción general, cuando sea posible, de las medidas técnicas y de seguridad adoptadas[209].

---

[208] El tenor literal del artículo incluye estos supuestos de forma más detallada y otros a los que no hemos hecho referencia: «a) Cuando el tratamiento pudiera generar situaciones de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la *seudonimización* o cualquier otro perjuicio económico, moral o social significativo para los afectados. b) Cuando el tratamiento pudiese privar a los afectados de sus derechos y libertades o pudiera impedirles el ejercicio del control sobre sus datos personales. c) Cuando se produjese el tratamiento no meramente incidental o accesorio de las categorías especiales de datos a las que se refieren los artículos 9 y 10 del Reglamento (UE) 2016/679 y 9 y 10 de esta ley orgánica o de los datos relacionados con la comisión de infracciones administrativas. d) Cuando el tratamiento implicase una evaluación de aspectos personales de los afectados con el fin de crear o utilizar perfiles personales de los mismos, en particular mediante el análisis o la predicción de aspectos referidos a su rendimiento en el trabajo, su situación económica, su salud, sus preferencias o intereses personales, su fiabilidad o comportamiento, su solvencia financiera, su localización o sus movimientos. e) Cuando se lleve a cabo el tratamiento de datos de grupos de afectados en situación de especial vulnerabilidad y, en particular, de menores de edad y personas con discapacidad. f) Cuando se produzca un tratamiento masivo que implique a un gran número de afectados o conlleve la recogida de una gran cantidad de datos personales. g) Cuando los datos personales fuesen a ser objeto de transferencia, con carácter habitual, a terceros Estados u organizaciones internacionales respecto de los que no se hubiese declarado un nivel adecuado de protección. h) Cualesquiera otros que a juicio del responsable o del encargado pudieran tener relevancia y en particular aquellos previstos en códigos de conducta y estándares definidos por esquemas de certificación».

[209] *Vid.* art. 31 de la LOPD 2018.

Los responsables del tratamiento tendrán la obligación de nombrar un *Delegado de Protección de Datos* en los casos previstos por el art. 37 del RGPD[210]. Según este precepto, serán preceptivo nombrarlo cuando: a) el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales en ejercicio de su función; b) cuando las actividades principales del responsable o encargado sean el tratamiento a gran escala de categorías especiales de datos o de datos relativos a condenas e infracciones penales.

Por último, la norma recuerda la oportunidad de diseñar *Códigos de conducta*, que serán vinculantes para quienes se adhieran a ellos, y que los Estados *acrediten instituciones de certificación*, en los términos previstos por el RGPD[211]. Estos *Códigos de conducta* están dirigidos a la correcta aplicación del RGPD, que podrán tener por objeto especificar su aplicación en materia de a) tratamiento leal y transparente; b) intereses legítimos perseguidos por el responsable; c) recogida de datos personales; d) *seudonimización* de datos personales; e) información proporcionada al público y a los interesados; f) ejercicio de los derechos de los interesados; g) «información proporcionada a los niños y su protección, así como la manera de obtener el consentimiento de los titulares de la patria potestad o tutela sobre el niño»; h) medidas para garantizar la seguridad o para diseñar los procedimientos de protección desde el diseño y por defecto, etc.[212]

3. REFLEXIONES PARA CONSTRUIR UN MARCO JURÍDICO ADECUADO PARA EL USO DE DATOS PERSONALES EN LA GESTIÓN DE LA DIVERSIDAD RELIGIOSA

Como punto de partida consideramos importante convenir que toda iniciativa legislativa que se desarrolle para proteger los datos de aquellas personas vinculadas con las confesiones religiosas que se recojan en el marco del proceso registral desarrollado por el RER, deberá tomar como punto de referencia el régimen legal previsto en la LOPD 2018 y en el RGPD. Es el propio desarrollo normativo que regula la organización y funcionamiento del RER quien se remite formalmente al régimen general de protección de los datos personales para regular aquellos supuestos en los que al desempeñar las actividades que le son propias, fundamentalmente la inscripción y reconocimiento jurídico de entidades religiosas, el encargado del RER procesa datos e información personal de

[210] *Vid.* art. 34 de la LOPD 2018.
[211] *Vid.* art. 38 de la LOPD 2018.
[212] *Vid.* art. 40 del RGPD.

sujetos directamente relacionados con ellas. Técnicamente la referencia genérica que realiza el RD 594/2015 se concreta en lo que conocemos como una *remisión formal*, tan propia del ordenamiento jurídico, sin que hasta el momento de realizar este trabajo tengamos constancia que se haya producido un desarrollo específico de su contenido, salvo algunas referencias expresas en el RD 594/2015 a los requisitos que debe cumplir el necesario consentimiento y los formularios para recogerlo y, en consecuencia los términos previstos en el documento de solicitud recientemente adoptado que el Ministerio de Justicia pone a disposición de los solicitantes en su página web[213]. Por lo tanto, legislación general sobre protección de datos, que hemos estudiado con anterioridad, nos permitirá extraer el conjunto de requisitos formales y materiales que debe cumplir todo sistema de protección de los datos vinculados al ejercicio de la libertad religiosa, diseñar las garantías que han de formularse para que el responsable y encargado del tratamiento cumplan con su compromiso de *responsabilidad proactiva*, e identificar las acciones que deban aplicarse para certificar y asegurar que todo ello se cumple.

Pero, además, esta vinculación técnica entre ambos derechos, producida por una *remisión formal*, no es la única justificación que nos obliga a acudir al régimen general. Como hemos advertido durante el análisis anterior, el propio derecho de protección de datos, que nace en el seno de los derechos de personalidad, –honor, intimidad, vida privada, etc.– con una evidente conexión al respeto de la dignidad y el libre desarrollo de la personalidad, se configura como un derecho con *carácter instrumental* en la protección de los demás derechos fundamentales. De este modo, *construir un sistema de gestión de los datos, en el marco del proceso de inscripción y reconocimiento de las entidades religiosas,* basado en los requisitos establecidos en la normativa general *no solo garantizará,* como es lógico, *el derecho de protección de datos del sujeto concernido, sino que, además, redundará en una mejor protección de su libertad ideológica y religiosa, garantizando su ejercicio pleno*. Por otra parte, sin olvidar la evolución que ha vivido el fundamento de su tutela jurídica, completándose desde una dimensión meramente estática a otra dinámica, habrá que considerar no solo la *calidad* de los datos: que son exactos, actualizados y los estrictamente necesarios para cumplir con los objetivos propuestos, etc., sino también la *legitimidad* de su finalidad y uso, especialmente cuando provoca consecuencias indeseadas o discriminatorias.

