VISTO BUENO DEL TUTOR DEL TRABAJO DE FIN DE MÁSTER

El Profesor **D. Eduardo Ángel Risueño Díaz**, como Tutor del Trabajo Fin de Máster titulado *"LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL EN EL ÁMBITO DE LAS ADMINISTRACIONES PÚBLICAS"*, realizado por **Natalia Hernández Delgado**, informa favorablemente el mismo, dado que reúne las condiciones necesarias para su defensa.

En cumplimiento de lo previsto en la Guía docente de la asignatura, se propone la calificación de 8, en atención al estudio profundo y sistemático de una materia específica y de recientes y sustanciales cambios normativos *(Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales)*, en el que aborda las figuras de nueva creación (Delegado de Protección de Datos, Evaluación de Impacto sobre la protección de datos, derecho al olvido, ...) con cita de numerosas opiniones doctrinales e Instrucciones y Guías de la Agencia Española de Protección de Datos, así como de las Sentencias recaídas al respecto.

En La Laguna, a 27 de enero de 2020.

NOMBRE RISUEÑO DIAZ EDUARDO ANGEL - NIF 43773000K

Firmado digitalmente por NOMBRE RISUEÑO DIAZ EDUARDO ANGEL - NIF 43773000K
Fecha: 2020.01.27 11:24:56 Z

C/ Padre Herrera s/n
38207 La Laguna
Santa Cruz de Tenerife. España

T: 900 43 25 26

ull.es

Máster Universitario en Abogacía

Facultad de Derecho

Ilustre Colegio Abogados de Santa Cruz de Tenerife

Curso: 2019/2020

Convocatoria: Enero

LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL EN EL ÁMBITO DE LAS ADMINISTRACIONES PÚBLICAS.

-

THE PROTECTION OF PERSONAL DATA IN THE FIELD OF PUBLIC ADMINISTRATIONS.

Realizado por la alumna Natalia Hernández Delgado.

Tutorizado por el Profesor Don Eduardo Ángel Risueño Díaz.

Departamento: Disciplinas Jurídicas Básicas.

Área de conocimiento: Derecho Administrativo.

ABSTRACT

The main purpose of this research is to offer a systematic analysis of data protection regulations from the perspective of the Public Administration against the citizen as the holder of personal data. On the other hand, security measures in data processing will be examined, as well as the mechanisms to avoid personal data breach and keep an adequate control of the data in accordance with the principles, duties and obligations that affect the Public Administration.

In addition, the figure of the Data Protection Officer that takes on special importance within public entities will be taken into account as it will be responsible for ensuring that they comply with their obligations and duties. Finally, the sanctioning regime and the administrative resolutions issued in the matter will be analyzed as they constitute a reference to assess compliance with data protection regulations.

Keywords: Data protection, Public Administration, controller/processor, processing of personal data and duty of transparency.

RESUMEN

El objetivo principal del presente estudio consiste en ofrecer un análisis sistemático de la normativa de protección de datos desde la perspectiva de la Administración Pública frente al ciudadano como titular de los datos personales. Por otro lado, se examinarán las medidas de seguridad en el tratamiento de datos, así como los mecanismos para evitar brechas de seguridad y llevar un adecuado control de los datos en atención a los principios, deberes y obligaciones que debe respetar la Administración Pública.

Además, se tomará en consideración la figura del Delegado de Protección de Datos que cobra especial importancia dentro de las entidades públicas pues será el encargado de velar por que éstas cumplan con sus obligaciones y deberes. Por último, se analizará el régimen sancionador y las resoluciones administrativas emitidas en la materia ya que constituyen una referencia para evaluar el cumplimiento de la normativa en protección de datos.

Palabras clave: Protección de datos, Administración Pública, responsable/encargado, tratamiento de datos personales y deber de transparencia.

ÍNDICE

1.- Introducción.

El presente trabajo tiene por objeto el análisis jurídico de la normativa de protección de datos desde su ámbito de aplicación en la Administración Pública. Cualquier ente público, en el desarrollo de sus funciones y el ejercicio de sus competencias, necesita recabar y tratar datos. Gran parte de estos datos tienen la consideración de datos personales, motivo por el cual resulta de aplicación la normativa objeto de estudio a la Administración Pública.

Aparte de la protección de datos, las nuevas tecnologías plantean nuevos desafíos en el ámbito de la seguridad pública, marco en el cual se desarrolla el reciente Real Decreto-ley 14/2019, de 31 de octubre, que se aprueba para garantizar el interés general y, en particular, la seguridad pública con el objeto de una adecuada prestación de los servicios públicos y para que la administración digital sea empleada para fines legítimos que no comprometan los derechos y libertades de los ciudadanos[1].

El meritado Real Decreto-ley 14/2019 se encuentra avalado por la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional que reconoce los riesgos asociados a las nuevas tecnologías como uno de los principales desafíos de la sociedad actual. Entre las nuevas amenazas que afectan a la seguridad pública se encuentran las *«asociadas al ciberespacio, tales como el robo de datos e información, el hackeo de dispositivos móviles y sistemas industriales, o los ciberataques contra infraestructuras críticas»* y, por otro lado, *«la hiperconectividad actual agudiza algunas de las vulnerabilidades de la seguridad pública y exige una mejor protección de redes y sistemas, así como de la privacidad y los derechos digitales del ciudadano»*[2].

Sobre esta última cuestión -la privacidad y los derechos digitales del ciudadano- versa este trabajo, al igual que la necesaria correlación de la actividad de las Administraciones Públicas para preservar la seguridad pública en este campo de la información digital minimizando los riesgos para los ciudadanos. Por este motivo, el

[1] Preámbulo del Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.
[2] Ídem.

principal texto legal a analizar será la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, así como el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Por otro lado, dentro de los fines de la normativa de protección de datos se encuentra el deber de información, encontrándose íntimamente relacionado con la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, texto legal previo a la actual modificación legislativa en protección de datos. En especial, afecta a las Administraciones Públicas en lo que refiere a la transparencia en su gestión, así como el acceso a los expedientes administrativos de los ciudadanos.

Asimismo, se analizarán los procedimientos ante la vulneración de protección de datos y el régimen sancionador finalizando con un sucinto análisis de las resoluciones emitidas en vía administrativa acerca de la materia objeto de estudio de este trabajo.

2.- Conceptos y principios relativos a la protección de datos.

Con carácter previo se definirán los conceptos básicos de este estudio como pueden ser dato personal, responsable y encargado, tratamiento de datos, interesado o afectado, sin olvidar el contenido del derecho a la protección de datos y sus principios inspiradores.

La base de la protección de datos se encuentra en su reconocimiento como derecho fundamental que nace del derecho a la intimidad del artículo 18.4 de la Constitución Española y se ha configurado como un derecho que opera de manera autónoma extendiendo su garantía más allá de la dimensión constitucionalmente protegida por el artículo 18.1 de la Constitución. A este respecto, el Pleno del Tribunal Constitucional en su sentencia de 30 de noviembre de 2000 reconoció que *«el derecho a la protección de datos garantiza a los individuos un poder de disposición sobre esos*

datos […] el objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal»[3].

La meritada resolución también precisa el contenido del derecho que *«consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales (…) se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos»*[4].