---

[213] https://www.mjusticia.gob.es/cs/Satellite/Portal/1292428829453?blobheader=application%2Fpdf&blobheadername1=Content-Disposition&blobheadername2=Grupo&blobheadervalue1=attachment%3B+filename%3DSolicitud_de_Actuacion_en_el_Registro_de_Entidades_Religiosas. PDF&blobheadervalue2=Docs_Llibertad+religiosa

Por su parte, sabemos que con el nuevo diseño del sistema de protección de datos nos situamos ante una normativa que trasciende la mera protección de datos que se vinculan directamente con la intimidad de la persona, hasta alcanzar toda información, datos, características, etc. que además de formar parte de su identidad el sujeto concernido desea conservar auto-determinado incluso en su relación con terceros[214]. Entre ellos se incluye aquellos datos que pudieran servir para confeccionar el perfil ideológico y religioso, racial, sexual, etc. de la persona o que según el uso que se les diera pudieran suponer, bajo determinadas circunstancias, una amenaza para la persona y sus derechos. Por ello, ya desde el *Convenio 108* el legislador viene considerando la existencia de unos datos personales que, por su singularidad, han de ser tratados de manera específica, generalmente reforzando su nivel de protección. Entre estos datos se encuentra, como sabemos, los datos que revelan las convicciones personales del sujeto. Como ya puso de manifiesto la profesora Cano, la doctrina especializada no ha escatimado esfuerzos para resolver si el fundamento de su tipificación se debe a una vinculación directa con la libertad específica, la libertad ideológica y religiosa, o con el *principio de no discriminación*, por su evidente conexión con las causas previstas en el precepto constitucional –raza, religión sexo, etc.–. Esta circunstancia nos lleva a reflexionar sobre su interacción con los derechos y principios protegidos en otros dos preceptos constitucionales, los artículos 16 y 14 de la CE[215].

Desde esta perspectiva, en nuestra opinión ambos preceptos son clave para determinar el fundamento, pero dependiendo de cuál sea la situación en la que se aplique nos encontramos con dos situaciones completamente distintas.

Primero, parece relativamente adecuado conectar la primera dimensión del derecho a la protección de datos, la *autonomía y no injerencia* sobre sus datos personales, con la *dimensión interna de la libertad religiosa:* una esfera de *agerece licere* que *garantiza la autonomía del sujeto* para determinar y controlar su identidad religiosa[216] y queda coronada por el *principio de no intervención o injerencia*[217]. Esta *dimensión interna* coincidente se materializa en la *autodeterminación informativa* y en *el derecho a no ser obligado a declarar sobre sus creencias religiosas* previsto en el art. 16.2 CE. A su vez actúa como puente con la *dimensión externa*. El derecho de protección de datos en esta segunda *dimensión externa* está asociado con su carácter de derecho au-

[214] LLAMAZARES FERNÁNDEZ, Dionisio, *Derecho de libertad de conciencia II…, op. cit.* p. 38.
[215] CANO RUIZ, Isabel, *Los datos religiosos…, op. cit.* pp. 26 y ss.
[216] PALOMINO LOZANO, Rafael, *Neutralidad y espacio público*, Aranzadi, Pamplona, 2014, *Vid.* p. 45.
[217] FERNÁNDEZ-CORONADO, Ana y SUÁREZ PERTIERRA, Gustavo, *Identidad social, pluralismo religioso y laicidad del Estado*, Fundación Alternativas, Madrid, 2013, pp. 46 y 47.

tónomo, el *poder de uso y disposición* de los datos personales, y se conectaría con el ejercicio de la *dimensión externa de la libertad religiosa*, integrada por el conjunto de manifestaciones externas donde, por disposición constitucional, queda habilitada la interacción con los poderes públicos. Esta interacción entre los sujetos y los poderes públicos en el ámbito de lo religioso se concreta en la doble función que desarrolla el Estado en el tratamiento de los derechos fundamentales: a) la labor de *gestión y promoción*, fundamentada en el carácter positivo de nuestro modelo de aconfesionalidad o laicidad positiva y específicamente en el mandato del art. 9.2 CE. Una labor de promoción donde, según el propio TC en su sentencia 46/2001, se sitúa la función del RER; y b) la *labor de prevención o control*, perfilada en el texto constitucional con la posibilidad de establecer límites al ejercicio de la libertad religiosa en un contexto similar al del propio derecho de protección de datos: el necesario respeto a los derechos y libertades fundamentales, el orden público establecido por la Ley y la seguridad, la salud y la moral públicas. Una dimensión que en este caso tendría más impacto en el tratamiento de los datos legitimados en el ejercicio de las competencias necesarias para mantener la seguridad. En esta ocasión, el peligro podría plasmarse en la utilización de información personal para generar perfiles de comportamiento susceptibles de ser investigados, perseguidos, castigados, etc. que podrían redundar en situaciones de discriminación por razón de la religión.

Segundo, con relación a la *igualdad formal* y el *principio de discriminación, el dato religioso no debe ser utilizado para minorar la capacidad jurídica de una persona ni amparar conductas discriminatorias de terceros,* sea la Administración o no. Desde la perspectiva de su conexión con la libertad ideológica y religiosa tiene como resultado proscribir los efectos y consecuencias indeseadas que pudiera tener el uso ilegítimo de esos datos y/o la desconexión entre la realidad y esa información (es decir su inexactitud). Para garantizar el *principio de exactitud*, se requiere comprobar regularmente los datos y mantenerlos actualizados. Para evitar los efectos indeseados sobre los derechos del interesado o conductas discriminatorias como consecuencia de su tratamiento, se refuerza el papel y requisitos del consentimiento: su carácter explícito, expreso y por escrito, se asegura la necesidad de mantener informado al sujeto concernido y se garantiza la intervención humana cuando se puedan producir decisiones automatizadas que impliquen la elaboración de un perfil personal. Estas ideas se conectan con las previsiones del RD 594/2015 cuando refuerza el consentimiento para la cesión de los datos, advierte a las entidades de la necesidad de mantener actualizada su información y, por otra parte, cubre de garantías la capacidad de acceso y cesión de la información según las disposi-

ciones en las que se concreta el proceso de publicidad. Por ejemplo, en el régimen de publicidad del RER las consultas genéricas están excluidas, salvo para su consideración por el responsable, cualquier acción que se desarrolle en este sentido está sometida a su conformidad con la legislación sobre protección de datos, por otra parte, se contempla un uso y contenido diferente de las notas y certificaciones, facilitando así la salvaguarda de la información que obra en el expediente anejo, donde realmente se anotarán los *ministros de culto* y de los *titulares de los órganos de representación*, dado el modo en que se prevé su inscripción –como actos inscribibles–. Este hecho, además, permitiría aplicar procedimientos de *seudonimización* de los datos, considerado como el proceso técnico que puede garantizar la seguridad de los datos en la mayoría de los casos. Con este procedimiento, como hemos visto, se favorece el tratamiento de los datos de una persona de tal manera que no puedan atribuirse a un interesado sin utilizar información adicional. Esa información adicional debe figurar por separado y debe estar sujeta las medidas técnicas y organizativas adecuadas destinadas a garantizar que esos datos no se puedan atribuir a una persona identificada o utilizar para que sea identificable. De este modo apuntamos nuestra idea de que *sería más operativo crear un fichero anejo donde se contengan estos datos, que quedaría excluido de la consulta general a los datos del RER y donde se conservarían exclusivamente por el tiempo necesario para cumplir los objetivos previstos.*

En todo caso, cuando el tratamiento se dirija a elaborar un perfil que se utilice como información para prevenir o controlar a personas susceptibles de ser considerados un peligro para la seguridad del Estado, la normativa es clara al impedir que una persona sea sujeto de una decisión basada en el mero tratamiento automatizado de los datos, como pueda ser la elaboración de perfiles, garantizando el derecho de la persona a que se produzca intervención humana en la decisión, a expresar su opinión y a impugnar la decisión. Por ello el nuevo documento oficial para la solicitud de inscripción recuerda en su apartado «Fines del Tratamiento», dentro la información adicional sobre protección de datos, la declaración expresa de que los datos recabados no será objeto de decisiones basadas en el tratamiento automatizado ni utilizados para elaborar perfiles. Además, *nuestra sugerencia sería incorporar la referencia a los derechos que asisten al interesado en el caso de que se produjera alguna actuación en este sentido que derivara de la cesión de esos datos, recordándole que podrá solicitar la intervención humana, expresar su opinión e impugnar la decisión*[218].