A pesar de que el Tribunal Constitucional ha configurado este derecho mediante sus resoluciones, los tribunales españoles no han sido los pioneros en la materia pues ya había sido reconocido el derecho a la protección de datos en la Carta de los Derechos Fundamentales de la Unión Europea[5]. Los máximos precursores en ampliar la protección de datos han sido el Parlamento Europeo y el Consejo de la Unión Europea tras la aprobación del Reglamento (UE) 2016/679 del Parlamento

[3] Sentencia del Pleno del Tribunal Constitucional de 30 de noviembre de 2000 (RJ 2000/292). Fundamento Jurídico nº 6.
[4] Sentencia del Pleno del Tribunal Constitucional de 30 de noviembre de 2000 (RJ 2000/292). Fundamento Jurídico nº 7.
[5] El considerando nº 1 del Reglamento General de Protección de Datos señala que *«la protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental. El artículo 8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea («la Carta») y el artículo 16, apartado 1, del Tratado de Funcionamiento de la Unión Europea (TFUE) establecen que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan».*

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 (en adelante «RGPD o Reglamento»).

El Reglamento se configura actualmente como la norma básica en esta materia en el ámbito de la Unión Europea y a pesar de haber sido aprobado en 2016 no fue aplicable hasta el 25 de mayo de 2018[6] tal y como dispone el artículo 99 del mismo texto legal que además señala que el *«Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro».* Al ser directamente aplicable no requería de transposición a la normativa nacional facilitando de esta forma la homogeneización en la aplicación de las normas contenidas en el Reglamento. No obstante, resultaría inviable para el Parlamento Europeo y el Consejo de la Unión Europea que el RGPD pueda englobar la regulación de todos los aspectos necesarios para su correcta aplicación, por este motivo, se encomendó a los Estados miembros el desarrollo de sus normas con el fin de adaptar su aplicación.

A efectos de desarrollar y adaptar el Reglamento se aprobó la actual Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales[7] (en adelante «LOPDGDD»), sin embargo, el hecho que el Reglamento sea de aplicación directa ha supuesto que un número considerable de preceptos que contiene esta Ley Orgánica se limiten a la simple remisión al Reglamento. Sobre esta cuestión pudieron surgir dos situaciones, que las disposiciones del RGPD fueran tan precisas que el legislador español no considerara necesario ampliarlas y matizarlas o bien que sólo regulara aquello que no prevé el Reglamento pues la mayor novedad se encontraría únicamente en el Título X acerca de la *«garantía de los derechos digitales»* que será objeto de análisis en el siguiente apartado.

[6] El RGPD presentaba un periodo de transición de dos años para facilitar a las empresas, entidades y profesionales su adaptación.

[7] El apartado III del preámbulo de la Ley Orgánica 3/2018 utiliza los siguientes términos: *«el Reglamento general de protección de datos pretende con su eficacia directa superar los obstáculos que impidieron la finalidad armonizadora de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos. La transposición de la directiva por los Estados miembros se ha plasmado en un mosaico normativo con perfiles irregulares en el conjunto de la Unión Europea lo que, en último extremo, ha conducido a que existan diferencias apreciables en la protección de los derechos de los ciudadanos».*

Tras las consideraciones anteriores y una vez definido el derecho fundamental a la protección de datos, debe delimitarse que se entiende por dato personal y, en concreto, el RGPD en su artículo 4.1 lo define como *«toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona»*.

Esto implica que la existencia de un dato personal no lleva aparejada una coincidencia plena entre el dato y un individuo en concreto, pues basta que pueda identificarse sin mediar un esfuerzo desproporcionado. Por esta razón, el concepto no ha sido pacífico y ha propiciado el pronunciamiento de la Audiencia Nacional en su resolución de 8 de marzo de 2002 reconociendo que *«para que exista dato de carácter personal (en contraposición con dato disociado) no es imprescindible una plena coincidencia entre el dato y una persona concreta, sino que es suficiente con que tal identificación pueda efectuarse sin esfuerzos desproporcionados (...) para determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona; que los principios de la protección no se aplicarán a aquellos datos hechos anónimos de manera tal que ya no sea posible identificar al interesado»*[8].

Incluidos dentro del concepto de dato personal se encuentran aquellos datos especialmente sensibles que presentan una protección más cualificada, en específico, son los relativos a la ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico[9]. Estos datos suelen estar en manos de las Administraciones Públicas, de ahí que su especial protección por parte de los entes

[8] Sentencia de la Sala de lo Contencioso-Administrativo, Sección 1ª de la Audiencia Nacional de 8 de marzo de 2002 (RJ 2002/143289). Fundamento Jurídico nº 5.
[9] Artículo 9 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales que proviene del artículo 9.1 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.

públicos sea determinante para el cumplimiento de las previsiones del artículo 9.1 del RGPD y su análogo artículo 9 en la LOPDGDD. No obstante, su protección no presenta un alcance absoluto pues el tratamiento de estos datos sensibles[10] será posible, por ejemplo, cuando sea necesario por razones de interés público esencial, en el ámbito de la salud pública o para fines de medicina preventiva o laboral y especialmente cuando sea necesario para el adecuado ejercicio de la tutela judicial efectiva.

Por otro lado, de la definición de dato personal se extrae el concepto de interesado como ciudadano afectado por un tratamiento y acerca del tratamiento, el RGPD establece la definición de *«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»*[11].

En este mismo sentido no todo tratamiento de datos está sujeto a la normativa de protección de datos pues los tratamientos realizados de forma no automatizada quedarían excluidos del ámbito de aplicación. En este sentido se ha pronunciado en diversas ocasiones la Audiencia Nacional pues señala que *«para que una actuación manual sobre datos personales (recogida, grabación, conservación, elaboración, modificación, bloqueo etc...) tenga la consideración de tratamiento de datos sujeto al sistema de protección de la LOPD es necesario, según criterio reiterado de la Sala, que dichos datos estén contenidos o destinados a ser contenidos en un fichero, esto es, en un conjunto estructurado u organizado de datos con arreglo a criterios determinados. Si no es así el tratamiento manual de datos personales quedará fuera del ámbito de aplicación de la citada LOPD, no será un "tratamiento de datos personales" según el concepto normativo que la citada Ley proporciona»*[12].

[10] Guía sectorial de *Protección de Datos y Administración Local* publicada el 16 de mayo de 2018 por la Agencia Española de Protección de Datos, pp. 14-15.
[11] *Ex* artículo 4.2) del RGPD.
[12] Sentencia de la Sala de lo Contencioso-Administrativo, Sección 1ª de la Audiencia Nacional de 9 de julio de 2009 (RJ 2009/363726). Fundamento Jurídico 4º.

Continuando con los conceptos del presente estudio, el titular de los datos, habitualmente denominado interesado no deberá confundirse con el concepto de «interesado» que recoge la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante «LPAC»). En contraposición, cualquier sujeto, ya sea público o privado, que tome datos de los ciudadanos y realice un tratamiento sobre los mismos será responsable, por ello, la regulación legal sobre protección de datos afecta a la Administración Pública como si de cualquier responsable[13] o encargado[14] del tratamiento de datos se tratara.

Por lo que respecta a los principios inspiradores del tratamiento de datos se encuentran regulados en el capítulo II del RGPD (artículos del 5 al 7) y pueden enumerarse en los siguientes:

1º. Principio de licitud, lealtad y transparencia[15]: supone que los datos sean tratados de manera lícita, leal y transparente en relación con el sujeto, por ello, para realizar un tratamiento de datos se requiere la concurrencia de un motivo o una base jurídica que legitime el tratamiento. El motivo se identifica con el fin del tratamiento que deberá ser determinado, explícito y legítimo. Entre las causas que legitiman los tratamientos se encuentra el consentimiento del afectado, una relación contractual, una obligación legal de una empresa, el interés público o que derive del ejercicio de poderes públicos[16].

El consentimiento presenta una serie de requisitos para ser válido, en concreto, que sea emitido de forma libre; que sea específico en referencia a un tratamiento y finalidad determinada; que sea informado debiendo ser conocido por el afectado; que sea inequívoco de forma que no existan dudas acerca de la prestación

[13] En atención al artículo 4.7) del RGPD el responsable del tratamiento o responsable es definido como toda aquella persona física o jurídica, autoridad pública, servicio u otro organismo que, sólo o junto con otros, determine los fines y medios del tratamiento. Estos fines y medios del tratamiento podrán establecerse por el Derecho de la Unión o por los Estados miembros.
[14] El artículo 4.8) del RGPD define al encargado del tratamiento o encargado como la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.
[15] *Guía para el ciudadano* publicada el 7 de febrero de 2019 por la Agencia Española de Protección de Datos, pp. 7 y 8.
[16] *Ex* artículo 5 y 6 del RGPD.

del consentimiento; y que, además, sea fácil de retirar[17]. Con carácter general, el consentimiento requiere una acción positiva del ciudadano resultando no ser válido el consentimiento tácito. Sin embargo, en el caso de los datos sensibles, será necesario que el consentimiento sea explícito de forma que el responsable pueda probar que el afectado ha prestado dicho consentimiento[18].

Respecto a la lealtad y transparencia, supone que la información y comunicación que se refiera al tratamiento pueda ser accesible y fácil de comprender con la utilización de lenguaje claro y sencillo[19].

2º. Principio de limitación de la finalidad[20]: los datos deben recogerse con fines determinados, concretos y legítimos y no serán tratados ulteriormente de manera incompatible con dichos fines[21]. Esto supone que los fines no pueden verse ampliados respecto a los iniciales.

3º. Principio de minimización de los datos[22]: supone que los datos sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados[23]. No resulta lícita la obtención de datos para su simple conservación si no se prevé un tratamiento. Este principio contiene como excepción aquellos casos de archivo, investigación científica y estadística.

4º. Principio de exactitud[24]: los datos deberán ser exactos y, si fuera necesario, actualizados para que sean veraces en atención a la situación actual del

[17] Grupo de trabajo del artículo 29. Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679 de 10 de abril de 2018 (WP 259 y rev.01).
[18] AA.VV., MOSCOSO DEL PRADO MUÑOZ, J. (coord), *La Protección de Datos y la Administración Local*, «La administración local ante la gestión de la protección de datos», 1ª edición, Ed. Aranzadi, Cizur Menor, 2019, pp. 66-70.
[19] El afectado deberá conocer los riesgos del tratamiento, normas aplicables y derechos relativos al tratamiento, cómo ejercitar sus derechos y los fines del tratamiento.
[20] *Guía para el ciudadano* publicada el 7 de febrero de 2019 por la Agencia Española de Protección de Datos, p. 8.
[21] *Ex* artículo 5.1.b) del RGPD.
[22] *Guía para el ciudadano*…, op. cit., p. 8.
[23] Artículo 5.1.c) del RGPD.
[24] *Guía para el ciudadano* publicada el 7 de febrero de 2019 por la Agencia Española de Protección de Datos, p. 8.

afectado. Se evitará que los datos puedan inducir a error a través de la rectificación o cancelación que operará sin dilaciones indebidas[25].

5º. Principio de limitación del plazo de conservación[26]: la conservación de los datos se encuentra ligada a los fines del tratamiento de modo que cuando ya no sean necesarios para ese fin deberán ser eliminados. Sólo podrán conservarse los datos durante períodos más largos cuando se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos[27]. Esta excepción no supone deje de operar el principio de minimización de los datos pues este tipo de tratamientos están sujetos a garantías adecuadas como puede ser la seudonimización con el objeto de proteger los derechos y libertades de los ciudadanos.

6º. Principio de integridad y confidencialidad[28]: en el tratamiento se debe garantizar la adecuada seguridad de los datos que incluirá la protección frente a tratamientos no autorizados o ilícitos y contra la pérdida, destrucción o daño accidentales a través del uso de medidas técnicas u organizativas apropiadas[29].

7º. Principio de responsabilidad proactiva[30]: se tratará en el apartado IV al tratarse de una obligación que deben cumplir los responsables y encargados del tratamiento.

Los principios enumerados deberán inspirar cualquier tratamiento de datos personales y ser respetados por parte de los responsables y encargados, así como los derechos de los afectados que se describen a continuación.

[25] *Ex* artículo 5.1.d) del RGPD.
[26] *Guía para el ciudadano*…, op. cit., p. 9.
[27] *Ex* artículo 5.1.e) en relación con el artículo 89 del RGPD.
[28] *Guía para el ciudadano*…, op. cit., p. 9.
[29] *Ex* artículo 5.1.f) del RGPD.
[30] *Guía para el ciudadano*…, op. cit., p. 9.

3.- Derechos de los ciudadanos en materia de protección de datos.

Los derechos inherentes al tratamiento de datos personales reconocidos inicialmente comprendían el derecho de acceso, rectificación, cancelación y oposición (denominados derechos ARCO[31]), sin embargo, el RGPD que se encuentra vigente introdujo el derecho a la portabilidad, derecho de supresión o derecho al olvido y derecho a la limitación del tratamiento (por la adición de éstos últimos ahora son conocidos como ARCO-POL). Los derechos enumerados se encuentran regulados entre los preceptos 15 a 21 del citado RGPD y la LOPDGDD se limita a remitirse a estos.

No obstante, la LOPDGDD incluye un elenco de derechos bajo el título *«garantía de los derechos digitales»* (Título X) en el que engloba los nuevos derechos de la Era digital. Con el fin de centrar el objeto de estudio no se analizarán estos derechos pues afectan en mayor medida a las relaciones entre los usuarios con los proveedores de servicios de Internet, aunque cabe señalar que ha supuesto modificaciones a otras normas.

En concreto, se introducen modificaciones en la Ley Orgánica 2/2006, de 3 de mayo, de Educación y la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades por motivo del artículo 83 relativo al derecho a la educación digital que dispone lo siguiente: *«las Administraciones educativas deberán incluir en el diseño del bloque de asignaturas de libre configuración la competencia digital […] así como los elementos relacionados con las situaciones de riesgo derivadas de la inadecuada utilización de las TIC, con especial atención a las situaciones de violencia en la red».* Por otro lado, también afecta al ámbito laboral con modificaciones en el Texto Refundido de la Ley del Estatuto de los Trabajadores y en el Texto Refundido de la Ley del Estatuto Básico del Empleado Público en lo relativo al uso de dispositivos,

[31] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respeta al tratamiento de datos personales y a la libre circulación de estos datos. Esta Directiva fue derogada por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

desconexión digital, utilización de sistemas de geolocalización en el ámbito laboral, entre otros.

En el ámbito de las entidades públicas, a este respecto, el artículo 97 establece un mandato al Gobierno para que en colaboración con las Comunidades Autónomas elabore un Plan de Acceso a Internet con el objetivo de garantizar el acceso a Internet a los ciudadanos y de fomentar medidas educativas en relación con las TICs. Esta cuestión podría plantear algunos problemas debido a que el uso de redes públicas es más sensible a los ataques y posibles vulneraciones de seguridad que deberán ser tomadas en consideración con el fin de garantizar la seguridad de los usuarios[32].