[218] https://www.mjusticia.gob.es/cs/Satellite/Portal/1292428829453?blobheader=application%2Fpdf&blobheadername1=Content-Disposition&blobheadername2=Grupo&blobheadervalue1=

Teniendo en cuenta todo lo dicho, una de las cuestiones esenciales que debemos atender para confirmar la legitimidad del uso y colección de los datos será la finalidad para los que son recabados y sus consecuencias, que podrán ser un impacto sobre el ejercicio pleno de la libertad religiosa o una posible actuación que derive en situaciones discriminatorias. Por eso consideramos que, aunque en todas las situaciones resulta imprescindible que se cumpla con el *principio de calidad de los datos y transparencia*, aportando al interesado, de forma clara y sencilla, toda la información necesaria para conocer qué tratamiento se va a realizar y las consecuencias o resultados podría tener, cada situación prevista en el RD 594/2015 requiere un estudio específico por separado de las circunstancias que determinan el contexto de su tratamiento:

— Respecto a las *personas que deciden avalar el establecimiento o fundación de la entidad religiosa en España* debemos remitirnos al art. 6.2 del RD 594/2015 cuando, al enumerar los requisitos necesarios para proceder a la inscripción de la entidad religiosa, requiere que se presente, en documento elevado a escritura pública, el acta de fundación o establecimiento de la entidad en España. Según la redacción literal del texto: «En dicha acta se podrá hacer constar la relación nominal de, al menos, veinte personas mayores de edad y con residencia legal en España que avalan la fundación o establecimiento de la Iglesia, Confesión o Comunidad religiosa». Al solicitar expresamente una «*relación nominal*» podemos entender que la información aportada al expediente de inscripción deberá incluir, como mínimo, los nombres y apellidos de las personas. Por su parte, al fijarse como requisitos que han de concurrir en estos sujetos la «mayoría de edad» y «residencia legal en España», consideramos que deberán incluir un documento donde se contenga el dato de la edad y el domicilio o residencia legal del sujeto, para certificar que se cumplen ambas condiciones. En nuestra opinión, ambas condiciones podrían ser acreditadas a través de la presentación del documento de identidad o residencia legal correspondiente y/o un certificado de nacimiento y padrón.

La segunda cuestión que debemos tener en cuenta es que el propio precepto señala que se «podrá hacer constar». Con esta redacción consideramos que debemos partir de entender su inscripción como algo potestativo, no obligatorio. Esta idea nos hace suponer que, al ser voluntario, la cesión de los datos depende en todos los sentidos de la voluntad del individuo y se presupone la

attachment%3B+filename%3DSolicitud_de_Actuacion_en_el_Registro_de_Entidades_Religiosas. PDF&blobheadervalue2=Docs_Llibertad+religiosa –última vez visitada 15/01/2015-

existencia de su consentimiento, aunque sea de forma tácita, para facilitar los datos. Sin embargo, como hemos visto en el régimen general previsto para los datos sensibles, el consentimiento tácito no cumple con los requisitos formales y materiales que este debe reunir para el uso de datos sensibles, salvo que se trate de registros o archivos confesionales. Según la LOPD 2018 el mero consentimiento tampoco es suficiente para legitimar su tratamiento, que en todo caso dependerá de su conformidad con alguno de los fines previstos en el RGPD: a) el *cumplimiento de obligaciones específicas del responsable y ejercicio de derechos del interesado en el ámbito laboral, seguridad y protección social*; b) el tratamiento desarrollado por *fundaciones, asociaciones u organismos sin ánimo de lucro que tengan fines políticos, religiosos, etc.*, de sus *miembros actuales o antiguos y de personas que mantengan contacto regulares en relación a sus fines,* teniendo en cuenta en todo caso que la cesión de los datos está sujeta a la necesidad de contar con su consentimiento expreso; c) el tratamiento se realice en cumplimiento de un *interés público esencial*.

Al preguntamos por el motivo o finalidad que impulsa la solicitud de los datos de personas que *avalan la fundación o establecimiento* de una entidad en España, en nuestra opinión parece que el legislador recupera la idea de que la existencia de un número determinado de personas adscritas a la comunidad religiosa permite constatar su existencia y estabilidad[219]. Con independencia del número de personas que, desde un punto de vista teórico, se considere necesario[220], de su necesidad o importancia como elemento para certificar la existencia de una entidad religiosa y de las verdaderas razones que hayan motivado a determinar en la nueva regulación la cantidad definitiva de 20 personas[221], com-

[219] A favor, por ejemplo, *Vid.* MANTECÓN SANCHO, Joaquín, «Confesiones religiosas y Registro» en VV. AA. *Libertad religiosa a los veinte años de su Ley Orgánica*, Ministerio de Justicia, Madrid, 1999, pp. 79 a 166, *Vid.* p. 94 o MARTÍNEZ TORRÓN, Javier, *Separatismo y cooperación en los Acuerdos del Estado con las minorías religiosas*, Comares, Granada 1994, *Vid.* p. 85.

[220] El rango va desde 50 fieles como mínimo necesario, en este sentido *Vid.* LÓPEZ-SIDRO LÓPEZ, Ángel, «La cuestión de la reforma del Registro de Entidades Religiosas: examen de las propuestas reglamentarias de 2003 y 2004», *Revista General de Derecho Canónico y Derecho Eclesiástico del Estado*, n.º 19 (2009), pp. 1 a 22, *Vid.* p. 7, hasta 1.000 personas, *Vid.* CAMARASA CARRILLO, José, *La personalidad jurídica de las entidades religiosas en España,* Marcial Pons, Madrid, 1995, *Vid.* p. 60. No somos el único país europeo o del entorno que en su legislación ha incluido la necesidad de contar con un mínimo de fieles para constituir una entidad religiosa, por ejemplo *Vid.* el estudio aportado en FERNÁNDEZ-CORONADO, Ana, «Evolución del derecho de Libertad religiosa en los Estados de la Unión Europea que formaron parte de la Unión Soviética», *Derecho y Religión*, Vol. III, 2013, pp. 85 a 100, *Vid.* p. 92; RODRÍGUEZ MOYA, Almudena, «Derecho y Religión en Armenia», *Derecho y Religión*, Vol. III, 2013, pp. 209 a 224, *Vid.* p. 221.

[221] Según el profesor García, se trata de la aplicación analógica del requisito exigido en el caso del ejercicio del derecho de reunión, *Vid.* GARCÍA GARCÍA, Ricardo, «Real Decreto 594/2015, de 3 de julio, por el que se regula el Registro...», *op. cit.*, *Vid.* p. 263.

partimos plenamente la opinión mantenida por el profesor Motilla en su estudio esencial sobre el concepto de confesión religiosa en la praxis administrativa y jurisprudencial española, de que nos situamos ante una *concepción institucional* de las comunidades religiosas[222], con las ventajas e inconvenientes que han sido puestos de manifiesto por la doctrina[223].