A continuación, se realizará una breve exposición de los derechos de los titulares de los datos personales[33] que deberán ser respetados por la Administración Pública como responsable de los tratamientos de datos que lleven a cabo.

a) Derecho de acceso.

El derecho de acceso se encuentra regulado en el artículo 13 de la LOPDGDD y su objeto es garantizar que los afectados por un tratamiento puedan conocer que información, precisamente, está siendo tratada. Mediante solicitud del interesado, el responsable atenderá su petición facilitando una copia de los datos personales objeto de tratamiento en formato electrónico de uso común[34]. En el supuesto que la solicitud de acceso conlleve una gran cantidad de información, la Administración podrá requerir al afectado para que concrete su solicitud.

No debe confundirse con el derecho de acceso de los interesados a los expedientes administrativos que regula el artículo 53 de la LPAC ni el derecho de acceso a la información pública que regula la Ley 19/2003 de 9 de diciembre, de

[32] La Oficina de Seguridad del Internauta ofrece recomendaciones de cara al acceso a redes públicas debido a que éstas no cifran la información que transmiten propiciando que no sean seguras. https://www.osi.es/es/wifi-publica última consulta: 10/01/2020.

[33] LÓPEZ CALVO, J. (Coord*.). Derechos del interesado (Arts. 12-19 RGPD. ARTS. 11-16 LOPDGDD)*. «La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD», 2019, pp. 345-385.

[34] Guía sectorial de *Protección de Datos y Administración Local* publicada en fecha 16 de mayo de 2018 por la Agencia Española de Protección, pp. 33-34.

transparencia, acceso a la información pública y buen gobierno en su capítulo III, sección 1ª de acceso a la información pública ya que se refiere a datos de la Administración General del Estado, Administraciones de las Comunidades Autónomas y el resto de organismos del ámbito subjetivo de aplicación de dicho texto legal.

b) Derecho de rectificación.

Supone la rectificación de datos inexactos del afectado por el tratamiento sin dilaciones indebidas en los términos del artículo 14 de la LOPDGDD. La rectificación de los datos se hará extensible a los datos que hubieran sido cedidos, en ese caso, el responsable deberá notificar de la rectificación al cesionario para que en el mismo plazo realice la rectificación[35].

c) Derecho de supresión o derecho al olvido.

El derecho de supresión u olvido se equipara con el anterior derecho de cancelación. El afectado podrá ejercitar este derecho cuando desee suprimir sus datos personales cuando ya no sean necesarios en relación con los fines para los que se recabaron o cuando sean tratados de otro modo[36]. También cuando el ciudadano retire el consentimiento siempre y cuando no concurran otros motivos legítimos para el tratamiento; cuando el afectado se oponga al tratamiento; cuando los datos hayan sido tratados ilícitamente; cuando deban suprimirse para el cumplimiento de una obligación legal y, en todo caso, cuando se hayan obtenido datos de un menor de edad a través de los servicios de información o TICs. El responsable también se encargará de comunicar la supresión a cada uno de los destinatarios a los que hubiera comunicado los datos salvo que suponga un esfuerzo desproporcionado o incluso sea imposible.

Este derecho también se ha denominado derecho al olvido, aunque ya está previsto en los artículos 93 y 94 de la LOPDGDD en lo que refiere a la eliminación de

[35] El plazo máximo para atender la solicitud es de un mes, debiendo indicar los motivos por los que no ha podido atender la solicitud en plazo que podrá prorrogarse otros dos meses. Sólo podrá prorrogarse de ser necesario atendiendo a la complejidad y número de solicitudes, si bien deberá informar al afectado.

[36] Guía sectorial de *Protección de Datos y Administración Local*, op. cit., pp. 33-34.

datos de los motores de búsqueda en Internet y de los servicios de redes sociales y servicios equivalentes.

d) Derecho a la limitación del tratamiento.

El afectado podrá solicitar la limitación del tratamiento cuando impugne la exactitud de los datos personales durante un plazo que permita al responsable verificar su exactitud y cuando el afectado se haya opuesto al tratamiento ejercitando el derecho de oposición, en estos casos se suspenderá el tratamiento[37]. Por otro lado, cuando el tratamiento sea ilícito y el afectado no opte por la supresión de los datos y solicite simplemente la limitación de su uso, estos datos se conservaran. Lo mismo ocurrirá cuando el responsable ya no necesite los datos personales para los fines del tratamiento, pero el afectado si los necesite para formular los derechos mencionados.

e) Derecho a la portabilidad.

Faculta al afectado por un tratamiento para recibir los datos que hubiera facilitado al responsable en un formato estructurado, de uso común y lectura mecánica para su uso personal o para transmitirlos a otro responsable[38] en atención al artículo 17 de la LOPDGDD en relación con el artículo 20 de la RGPD.

f) Derecho de oposición.

El ejercicio de este derecho faculta al afectado a oponerse al tratamiento[39] salvo que se acredite un interés legítimo o sean necesarios para el ejercicio o defensa de reclamaciones, además, también podrá solicitarlo cuando el tratamiento tenga por objeto la mercadotecnia directa sin mediar consentimiento. Este derecho no será de aplicación cuando el tratamiento cumpla con un objetivo de interés público o para el ejercicio de poderes públicos que hayan sido conferidos al responsable. En estos casos será el responsable quien deberá acreditar los intereses legítimos que prevalecen sobre los individuales y las libertades fundamentales. Cuando existan dudas acerca de la prevalencia del derecho se realizará una ponderación de intereses en el tratamiento.

[37] Guía sectorial de *Protección de Datos y Administración Local*, op. cit., pp. 33-34.
[38] Guía sectorial de *Protección de Datos y Administración Local*, op. cit., pp. 33-34.
[39] Guía sectorial de *Protección de Datos y Administración Local*, op. cit., pp. 33-34.

Conviene señalar que la LOPDGDD se remite al RGPD para indicar que el ejercicio de los derechos se realizará de acuerdo con lo establecido en sus preceptos -en concreto los artículos 15 a 22- por lo que supone una remisión que requiere de un doble estudio de ambos textos legales.

Como ya se mencionó en el anterior apartado, el derecho a la autodeterminación informativa no es absoluto y de la misma forma los derechos que ostentan los particulares relativos a protección de datos tampoco lo son. A este respecto, el Derecho de la Unión Europea o bien los Estados miembros podrán establecer limitaciones a través de medidas legislativas con el requisito de respetar los derechos y libertades fundamentales y que se trate de una medida necesaria y proporcionada[40]. Estas limitaciones deben presentar un claro objetivo como puede ser salvaguardar la seguridad del Estado, perseguir un interés público general o la propia protección de los afectados por un tratamiento de datos[41].

El elenco de derechos expuestos debe ser respetado por las entidades públicas como responsables que determinan los fines y los medios de los datos, así como los encargados que realicen tratamientos de datos por cuenta de los responsables. En este cometido también se comprometerán a respetar aquellas obligaciones previstas legalmente y que se tratan en el siguiente apartado.

4.- La Administración Pública como responsable del tratamiento de datos.

Las Administraciones Públicas realizan un sinfín de tratamientos para el cumplimiento de los servicios públicos ligados a sus diferentes competencias o funciones que éstas llevan a cabo. No obstante, por sus particularidades, las entidades públicas no se encuentran en plano de igualdad con el resto de los responsables de carácter privado pues el volumen de datos y el nivel de exigencia en el cumplimiento de obligaciones será superior. A su vez, dispone de prerrogativas, por ejemplo, cuando

[40] AA.VV., MOSCOSO DEL PRADO MUÑOZ, J. (coord.), *Los derechos de los interesados*. «La administración local ante la gestión de la protección de datos», 1ª edición, Ed. Aranzadi, Cizur Menor, 2019, p. 198.
[41] *Ex* artículo 32 del RGPD.

el tratamiento de datos que realicen sea del ámbito de la función estadística pública[42], los organismos competentes podrán denegar las solicitudes de ejercicio de los derechos ARCO-POL cuando los datos se encuentren amparados por las garantías de secreto estadístico. Asimismo, cuando el tratamiento sea con fines de archivo en interés público[43] podrá ignorarse el principio de limitación del plazo de conservación de los datos y lo mismo ocurre cuando el tratamiento se refiera a datos relativos a infracciones y sanciones administrativas[44].

Los tratamientos anteriores probablemente no sean los que preocupen a los ciudadanos, por este motivo quizás resulten más ilustrativos los tratamientos de datos que puede realizar la Administración Local y, a este respecto, se pueden considerar los siguientes: padrón municipal de habitantes; subvenciones y ayudas; sanciones; obras y licencias; policía local; gestión de tributos; bolsas de trabajo; recaudación ejecutiva; registro de documentos; cementerio municipal; recursos humanos; biblioteca municipal; servicios sociales; educación infantil y gestión económica[45].

A efectos de concretar quiénes serán los responsables, en el ámbito municipal, los Ayuntamientos serán responsables de los tratamientos de datos que realicen a través de la figura de los Alcaldes que tienen atribuida la dirección y representación del Ayuntamiento en atención a los artículos 21 y 121 de la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local (en adelante LBRL).

En el caso de las diputaciones Provinciales, Consejos y Cabildos insulares también serán responsables de los tratamientos sobre los que decidan sus fines y/o encargados del tratamiento cuando presten asistencia para la consecución de los fines delimitados por los responsables.

[42] *Ex* artículo 25 de la LOPGDD.
[43] *Ex* artículo 27 de la LOPGDD.
[44] *Ex* artículo 27 de la LOPGDD.
[45] AA.VV., MOSCOSO DEL PRADO MUÑOZ, J. (coord.), *El régimen del tratamiento de los datos personales.* «La administración local ante la gestión de la protección de datos», 1ª edición, Ed. Aranzadi, Cizur Menor, 2019, p. 66.

Por otro lado, en el ámbito supramunicipal, es decir, las Comarcas, Áreas metropolitanas y mancomunidades serán responsables en la medida que realicen tratamiento de datos personales y lo mismo ocurre con la Administración Institucional de las Corporaciones Locales integrada por los organismos autónomos y entidades públicas empresariales locales.

Los responsables del tratamiento deben velar por el cumplimiento de una serie de obligaciones que se identifican con los principios en materia de protección de datos y se pueden resumir en los siguientes puntos:

a) Garantizar y acreditar que el tratamiento de datos se realice de acuerdo a su normativa específica.

b) Estar en condiciones de acreditar y demostrar el cumplimiento del anterior punto.

c) Que la protección de datos se realice desde el diseño y por defecto.

d) Cooperar con las autoridades de control en caso de ser necesario.

e) Realizar la Evaluación de Impacto sobre la Protección de Datos (EIPD) que es obligatoria para las entidades públicas.

f) Deber de notificar cualquier violación de seguridad de los datos a la autoridad de control correspondiente.

g) Comunicar la violación de seguridad de los datos al afectado cuando sea necesario.

h) Designar a un delegado de protección de datos.

Respecto a la primera se identifica con las obligaciones generales que afectan tanto a responsables y encargados que se regulan en el artículo 28 de la LOPDGDD basándose en que sean capaces de determinar las medidas técnicas y organizativas apropiadas a aplicar con el fin de garantizar y acreditar que el tratamiento se realiza de forma adecuada. La adecuación vendrá determinada, especialmente, por las disposiciones del Título V, Capítulo I de la LOPDGDD y los artículos 24 y 25 del RGPD, así como las normas de desarrollo y la legislación sectorial aplicable. Las medidas técnicas y organizativas se adoptarán cuando un

tratamiento entrañe un mayor riesgo como por ejemplo el tratamiento de datos de menores de edad o que suponga la creación de perfiles personales[46].

Lo anterior supone que con carácter previo al inicio de un tratamiento los responsables deban analizar las medidas técnicas y organizativas necesarias para el tratamiento y para ello deberán verificar el estado de la técnica; el coste de su aplicación; la naturaleza, ámbito, contexto y fines del tratamiento y, por último, la probabilidad que riesgos en el tratamiento se produzcan y su gravedad en el hipotético caso que se materialicen[47]. Esta tarea no sólo debe realizarse al inicio pues deberá ser objeto de revisión y actualización durante el tratamiento.

La segunda obligación requerirá que los responsables puedan garantizar y ser capaces de acreditar que el tratamiento se realiza conforme a la normativa de protección de datos. Los responsables deben estar en condiciones de demostrar dicho cumplimiento pues sobre éstos impera el «principio de responsabilidad proactiva»[48] recogido en el RGPD. El término de responsabilidad proactiva también se conoce como «accountability» cuyo origen se encuentra en el mundo anglosajón y se refiere a una responsabilidad con el añadido de adopción de medidas y garantías necesarias.

El referido principio fue introducido por la Organización para la Cooperación y el Desarrollo Económico (OCDE) en 1980 al ser incluido en sus Directrices sobre protección de la privacidad y flujos transfronterizos de datos[49], sin embargo, es gracias al Grupo de Trabajo del artículo 29[50] que actualmente aparece en la normativa de protección de datos mediante el Dictamen 3/2010 adoptado el 13 de julio de 2010[51] en cuyo apartado II.3 – 21 recoge que *«el término «responsabilidad»*

[46] Los supuestos de mayor riesgo en un tratamiento se enumeran en el artículo 28 apartado segundo de la LOPDGDD.
[47] AA.VV., MOSCOSO DEL PRADO MUÑOZ, J. (presidente), *Capítulo IV – Las figuras del responsable del tratamiento y encargado*, «La administración local ante la gestión de la protección de datos», 1ª edición, Ed. Aranzadi, Cizur Menor, 2019, p. 303.
[48] Previsto en el artículo 5.2 del RGPD.
[49] *Principio de accountability (Protección de Datos),* Guías Jurídicas de Wolters Kluwer, Madrid, última consulta: 10/01/2020.
[50] El Grupo de Trabajo del artículo 29 fue un órgano consultivo independiente que, entre otras funciones, elaboraba dictámenes y que desapareció tras la entrada en vigor del RGPD.
[51] Grupo de trabajo del artículo 29. Dictamen 3/2010 sobre el principio de responsabilidad de 13 de julio de 2010 (WP173).

(accountability) proviene del mundo anglosajón donde es de uso general y donde se da una comprensión ampliamente compartida de su significado, aunque la definición exacta de «responsabilidad» resulta compleja en la práctica. Pero de forma general, el término apunta sobre todo al modo en que se ejercen las competencias y al modo en que esto puede comprobarse. Competencia y responsabilidad son dos caras de la misma moneda y sendos elementos esenciales de la gobernanza. Solo cuando la responsabilidad funciona en la práctica puede desarrollarse la confianza suficiente».