Por ese motivo el primer escollo con el que nos encontramos es que dicha finalidad tiene un interés más institucional que personal, que incrementa la complejidad de justificar su inclusión en el régimen de protección de datos, al no estar prevista su aplicación a las personas jurídicas. El propio documento oficial de solicitud mantiene como finalidades: la inscripción, modificación y cancelación de las entidades religiosas y como criterio para constatar su legitimación el ejercicio de una actividad en *interés público*. Sin embargo, no podemos olvidar que esta inscripción trasciende en la práctica los meros objetivos institucional y genera resultados o consecuencias personales para el sujeto concernido, por lo que requerirá medir su legitimidad en pro de su *fundamento dinámico*. Dado que se trata de datos sensibles y la finalidad no parece estar vinculada con ningún objetivo personal, su inclusión nos conduciría posiblemente a calificarla de contraria al derecho y con ello aconsejar su no incorporación en el proceso de inscripción. Si bien, dado que desde el punto de vista constitucional y orgánico[224] la constitución de las entidades religiosas está prevista como parte del contenido esencial del derecho de libertad religiosa del individuo, ejercido colectivamente, y en nuestra opinión el reconocimiento de las comunidades religiosas tiene como fundamento el pleno ejercicio del derecho de la persona (situando así su dimensión personal sobre institucional) *podría (debería) tratarse esos datos informando de que la verdadera finalidad por la que se recogen es cumplir con un interés de la persona concernida: facilitar el ejercicio su derecho fundamental a través de un adecuado reconocimiento de la institución en la que desarrollara su ejercicio colectivo.*

En ese sentido habrá que dejar constancia de que la persona que se incorpora en el expediente como aval *consiente expresamente y por escrito* en ceder sus datos. En todo caso, nuestra opinión es que esta información personal, como medida de seguridad específica, debería excluirse de la hoja registral principal y formar parte, como mucho, del protocolo anejo. Dada la prohibición

---

[222] Motilla de la Calle, Agustín, *El concepto de confesión religiosa en el Derecho español. Práctica administrativa y doctrina jurisprudencial*, CEPC, Madrid, 1999, *Vid.* p.

[223] Aldanondo Salaverria, Isabel, «Nuevos movimientos religiosos y Registro de Entidades Religiosas», *Anuario de la Facultad de Derecho de la Universidad Autónoma de Madrid,* n.º 17 (2013), pp. 355 a 398, *Vid.* p. 358.

[224] *Vid.* art. 16 CE y art. 2 y 6 de la LOLR.

general de constituir un registro con la única finalidad de almacenar datos religiosos, no resulta aconsejable la existencia de un registro o fichero específico separado del general, pero consideramos más acorde con el régimen de protección de datos su inclusión en el expediente anejo que, además, no es objeto de acceso público general[225]. La única cuestión que habría que concretar es el plazo adecuado por el que se debería almacenar esta información. Esto nos obligaría a concretar el tiempo requerido para dar por válido el aval de la fundación de una entidad, lo que se antoja ambiguo y en muchas ocasiones indefinible. *Como única opción podría aplicarse el plazo de dos años previsto para aportar la declaración de funcionamiento226, que habría que hacer coincidir con una información a los sujetos concernidos y la solicitud de renovación o revocación de su consentimiento para mantener los datos.* Por último, sea como fuere durante el plazo en el que se mantenga estos datos sería aconsejable aplicar cuando menos un proceso de *seudonimización*.

— Respecto a los *titulares de los órganos de representación* de la entidad religiosa, la redacción del RD solicita una «relación nominal»[227] o se refiere a la «identidad»[228] de estas personas, por lo que parece claro que deberá aportarse, como mínimo, los nombres y apellidos de los sujetos. Esta presunción lógica viene confirmada por el propio Real Decreto, que en su art. 14 detalla expresamente los datos que debe contener la inscripción de la identidad de los titulares de los órganos de representación, por lo menos cuando se produzca su modificación o revocación. En él se solicita expresamente: a) nombre, apellidos, DNI o NIE y domicilio; b) fecha de nombramiento y de la ratificación y aceptación; c) fecha de revocación y cese; d) sus firmas. Además, por prescripción del propio RD 594/2015, en el caso de que estos fueran extranjeros, habrá de añadirse los datos de su domicilio o residencia legal en España[229]. El RD solo prevé como documento formal para proceder a su inscripción el emitido por la entidad para certificar su condición de titular del órgano de representación. Por otra parte, debemos tener en cuenta que cuando se trata de una entidad extranjera el propio Real Decreto incrementa los requisitos exigidos a su solicitud, añadiendo la

[225] Según el art. 31.4 del RD 594/2015: «La certificación total del protocolo anejo al Registro contiene la reproducción íntegra de todos los documentos archivados presentados por los particulares y relativos a una entidad determinada. En este caso, el acceso estará limitado a la propia entidad o persona autorizada por esta, sin perjuicio de las competencias que corresponden a las autoridades judiciales y administrativas».

[226] *Vid.* art. 29 del RD 594/2015.

[227] *Vid.* art. 6.1 f) del RD 594/2015

[228] *Vid.* art. 3 c) del RD 594/2015.

[229] *Vid.* art. 6.1 f) del RD 594/2015.

obligación de aportar un certificado emitido por la entidad que incluya la relación de titulares en el país de origen y quienes han sido designados como tales en España[230]. De esta forma, se está ampliando el rango de datos personales que se gestionan, en este caso los de personas que ejercen su función en el extranjero, siendo aplicables del mismo modo las previsiones del RGPD, como vimos al explicar el criterio territorial de aplicación del Reglamento, dado que el responsable del tratamiento se encuentra dentro del territorio de la UE.

En la actualidad, la inclusión de esta información se presenta como preceptiva en el procedimiento de inscripción de una entidad, a diferencia de lo que ocurría en el RD 142/1981 cuya inscripción era voluntaria. La transformación de su carácter potestativo a obligatorio tiene su fundamento en un interés específico de la propia persona y de la entidad que, de hecho, ya servía en el régimen anterior para incentivar su inscripción: asociar a su inscripción la posibilidad de obtener una certificación emitida por el responsable del RER donde se acreditaba su condición como representante de la entidad. En realidad, fue la utilidad práctica e importancia que las propias entidades concedieron a su inclusión en el expediente registral la que impulsó su inclusión en el procedimiento registral [231] hasta que definitivamente aparece prescrita en el nuevo Reglamento, bien como requisito inicial de la inscripción de una entidad[232] bien como acto inscribible[233]. Por lo tanto, en esta ocasión partimos de la base de que su inclusión en el expediente registral resulta obligatoria, no depende de la voluntariedad inicial del sujeto, por lo que no puede deducirse la existencia de un consentimiento tácito. En todo caso, además, habrá que cuidar que a la hora de ceder sus datos personales se emite el consentimiento en los términos establecidos.

Como en los casos anteriores, su previsión dentro de un sistema de reconocimiento de entidades religiosas podría llevarnos a señalar que la finalidad de incluir los datos de los *titulares de los órganos de representación*[234] tiene una dimensión más institucional que personal. Sin embargo, primero no debemos olvidar lo que acabamos de señalar, según las propias prescripciones del RD esta acción conlleva un resultado o consecuencia práctica para el sujeto, pero además también lo tiene

---

[230] *Vid.* art. 9 b) del RD 594/2015.

[231] *Instrucción de 4 de junio de 2014, de la Dirección General de Cooperación Jurídica Internacional y Relaciones con las Confesiones, por la que se establecen determinados procedimientos en el Registro de Entidades Religiosas. BOE* n.º 145, de 16 de junio de 2014, pp. 45362 a 45363.

[232] *Vid.* art. 6.1 f) del RD 594/2015.

[233] *Vid.* art. 3 del RD 594/2015.

[234] Con carácter previo, ya se pronunció la AEPD en su Informe 486/2005, sobre la posibilidad de generar un fichero específico para contener los datos de los titulares de los órganos de representación de conformidad con la LOPD 1999, basculando sobre la existencia de consentimiento.

para la Administración. Así, *no solo se facilita un interés personal del sujeto concernido, acreditar su condición, sino que además cumple con el interés general de facilitar la interacción las comunidades religiosas con la Administración del Estado y simplificar su relación mediante la identificación de quien puede instar la mayoría de las acciones previstas en el proceso registral,* según las directrices del propio RD, *o a quien dirigirse en el caso de comunicación oficial.* Sin embargo, que el Estado intervenga como institución acreditadora de una condición que forma parte de la autonomía organizativa de la entidad supone plantearnos su posible interferencia con el *principio de separación* previsto en el sistema de *aconfesionalidad* o *laicidad positiva* español[235]. Y no solo ello, sino que en realidad será la entidad la responsable de informar de tal hecho, con la emisión de su certificado como documento necesario para la inscripción. Podría suceder que en caso de modificación o sustitución y sin que se haya producido notificación por parte de la entidad al Registro, la Administración pública esté acreditando una condición que no es cierta, lesionando la *exactitud* de los datos como principio esencial de la protección de datos. Es cierto que el RD utiliza una fórmula que le permite eximirse de esa responsabilidad: «*En las certificaciones que se expidan para acreditar la representación legal de una entidad habrá de constar la fecha de inscripción del representante o representantes, indicando expresamente que, con posterioridad a esa fecha, no se ha recibido en el Registro ninguna comunicación que modifique la representación de la entidad*». Si bien, a efectos de protección de datos, esta cláusula no le exime de la responsabilidad de establecer un plazo, los trámites y documentos adecuados para concretar el almacenaje los datos y su exactitud (adecuación, actualización, etc.), en el mismo sentido que lo debería ser previsto para el *ministro de culto*, como veremos a continuación.

— Respecto a los *ministros de culto*[236] el art. 18 del RD 594/2015 sostiene que, con carácter potestativo, se «*podrán*» anotar los *ministros de culto* de las enti-

[235] En determinación de este sistema, las distintas posiciones y sus consecuencias *Vid.* CATALÁ RUBIO, Santiago, «Aconfesionalidad y laicidad, dos principios del Derecho Eclesiástico español», *Anuario de derecho eclesiástico del Estado*, n.º 24, 2008, pp. 363 a 386; FERNÁNDEZ-CORONADO, Ana y SUÁREZ PERTIERRA, Gustavo, *Identidad social, pluralismo…», op. cit.*. FERRER ORTIZ, Javier, «Aconfesionalidad y laicidad: ¿Nociones coincidentes, sucesivas o contrapuestas?», *Cuadernos de Derecho judicial. Estado aconfesional y laicidad*, n.º 1, 2008, pp. 391 a 425; LLAMAZARES FERNÁNDEZ, Dionisio, *Derecho de libertad de conciencia I. Conciencia, tolerancia y laicidad,* Civitas, Pamplona, 2011, pp. 46 a 354, PALOMINO, Rafael, «Laicidad y ciudadanía», *Anuario de derecho eclesiástico del Estado*, n.º 24, 2008 pp. 337 a 362, *Vid.* pp. 339 y ss.

[236] Para una caracterización jurídica de la figura en el ordenamiento jurídico español puede verse MOTILLA DE LA CALLE, Agustín, *Ministros y lugares de culto*, en IBÁN PÉREZ, Iván Carlos, PRIETO SANCHÍS, Luis, MOTILLA DE LA CALLE, Agustín, Manual de Derecho eclesiástico, Trotta, Madrid, 2016, pp. 179 a 200; GONZÁLEZ SÁNCHEZ, Marcos, *Los Ministros de culto en el ordena-*

dades religiosas inscritas que posean residencia legal en España y, con carácter obligatorio, se «*deberán*» inscribir aquellos que estén habilitados «(…) para realizar actos religiosos con efectos civiles»[237]. A diferencia de los casos anteriores, en este supuesto no encontramos ninguna referencia directa o indirecta a qué debe inscribirse (no habla de relación nominal, ni de identidad, etc.) y su inscripción será potestativa en unos casos y obligatoria en otros. Tratando de resolver ambas cuestiones consideramos que será necesario hacer una determinación exacta de qué datos habrá de aportar el *ministro de culto* que decida o deba inscribirse, partiendo de la lógica de que, como mínimo, deberá identificarse (como información adicional, por ejemplo, podría ser necesario identificar su domicilio o, en su defecto, el lugar en el que ejerce su labor como *ministro de culto*, etc.). En todo caso, el RD 594/2015 no se refiere a ningún dato específico ni documento que lo contenga, tan solo considera que para practicar la inscripción deberá aportarse: a) la certificación de la Iglesia, Confesión o Comunidad religiosa a la que pertenezca en la que se acredite su condición de *ministro de culto*; b) el visto bueno del órgano competente en España, si se trata de entidades integradas en una Federación.

Por su parte, en aquellos casos en los que la inscripción sea voluntaria, nuestra opinión es que no será suficiente con el consentimiento tácito que se deriva de su solicitud, como sucede en el caso de ser obligatorio, sin duda deberá cumplir con lo previsto para estos casos en el marco de la protección de datos.

De los resultados previstos que produce la identificación e inscripción de la figura de *ministro de culto* podemos inferir tres posibles finalidades o intereses:

a) uno más específico o personal, que beneficia a la persona que mantiene la relación con la entidad inscrita: la posibilidad de utilizar su inscripción como elemento para acreditar la condición de *ministro de culto*. Como sabemos, el propio Reglamento prevé la posibilidad de solicitar y expedir una certificación, según los términos generales previstos para desarrollar la publicidad formal en el RER, que servirá para acreditar su condición de *ministro de culto*. Sin embargo, esta cuestión también nos traslada a la necesidad de valorar la incompatibilidad de esta actuación pública con el sistema de *aconfesionalidad* o *laicidad positiva* previsto en el marco constitucional español, siendo el Estado (la Administración) quien está actuando como institución encargada de acreditar una condición propia de la organización interna de una entidad religiosa. Ciertamente la certifica-

miento jurídico español, Centro de Estudios Políticos y Constitucionales, Madrid, 2003 y sobre las actuales necesidades de revisar su régimen jurídico *Vid.* del mismo autor «Cuestiones revisables de los acuerdos de cooperación con las confesiones religiosas minoritarias: los ministros de culto», *Revista General de Derecho Canónico y Derecho Eclesiástico del Estado*, n.º 44, 2017.