El referido Dictamen fue emitido por el Grupo de Trabajo del artículo 29 (GT 173) que ha operado hasta el 25 de mayo 2018, es decir, hasta la entrada en vigor del RGPD. Actualmente, se encarga de elaborar este tipo de dictámenes el Comité Europeo de Protección de Datos (CEPD), aunque no es su única función, se trata de un organismo europeo independiente que contribuye a la aplicación coherente de las normas de protección de datos en toda la Unión Europea y promueve la cooperación entre las autoridades de protección de datos de la Unión Europea[52].

Por su parte, la LOPDGDD se refiere a medidas de responsabilidad activa -no utiliza el término proactiva- basándose en el principio acuñado por el RGPD que *«consiste en la capacidad del responsable, es decir, de la organización, de demostrar y proporcionar evidencias de dicho cumplimiento»*[53].

Entre las obligaciones inherentes a este principio se encuentra el deber de información que recoge el artículo 11 de la LOPDGDD que se trata de un derecho para los afectados y una obligación para los responsables. Para cumplir con la transparencia e información al afectado, como mínimo, se deberá indicar la identidad del responsable del tratamiento y, en su caso, del representante; la finalidad del tratamiento y la posibilidad de ejercer los derechos que se han mencionado. Esto ocurriría en el caso que los datos fueran obtenidos del afectado, de lo contrario, se deberá indicar dentro de que categoría se encuentran los datos y los medios utilizados

[52] El Comité Europeo de Protección de Datos (CEPD) se creó mediante el Reglamento General de Protección de Datos (RGPD) y tiene su sede en Bruselas. Extraído del sitio web https://edpb.europa.eu/about-edpb/about-edpb_es última consulta: 4/01/2020.
[53] Guía sectorial de *Protección de Datos y Administración Local* publicada el 16 de mayo de 2018 por la Agencia Española de Protección de Datos.

en la obtención de dichos datos. En ambos supuestos se deberá facilitar al afectado una dirección electrónica o cualquier otro medio por el que pueda acceder de forma sencilla e inmediata a la información mencionada. Por otro lado, si los datos obtenidos tienen por objeto un tratamiento para la elaboración de perfiles se deberá indicar esta circunstancia en la información básica y la posibilidad de ejercitar el derecho de oposición al tratamiento.

A este respecto, la autoridad de control publicó una Guía que aclara cómo los responsables deberían informar a través de la información por capas compuesta por la información básica que sería la primera capa y la información adicional como segunda capa. En ésta última no se puede omitir información y no está limitada en cuanto a extensión para poder ofrecer todos los detalles a los interesados[54].

En tercer lugar, la protección de datos se realizará desde el diseño y por defecto a tenor del artículo 25 del RGPD, obligación que se encuentra íntimamente relacionada con el principio de minimización de datos. La protección de datos desde el diseño o «privacy by design»[55] conlleva aplicar, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas con el objeto de cumplir la normativa y proteger los derechos de los interesados.

Respecto a la protección de datos por defecto o «privacy by default» comporta la aplicación de medidas técnicas y organizativas apropiadas con el fin de que sean objeto de tratamiento los datos personales estrictamente necesarios para cada uno de los fines específicos del tratamiento.

En cuarto lugar, se encuentra la obligación de cooperar con las autoridades de control en caso de ser necesario pues requerirá que la autoridad competente necesite de dicha cooperación o bien exista algún tipo de incidencia que el responsable deba

[54] *Guía general para el cumplimiento del deber de informar* publicada el 22 de mayo de 2018 por la Agencia Española de Protección de Datos con colaboración de la Autoridad Catalana de Protección de Datos y la Agencia Vasca de Protección de Datos.
[55] *Guía de Privacidad desde el Diseño* publicada el 12 de noviembre de 2019 por la Agencia Española de Protección de Datos. En esta Guía la privacidad desde el diseño se define como la suma integral del enfoque al riesgo y la responsabilidad proactiva.

comunicar. En aras de su cumplimiento se instauró el mecanismo de ventanilla única[56] para facilitar la cooperación entre la autoridad de control principal y otras autoridades de control interesadas, por ejemplo, de otros Estados miembros. Este mecanismo facilita la comunicación de los afectados por un tratamiento con la autoridad del Estado a la que pertenezca la Administración responsable independientemente de donde tuviera lugar la reclamación junto con la posibilidad de plantear reclamaciones donde tenga ubicada su residencia habitual, lugar de trabajo o donde se hubiese cometido la supuesta infracción. Sin embargo, no resulta de aplicación cuando el tratamiento de datos sea realizado por autoridades públicas u organismos privados en interés público en atención al considerando 127 y 128 del RGPD pues sólo será competente la autoridad de control del Estado miembro en cuestión.

En quinto lugar, las entidades públicas que realicen tratamientos de alto riesgo para los derechos y libertades de las personas físicas tendrán la obligación de realizar una Evaluación de Impacto sobre la Protección de Datos (EIPD)[57]. Esta evaluación comporta un análisis acerca de los riesgos que la actividad o servicio pueda entrañar en la protección de datos de los afectados, una vez detectados se adoptarán las medidas necesarias para eliminar o mitigar dichos riesgos. En el caso de las Administraciones Públicas resulta evidente que la realización de una EIPD es más que recomendable y este respecto se han creado metodologías para realizarla, incluso existen catálogos de amenazas y de sus posibles soluciones creados por la Agencia Española de Protección de Datos[58].

En sexto lugar se encuentra el deber de notificar cualquier incidente que afecte a la seguridad de los datos a la autoridad de control. En séptimo lugar, comunicar la violación de seguridad de los datos al afectado cuando sea necesario. Y, por último, designar a un delegado de protección de datos que será necesario cuando el tratamiento sea realizado por las entidades públicas. Por su importancia, estas tres últimas obligaciones serán objeto de análisis en el ulterior apartado.

[56] Considerando nº 127 del RGPD.
[57] El artículo 35 del RGPD.
[58] *Guía práctica para las Evaluaciones de Impacto en la Protección de los Datos sujetas al RGPD* (guía general) publicada el 17 de enero de 2018 por la Agencia Española de Protección de Datos.

En lo relativo a las obligaciones enumeradas y con el objeto de simplificar la tarea a los responsables, la autoridad de control ha elaborado la Guía del Reglamento General de Protección de Datos para Responsables de Tratamiento[59].

A pesar de que la responsabilidad en materia de protección de datos pueda intuirse que corresponde al responsable del tratamiento de forma exclusiva, se pueden dar supuestos en los que concurran varios responsables que determinen conjuntamente los objetivos y los medios del tratamiento surgiendo así la corresponsabilidad. La LOPDGDD no específica nada acerca de la corresponsabilidad limitándose a la remisión al artículo 26 del RGPD que determina que los corresponsables deberán alcanzar un acuerdo que pondrán a disposición de los afectados en el que especifiquen sus responsabilidades y respectivas obligaciones. No obstante, los afectados podrán dirigirse a cualquiera de los responsables en el ejercicio de sus derechos.

4.1.- Los encargados del tratamiento de datos.