[237] *Vid.* art. 18. 1 del RD 594/2015.

ción tendrá validez como prueba suficiente para acreditar dicha cualidad por un periodo exclusivo de dos años, prorrogable por periodos similares, siendo la entidad religiosa la responsable de comunicar la baja del *ministro de culto* (en un plazo máximo de un mes desde que se produzca) y solicitar la cancelación de su inscripción. Estas circunstancias previstas en el RD 594/2015 nos lleva a la idea de recordar la necesidad de reforzar el *principio de calidad* de datos, con la consiguiente previsión de informar al sujeto y establecer los plazos y requisitos para actualizar los datos, y concretar el plazo de dos años como periodo de tiempo máximo para almacenar los datos en cumplimiento de su objetivo.

b) otro intermedio entre el interés personal y el interés público general como fundamento para legitimar la recogida y tratamiento de datos: el ejercicio de sus derechos en el ámbito del Derecho laboral o de la protección social, en virtud de los dispuesto en los acuerdos de cooperación firmados con las confesiones[238].

c) otro genérico o de interés público general: la necesidad de acreditar y contar con una relación de aquellas personas que están autorizadas para realizar actos con efectos jurídico-civiles y cumplir con las actividades previstas en los acuerdos para facilitar la asistencia religiosa. Esta cuestión no solo tiene un alcance interno para la entidad, sino también externo o de interés general, la seguridad jurídica que puede otorgar al proceso de reconocimiento de efectos a negocios jurídicos religiosos en el ordenamiento civil, habiendo pasado por un proceso previo de inscripción las personas encargadas de realizarlo[239]. Se construye así un elemento más que ayuda a divisar el interés público que puede tener la recopilación y uso de estos datos.

4. A MODO DE PROPUESTA

Considerando todas estas circunstancias y retomando las ideas que hemos extraído de nuestro estudio general, nuestra propuesta parte de la idea de que a pesar de que la regla general es prohibir el tratamiento de los datos religiosos

[238] *Vid.* LLAMAZARES FERNÁNDEZ, Dionisio, *Derecho de libertad de conciencia II...*, *op. cit.*, *Vid.* pp. 361 y 362; RODRÍGUEZ BLANCO, Miguel, «La protección social de los Ministros de culto», en VV. AA. (Motilla del Calle, A. –Coord.–), *La jurisprudencia del Tribunal Europeo de Derechos Humanos en torno al derecho de libertad religiosa en el* ámbito laboral, Comares, Granada, 2016, pp. 225 a 256.

[239] Hasta tal punto que la doctrina ya ha reparado en (re)afirmar que la seguridad jurídica que otorga la inscripción podría avalar la extensión del reconocimiento a los matrimonios celebrados en forma religiosa previstos en la Ley de Jurisdicción Voluntaria sin necesidad de añadir el requisito de «*notorio arraigo*», *Vid.* PONS-ESTEL TUGORES, Catalina, «Novedades legislativas en torno a la eficacia civil del matrimonio religioso en España» en *Revista de Derecho Civil*, Vol. III, n.º 2 (abril-junio, 2016), pp. 171 a 185, *Vid.* p. 183.

y que caben muchas dudas sobre la adecuación técnica de su inclusión en una normativa que regula el reconocimiento de las personas jurídicas, la opción de prever un régimen de protección de datos aplicada por el legislador al tratar el sistema de reconocimiento de las entidades religiosas no es una medida desacertada e incorrecta. Lo primero que deberíamos solventar es su diseño técnico, que requiere su concreción y desarrollo legislativo adecuado. Varias razones nos llevan a sostener esta afirmación:

1.º Según la normativa europea analizada la prohibición general de tratar los datos ideológicos y religiosos podrá ser excepcionada cuando se disponga del consentimiento explícito del interesado, pero en el caso español la nueva LOPD 2018 advierte que ya no es posible excepcionar esta prohibición por el mero hecho de disponer del consentimiento del sujeto[240]. Este hecho invalida las disposiciones del RD 594/2015 que se ajustan exclusivamente al marco europeo al requerir exclusivamente la existencia del consentimiento y hace necesario, cuando menos, modificar el texto del precepto, para concretar jurídicamente un fundamento del tratamiento basado en algunas de las excepciones previstas en la normativa general para habilitar su tratamiento o, en su caso, sustituirlo por una legislación específica que contuviera *ex novo* todos los extremos, teniendo en cuenta lo que hemos dicho al inicio de este apartado. Desde esta perspectiva, atendiendo a la LOPD 2018 *el fundamento que podría utilizar una norma específica para legitimar el tratamiento de los datos en el contexto de la gestión de la diversidad religiosa tendría que ser:*

*a) el cumplimiento obligaciones del responsable del tratamiento o el ejercicio de derechos del interesado en el ámbito del Derecho laboral y de la seguridad y protección so*cial. Aunque esta circunstancia, por ejemplo, puede ser una de las causas ligadas al tratamiento de *los ministros de c*ulto, la Administración pública, como parte de un Estado laico o aconfesional, no debería inmiscuirse en esa relación interna, siendo una posible opción buscar un procedimiento para conectar un registro interno de la confesión, donde se contuvieran esos datos, con el de la Administración. Esto, lo que además facilitaría la aplicación de procesos *de seudonimiza*ción que solo podrían ser desbloqueados con la información adicional que obrará en los registros internos de las confesiones, factibles según la normativa de protección de datos actual. Este nivel de garantía se incrementaría en el caso de cesión de los datos, que

[240] Como por ejemplo se mantenía en varios informes de la AEPD: sobre el carácter de sacerdote *Vid.* Informe 44/2004, p. 3, sobre representantes *Vid.* Informe 486/2006.

deberían contar con consentimiento expreso, y por su condición de archivos inviolables garantizado en alguna disposición acordada, por lo que debería extenderse en la norma específica.

b) el tratamiento sea realizado por una entidad, asociación, fundación u organismo s*in ánimo de lucro con fines religi*osos y lo haga sobre los datos de sus miembros actuales o antiguos o personas que por sus fines mantienen relaciona con ellas para desarrollar sus actividades legítimas con las debidas garantías. Esta opción, que se añade a la anterior, podría llevarnos a la posibilidad de que la norma dispusiera las condiciones a través de las cuales la información que obrará en un registro de la propia entidad pudiera ser transferido al registro público, aplicando además un sistema de cifrad*o o seudonimiza*ción que ayudaría a asegurar el carácter anónimo de los datos. Este procedimiento podría desarrollarse en ejercicio del derecho de portabilidad, pero no es conveniente ya que supone el traspaso definitivo de los datos de un fichero a otro por voluntad del sujeto concernido, o mediante una cesión ordinaria contando con el imprescindible consentimiento expreso y por escrito de los interesados, para lo que debería ser expresamente informado de cuáles serán los objetivos del traspaso, los destinatarios, sus posibles usos y consecuencias.

c) que los datos s*ean manifiestamente públicos* por el interesado;

d) el tratamiento sea necesario para cumplir un interés público esencial.

Como hemos anunciado, podemos considerar con carácter general que el tratamiento de estos datos podría estar ligado *al interés público* que supone la labor de promoción y gestión de la diversidad religiosa que desarrolla la Administración, engarzada en el art. 9.2 y 16.3 de la CE y 2.3 de la LOLR. En este caso, sabemos que algunas de las personas cuyos datos son requeridos intervienen en el pleno ejercicio del derecho, aunque no como garantes públicos sino como participantes imprescindibles e insustituibles desde la dimensión confesional. Por ejemplo, a efectos más prácticos, como elemento expresamente previsto en el art. 2.3 de la LOLR para el desarrollo del derecho, cumplen el papel esencial de ser los encargados de prestar el servicio en cuestiones básicas como la asistencia religiosa[241]. Tampoco debemos olvidar que la tendencia actual es incrementar la atención sobre estos elementos confesionales, *los ministros de culto, lugares de culto*[242], etc., por su importancia en la concreción de modelos de integración

[241] Sobre la consulta de los datos de pacientes que solicitan asistencia religiosa en centros hospitalarios ya tuvo la oportunidad de pronunciarse la AEPD en su informe 287/2008, *Vid*, especialmente las pp. 30 y 32.

[242] En esta cuestión es una referencia imprescindible RODRÍGUEZ BLANCO, Miguel, *Libertad religiosa y confesiones el régimen jurídico de los lugares de culto*, Boletín Oficial del Estado, Madrid, 2000.

propios de las sociedades multiculturales[243]. En todo caso, al desarrollar esta normativa debemos tener en cuenta que solo podrá considerarse que el *tratamient*o de los datos está legítimamente *fundad*o en el cumplimiento de una *misión realizada en interés público* cuando derive de una competencia atribuida por una norma de rango legal, lo que nos devuelve a la idea de que sería conveniente sustituir la mera *remisión formal* del RD 594/2015 a la legislación sobre protección de datos por una disposición específica que, de conformidad con la LOPD 2018 y el RGPD, sea proporcional al objetivo perseguido, se respete en lo esencial el derecho a la protección de datos y establezca las medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.

2.º Según el *Convenio 108* el modelo de protección de datos podría ser aplicado a las personas jurídicas a instancias de cada Estado. Se trata de una mera hipótesis, pero, como sabemos, ya tuvo su impacto sobre el legislador español en el proyecto de la primera ley sobre protección de datos. Es cierto que esta afirmación/posibilidad queda neutralizada por la propia regulación actual, que mantiene su limitación a las personas naturales, pero consideramos que podría ser interesante retener este dato. No obstante, ni siquiera sería necesario impulsarlo, ya que los asuntos previstos que hasta el momento se han puesto encima de la mesa se refieren al tratamiento de datos de personas naturales que tienen relación con las personas jurídicas, no sobre las confesiones en sí. En todo caso, evitar que se genere confusión sobre la finalidad del tratamiento al incorporarse en una norma sobre reconocimiento de personas jurídicas apoyaría nuestra propuesta de aprobar una disposición específica, separada del RD 594/2015, que regulara los extremos en los que se concretaría el modelo de protección.

3.º Que debamos garantizar el derecho de protección de datos no supone blindarlo hasta evitar o prohibir cualquier tratamiento, sino en la necesidad de extremar las precauciones y disponer los requisitos necesarios cuando se trate de construir una disposición jurídica que asegure el equilibrio adecuado entre el uso de los datos para una finalidad legítima y la protección de los derechos de las personas. Para ello *sería necesario concretar el contenido de la legislación con los siguientes extremos:*

a) una adecuada identificación de quien puede ostentar la condición de sujeto y sus requisitos de capacidad. La condición de persona natural es un

[243] Contreras Mazario, José María, «Sociedades multiculturales y modelos de integración: dos casos paradigmáticos para la inclusión: lugares de culto (mezquitas) y personal religioso (imames)» *Laicidad y Libertades. Escritos jurídicos,* n.º 18, 2018, pp. 45 a 83.

requisito general, pero, además, deberíamos aclarar que deberá tener, como mínimo, 16 años de edad. Aunque este último extremo parezca insignificante lo cierto es que la idea de mayoría de edad ya se tiene en consideración de forma expresa en el caso de las personas que avalan la fundación de la entidad, pero no se menciona expresamente ni en los *titulares de los órganos de representación* ni en los *ministros de culto*, por lo que podría extenderse a su concreción en particular y en el resto de los casos previsto en esta propuesta de normativa. Y aunque la necesidad de ser mayor de edad se dedujera de las responsabilidades y actividades que deben realizar las personas mencionadas, cosa que no siempre ha de ser así en cuanto a los *ministros de culto* especialmente de confesiones no tradicionales en nuestro territorio, podría ser útil que la disposición normativa también recordara ese extremo o, en su defecto, que en el formulario de inscripción se habilite un espacio solicitando la fecha de nacimiento o se aporte, como anexo a la solicitud, un documento que acredite su mayoría de edad. Por último, consideramos que también convendría aclarar conceptualmente qué se debe entender por *titular del órgano de representación* y por *ministro de culto*, como mínimo con una remisión formal a los Acuerdos que a todas luces resulta insuficiente, pues tan solo cubriría los casos de las confesiones firmantes o comunidades que formen parte de ellas.

b) un conjunto de disposiciones que aclaren los requisitos formales y materiales de la emisión del consentimiento, donde se indique que:

— la solicitud de consentimiento se expresará en términos claros y sencillos y habrá de realizarse en un formulario específico;

— no será válido el silencio, las casillas de preselección o la inactividad como medio de acreditar la existencia de consentimiento;

— que la emisión del consentimiento será necesario para cada una de las actividades que se vayan a llevar a cabo, lo que como veremos requerirá incluir esa información en el formulario;

— y, finalmente, que le asiste al sujeto el derecho a retirar el consentimiento, para lo que el responsable del tratamiento le informará de forma clara y sencilla de la forma de hacerlo y con la misma facilidad que para solicitarlo.

Si tomamos como referencia el modelo de solicitud recientemente adaptado para solicitar la inscripción de la entidad[244], comprobaremos que algunos de

[244] https://www.mjusticia.gob.es/cs/Satellite/Portal/1292428829453?blobheader=application%2Fpdf&blobheadername1=Content-Disposition&blobheadername2=Grupo&blobheadervalue1=attachment%3B+filename%3DSolicitud_de_Actuacion_en_el_Registro_de_Entidades_Religiosas. PDF&blobheadervalue2=Docs_Llibertad+religiosa

estos elementos ya se han incluido. Si bien es cierto que hay algunas previsiones que, en los términos de nuestra propuesta, deberían ser modificadas y adaptadas a la nueva LOPD 2018:

En primer lugar, salvo error por nuestra parte no existe una previsión o formulario específico para las personas que se incluyen como aval, por lo que sería necesario prever unas disposiciones que se refirieran a la forma en la que se debe concretar la condición por la que facilitan sus datos –avales, miembros, fieles, etc.– y los requisitos que debe cumplir el documento anexo al acta de constitución por el que la entidad informa de tal extremo.

En segundo lugar, según los términos en los que está prevista la cesión de datos en el apartado de «información adicional sobre protección de datos» que se incluye al final del documento, estos se podrán ceder a cualquier interesado, ya que los datos son públicos, excepto el dato identificativo DNI. Como hemos señalado previamente, consideramos que no en todos los casos la información podrá (deberá) ser pública y por ese motivo, nuestra recomendación es que se retire o matice esta afirmación y la mayoría de los datos se incluyan en el expediente anejo, de tal forma que su inclusión se adecuaría a su condición de dato adicional a la verdadera inscripción de la entidad y siguiendo las reglas de publicidad del registro, que no admite la consulta genérica de expedientes, su cesión por medio de una certificación total del protocolo anejo se limitaría a la propia entidad o persona autorizada por ella, etc.