Tras analizar las obligaciones de los responsables quedan los encargados del tratamiento. En el ámbito de la Administración Pública resulta frecuente que requiera de terceros a la hora de realizar tratamientos de datos, estos serán encargados del tratamiento. A modo de ejemplo, los Ayuntamientos -como responsables de un tratamiento de datos- pueden solicitar a una empresa o tercero que realicen actividades en materia de protección de datos pasando a convertirse en verdaderos encargados del tratamiento. Entre las actividades que las entidades públicas pueden encomendar a terceros se encuentra la confección de nóminas del personal, la destrucción de documentación, los servicios de videovigilancia, la gestión del cobro de tributos, la gestión de subvenciones o ayudas, el mantenimiento de equipos informáticos, [60] etc.

Asimismo, los encargados tienen la posibilidad de encomendar el tratamiento a otro encargado siempre que el responsable lo autorice. El encargado no

[59] *Guía general del Reglamento General de Protección de Datos para Responsables de Tratamiento* adoptada el 22 de mayo de 2018 por la Agencia Española de Protección de Datos con colaboración de la Autoridad Catalana de Protección de Datos y la Agencia Vasca de Protección de Datos.
[60] AA.VV., MOSCOSO DEL PRADO MUÑOZ, J. (coord.), *Las figuras del responsable.* «La administración local ante la gestión de la protección de datos», 1ª edición, Ed. Aranzadi, Cizur Menor, 2019, p. 307.

necesariamente pertenecerá al sector privado pues el artículo 33 de la LOPDGDD ofrece la posibilidad de atribuir las competencias propias de un encargado a otro ente público como la *«Administración General del Estado, la Administración de las comunidades autónomas, las Entidades que integran la Administración Local o a los Organismos vinculados o dependientes de las mismas»* siempre y cuando exista una norma reguladora de estas competencias que incorporará las previsiones del artículo 28, apartado tercero, del RGPD.

El meritado artículo 28 del RGPD establece que los tratamientos de datos que realicen los encargados se regirán por un contrato o cualquier otro acto jurídico adecuado a la normativa de protección de datos. Este documento contendrá el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales, categorías de afectados y las estipulaciones previstas en el apartado tercero de dicho precepto. El contrato cobra especial importancia pues su inobservancia podría ocasionar incidencias de seguridad. A efectos informativos y para evitar cualquier incidencia la Agencia Española de Protección de Datos ha elaborado el documento denominado *«directrices para la elaboración de contratos entre responsables y encargados del tratamiento»*[61] que facilita la confección de este tipo de contratos.

A la vista de lo anterior puede intuirse que la normativa de protección ha propiciado un gran impacto en la Administración Pública que, además de su poner un aumento en su carga de trabajo, ha requerido de un proceso de adaptación y creación de mecanismos para velar por los derechos de los ciudadanos y atender sus solicitudes. En el posterior epígrafe se analizarán los aspectos más importantes que ha supuesto el RGPD para las entidades públicas.

5.- Impacto de la normativa de protección de datos en las entidades públicas.

La normativa relativa a protección de datos ha supuesto un impacto en las Administraciones Públicas tal y como se pronosticaba incluso antes de que fuera

[61] *Directrices para la elaboración de contratos entre responsables y encargados del tratamiento* de publicado el 16 de mayo de 2018 por la Agencia Española de Protección de Datos.

aplicable el RGPD, como a través de los informes publicados por la Agencia Española de Protección de Datos en los que se enuncia como afectaría la normativa a la actividad de las Administraciones Públicas[62].

Las cuestiones más relevantes que deberán atender las entidades públicas se centran en la necesidad de identificar las finalidades y la base jurídica de los tratamientos[63]. En esta labor la Administración sólo podrá esgrimir el interés legítimo en un tratamiento cuando no esté actuando en el ejercicio de sus funciones públicas debido a que el RGPD en su artículo 6.1.f) establece esta exclusión. Cobra sentido cuando las entidades públicas realicen tareas en el ámbito privado de forma que puedan legitimar estos tratamientos en el interés legítimo ya que entrarían dentro del ejercicio de sus funciones públicas[64]. Asimismo, cabe señalar que el interés legítimo no tiene un alcance ilimitado pues encuentra su límite en los derechos y libertades de los ciudadanos y a pesar de que el RGPD establece criterios para realizar una ponderación entre ambos, no será de aplicación, como regla general, a las entidades públicas[65] [66].

También deberán procurar la adecuación de la información que se ofrece a los ciudadanos y atención de las solicitudes que éstos inicien en relación con el ejercicio de sus derechos. Las solicitudes deben responderse en el plazo de un mes pudiendo prorrogarse otros dos meses si concurren motivos para ello[67] y a este respecto, resulta probable que este trabajo acabe siendo realizado por los encargados del tratamiento. Las entidades públicas deberán contar con encargados que actúen con la debida diligencia en las funciones que éstas les encomienden, puesto que el

[62] *El Impacto del Reglamento General de Protección de Datos sobre la Actividad de las Administraciones Publicas* publicado el 25 de mayo de 2018 por la Agencia Española de Protección de Datos, pp. 1-5.
[63] En el caso de las entidades públicas coincidirá con una tarea de interés público o el ejercicio de poderes públicos.
[64] MARTÍNEZ VILLASECA, M., *El interés legítimo como base legitimadora del tratamiento de datos de carácter personal,* Actualidad administrativa, nº 12, Wolters Kluwer, Madrid, 2019, pp. 5-6.
[65] En atención al apartado V del preámbulo de la LOPDGDD el legislador establece una presunción «iuris tantum» de prevalencia del interés legítimo a pesar de que sean tratamientos no incluidos en el Título IV de la LOPDGDD. La relación de disposiciones aplicables a tratamientos concetos del meritado Título IV no recoge un «numerus clausus» pudiendo extenderse a otros tratamientos.
[66] MARTÍNEZ VILLASECA, M., El interés legítimo como base legitimadora del tratamiento de datos de carácter personal, Actualidad administrativa, nº 12, Wolters Kluwer, Madrid, 2019, pp. 3-4.
[67] *Guía para el ciudadano* publicada en fecha 7 de febrero de 2019 por la Agencia Española de Protección de Datos, p. 18.

Reglamento establece a los responsables la obligación de elegir a aquellos encargados que se encuentren en condiciones de cumplir con la normativa[68]. Esta obligación puede traducirse en la denominada *«culpa in eligendo»* pudiendo incurrir en responsabilidad las Administraciones que no sean diligentes a la hora de elegir a sus encargados del tratamiento. Como ya se adelantaba en el apartado IV de este estudio, la relación entre los responsables y los encargados deberá formalizarse mediante un contrato o acto jurídico que vincule al encargado[69].

La normativa de protección de datos no sólo afectaría a la actividad del sector público sino a otras normas que rigen su funcionamiento. A este respecto, la LOPDGDD modifica el artículo 13, apartado h), de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPAC) que prevé el derecho a la protección de datos de carácter personal incluyendo *«la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas».* Además, modifica los apartados 2º y 3º del artículo 28, modificación que presenta relación con el principio de minimización de datos resultando en una ventaja para los ciudadanos al suponer una reducción de la carga burocrática debido a que el apartado 2º señala: *«las Administraciones Públicas no requerirán a los interesados datos o documentos no exigidos por la normativa reguladora aplicable o que hayan sido aportados anteriormente por el interesado a cualquier Administración»*. También modifica los artículos 16 y 17 en lo relativo a los registros y archivos de documentos que deberán respetar las normas relativas a la conservación de datos y, por otro lado, el artículo 18 acerca de la colaboración de los ciudadanos exigible por la Administración en el ejercicio de sus competencias y con los límites establecidos.