En tercer lugar, en cuanto a los fines del tratamiento, y también como elemento de su legitimación, habría que aclarar las diferentes posibilidades que antes hemos mencionado para cada caso, concretando en cada una de ellas la finalidad personal que puede legitimar su inclusión o la genérica de interés público. Lo mismo sucedería con la determinación del plazo de conservación, que no se restringe en el documento oficial. Como hemos señalado previamente, en nuestra opinión podría fijarse un plazo relativamente corto para las personas que avalan la fundación, a lo sumo dos años, dado que esos datos cumplen una finalidad en el proceso de certificación de su fundación o establecimiento en España cuando se procede a inscribir la entidad, un plazo indeterminado para los titulares de los órganos de representación, con indicación de que concluirá cuando se produzca y se notifique convenientemente la sustitución interna en la entidad y, si se quiere, con la sugerencia de un plazo mínimo para instar a su actualización y, por último, un plazo de dos años para los *ministros de culto*, prorrogable automáticamente cuando se produzca la actualización.

En cuarto lugar, según el Manual de usuario para el Registro de Ministros de Culto consultado en la página web[245], la emisión del consentimiento para este caso se realiza mediante la selección de una casilla donde se informa que «Doy mi consentimiento para que mis datos se incluyan en el Registro de Entidades Religiosas a efectos de su anotación como ministro de culto y para la comunicación derivada de la publicidad del Registro de Entidades Religiosas», refiriéndose como marco normativo a la LOPD 1999. Por ello, consideramos necesario (si no se ha realizado ya directamente en la aplicación y es un mero problema de actualización del manual) actualizar este proceso e incluir la información que hemos señalado con anterioridad (todo lo relativo al responsable del tratamiento, los fines, la legitimación, etc.) en el mismo sentido que el documento genérico para solicitar las actuaciones en el RER.

c) un conjunto de disposiciones destinadas a aclarar los extremos en los que deberán ser informados los sujetos concernidos de sus derechos, teniendo en cuenta que deberán conocer:

— la finalidad del tratamiento y su base o fundamento jurídico, como ya viene previsto en el modelo de solicitud actualizado. Sin duda, en línea con lo expuesto en ese documento, el tratamiento de los datos puede dotarnos de un sistema de reconocimiento de las entidades religiosas más efectivo y útil para la Administración, pero en nuestra opinión el *interés público esencial* y su legitimación se refuerza al identificarlo con el objetivo de lograr un mejor y pleno ejercicio del derecho fundamental (art. 9.2 y 16.3 CE), facilitando el ejercicio colectivo del derecho de libertad religiosa y específicamente el derecho de asociación religiosa en garantía del art. 2 y 6 de LOLR, y construir un modelo integrador para la gestión de la diversidad en nuestra sociedad multicultural.

— la categoría de datos que están siendo tratados, un requisito que no está del todo desarrollado en el modelo solicitud, salvo la referencia a que el DNI no será objeto de cesión;

— el plazo para conservar esos datos y los criterios que han sido utilizados para determinarlo, pudiéndose adoptar los términos en los que hemos concretado nuestra propuesta previamente;

— el origen de sus datos cuando no hayan sido facilitados por el sujeto;

— y, finalmente, si se han adoptado o se van a adoptar decisiones automatizadas, como la elaboración de perfiles. Ciertamente ya viene previsto en el mode-

[245] https://sede.mjusticia.gob.es/cs/Satellite/Sede/1292428868177?blobheader=application%2Fpdf&blobheadername1=Content-Disposition&blobheadervalue1=attachment%3B+filename%3DManual_de_usuario_para_Ministros_de_Culto_y_Representantes_Legales. PDF

lo de solicitud pero, como dijimos previamente, en nuestro caso incluiríamos la relación de derechos que asisten al interesado en el caso de que se desarrollara.

d) También deberá concretarse la facultad de que dispone el sujeto de rectificar los datos cuando se haya considerado que son inexactos o parciales o incluso la posibilidad de completarlos con una declaración adicional, tal y como viene reflejado en el documento oficial. Por último, deberá configurarse el derecho a borrar los datos cuando ya no sean necesarios para los fines por los que fueron recabados, cuando se hayan tratado ilícitamente o se oponga al tratamiento.

e) un conjunto de disposiciones destinadas a concretar las responsabilidades del encargado del tratamiento, señalando expresamente que será quien *determine los fines y los medios para llevar a cabo el procesamiento* de los datos. Además, es regulación deberá expresar de forma clara:

— su obligación de implementar medidas técnicas y organizativas, como por ejemplo la *seudonimización* y *minimización*;

— de mantener un registro (archivo) de todas las categorías de actividades de tratamiento desarrolladas bajo su responsabilidad;

— de realizar una evaluación previa al tratamiento y del impacto que las operaciones de tratamiento previstas puedan tener sobre el derecho de las personas;

— de asegurar el adecuado control del acceso a los equipamientos, a los soportes de los datos, a su almacenamiento, al tiempo que medidas para asegurar la integridad de los datos. Este último, se trataría de un elemento más que fundamentaría la no viabilidad de las consultas genéricas y el no acceso público de estos datos, recomendado un fichero específico.

Por último, sería conveniente incluir una disposición para recordar su sujeción al deber de confidencialidad y al *deber de secreto profesional.* Deberes que habrán de prolongarse en el tiempo, con independencia de que la relación del obligado con el responsable hubiera finalizado.

f) un conjunto de disposiciones donde se regule la designación, competencias y actuación del *Delegado de protección de datos en el Registro de Entidades Religiosas,* figura imprescindible en este caso ya que se cumplen las dos condiciones previstas por la LOPD 2018 para su establecimiento: el tratamiento lo realiza una autoridad u organismo público cuyas actividades principales son el tratamiento a gran escala de categorías especiales de datos.

Junto a estas consideraciones jurídicas esenciales sería necesario, que el responsable del tratamiento desarrollará una serie de actuación prácticas en dos puntos:

1.º Facilitar al interesado una *información básica* y una dirección electrónica u otro medio de contacto a través del cual puedan obtener el resto de información que exista en su caso, como de hecho ya prevé el documento oficial de solicitud. Esa *información básica* que contener:

a) la identidad del responsable y, en su caso, su representante;
b) la finalidad del tratamiento;
c) la posibilidad de ejercer los derechos establecidos en la normativa;
d) si los datos fueran a ser tratados para e*laborar perfiles*, el derecho a oponerse a la adopción de decisiones individuales automatizadas que le produzcan efectos jurídicos o le afecten significativamente;
e) las categorías de datos objeto de tratamiento y la fuente de la que proceden esos datos cuando no hayan sido obtenidos directamente del interesado.

2.º *Crear un Registro de las actuaciones de tratamiento desarrolladas.*
3.º Diseñar un *Código de conducta* donde:

a) se defina las condiciones de un tratamiento leal y transparente;
b) se aclare los intereses legítimos perseguidos por el responsable;
c) se concrete el procedimiento de recogida de datos personales;
d) se informe de los procesos de *seudonimización* de datos personales;
e) se identifique la información que será proporcionada al público y a los interesados;
f) se explique cómo se ejercen los derechos de los interesados;
h) se desarrolle la configuración de las medidas para garantizar la seguridad o para diseñar los procedimientos de protección desde el diseño y por defecto, etc.

La condición más práctica de estas dos últimas acciones justificaría establecer meramente una disposición en la legislación específica que recordará a la Administración su necesario desarrollo e incluirlo, como se hace con el modelo de solicitud genérico, entre los documentos prácticos que se utilizaran en el procedimiento, en la página web de la Subdirección, etc.