Desde otra perspectiva, aunque el objeto de estudio sean las Administraciones Públicas, también ha supuesto un impacto en los ciudadanos al ser más conscientes de los tratamientos que los entes públicos realizan sobre sus datos.

[68] *Ex* artículo 28 del RGPD.
[69] Será más frecuente la fórmula del acto jurídico como, por ejemplo, la creación de órganos encargados de la prestación de servicios informáticos a través del Real Decreto 806/2014, de 19 de septiembre, sobre organización e instrumentos operativos de las tecnologías de la información y las comunicaciones en la Administración General del Estado y sus Organismos Públicos.

Sirva de ejemplo el estudio realizado por el Centro de Investigaciones Sociológicas (CIS) en 2018[70] en el que un 76,1% de los ciudadanos que declaran que les preocupa «mucho» o «bastante» la protección de sus datos personales. Esta preocupación ciudadana se ha traducido en una mayor sensibilización y ha propiciado el aumento de solicitudes en el ejercicio de los derechos de protección de datos que ostentan los afectados[71].

Sin embargo, en el caso de presentar algún tipo de problema con sus datos personales, como primera opción, el 51,6% de los encuestados denunciaría a los Cuerpos y Fuerzas de Seguridad del Estado, el 22,3% acudiría a la propia entidad o empresa infractora, el 4,3 acudiría a una asociación de consumidores y usuarios frente al 4,2 que se decanta por la Agencia Española de Protección de Datos[72].

El organismo adecuado al que los ciudadanos deben acudir es la Agencia Española de Protección de Datos (en adelante «AEPD») como autoridad de control independiente que vela por el cumplimiento de la normativa sobre protección de datos y garantiza y tutela el derecho fundamental a la protección de datos de carácter personal[73] [74]. Aunque sea la autoridad de referencia también existen autoridades autonómicas de protección de datos como es la Agencia Vasca de Protección de Datos[75] o la Autoridad Catalana de Protección de Datos[76] que podrán ejercer las funciones y potestades previstas en el RGPD conforme a su normativa autonómica. Además, podrán dictar circulares en cuanto a los tratamientos que estuvieran sometidos a su competencia[77] [78].

[70] Estudio del Centro de Investigaciones Sociológicas (CIS) número 3213 realizado entre el 1 al 10 de mayo de 2018.
[71] Memoria anual de actividad del año 2018 de la Agencia Española de Protección de Datos, p. 82.
[72] Datos extraídos de la pregunta número 19 del Estudio del Centro de Investigaciones Sociológicas (CIS) número 3213 realizado entre el 1 al 10 de mayo de 2018.
[73] Apartado V del preámbulo de la LOPDGDD.
[74] Su régimen jurídico está previsto en el Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos.
[75] La Agencia Vasca de Protección de Datos fue creada y se regulada por la Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos.
[76] Prevista su creación ex artículo 156 del Estatuto de Autonomía de Cataluña de 20 de julio de 2006 y regulada por la Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos.
[77] AA.VV., MOSCOSO DEL PRADO MUÑOZ, J., (coord.), *Autoridades de control*, «La administración local ante la gestión de la protección de datos», 1ª edición, Ed. Aranzadi, Cizur Menor, 2019, p. 412.
[78] *Ex* artículo 57.2 de la LOPDGDD.

Entre las funciones de la AEPD se encuentra la atención de peticiones y reclamaciones que presenten los afectados lo cual no implica que el sector público pueda desatender sus obligaciones como responsable de los tratamientos[79]. Como ya se ha enunciado en los principios de protección de datos, las entidades públicas deberán facilitar toda la información pertinente con el objeto de que los ciudadanos puedan dirigir solicitudes y reclamaciones al propio responsable, no obstante, podrán optar entre ambas vías.

Los ciudadanos no serán los únicos que podrán relacionarse con la AEPD pues los responsables y encargados también podrán dirigir consultas y, en otros casos, estarán obligados a colaborar con la Agencia. Los supuestos se encuentran regulados en el artículo 52 de la LOPDGDD y dicho deber de colaboración se extiende al sector público, incluida la Administración Tributaria y de la Seguridad Social debiendo proporcionar datos, informes, antecedentes y justificantes que fueran necesarios para que la AEPD pueda llevar a cabo su actividad de investigación. Asimismo, cuando se inicien actuaciones previas de investigación, la Agencia podrá recabar directamente de las entidades públicas la información que estime conveniente para identificar a los responsables, aunque dependerá del medio utilizado en la comisión de la infracción, requiriendo de autorización judicial en los supuestos excluidos[80].

En los siguientes epígrafes se analizarán las medidas de cumplimiento de la normativa de protección de datos más relevantes, en concreto, la designación obligatoria de Delegado de Protección de Datos; el Registro de Actividades del Tratamiento de Datos, las Evaluaciones de Impacto en la Protección de Datos y, por último, la seguridad en el tratamiento de los datos personales.

[79] *Ex* artículo 4 del Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos.

[80] Cuando el medio por el que presuntamente se ha cometido una infracción de protección de datos sea a través de la utilización de un servicio de telefonía fija o móvil o bien un servicio de la sociedad de la información, la AEPD efectuará un requerimiento directamente a las compañías que presten estos servicios para que estas faciliten la información que tuvieran en su poder. Por el contrario, si los medios fueran distintos, la AEPD deberá obtener previa autorización judicial para solicitar la información (artículo 52.3 de la LOPDGDD).

5.1.- El Delegado de Protección de Datos en el sector público.

La figura del Delgado de Protección de Datos (en adelante «DPD» o «Delegado») fue introducida por el RGPD y se encuentra regulada entre los artículos 37 a 39 siendo obligatoria su designación por los responsables y encargados en los supuestos que estos preceptos recogen. Como podría intuirse, será obligatoria su designación cuando el tratamiento de datos sea realizado por un organismo público, aunque existen más entidades obligadas tal y como prevé el artículo 34 de la LOPDGDD.

El Delegado podrá ser una persona física o jurídica y sus funciones radican en informar y asesorar al responsable que lo hubiera designado y al encargado del tratamiento -si lo hubiera-, así como al resto de empleados de la entidad acerca de las obligaciones que contiene la legislación de protección de datos y supervisando su cumplimiento. Asimismo, deberá cooperar y actuar como punto de contacto con la autoridad de control[81] [82].

En el ámbito público podrá designarse a un único DPD para varias autoridades y organismos públicos en función de su estructura organizativa y tamaño, además, podrá formar parte de la plantilla del responsable o encargado o bien desempeñar sus funciones a través de un contrato de servicios. Su actividad la podrá desarrollar a tiempo completo o a tiempo parcial. Además, será designado conforme a sus cualidades profesionales primando aquellos profesionales con conocimientos especializados en el derecho y la práctica en materia de protección de datos[83][84]. A este

[81] CAMPOS ACUÑA, C., *Impacto de la nueva Ley Orgánica de protección de datos personales y garantía de los derechos digitales en el ámbito local*. Revista digital CEMCI, nº 40, Granada, 2018, p. 6-7.
[82] DAVARA RODRÍGUEZ, M.Á., *El Delegado de Protección de Datos en los ficheros y/o tratamientos de la Administración en consonancia con el Reglamento Europeo de Protección de Datos*. Actualidad Administrativa, nº 1, Ed. Wolters Kluwer, Madrid, 2017, pp. 7-8.
[83] *El delegado de protección de datos en las administraciones públicas* publicado el 1 de octubre de 2019 por la Agencia Española de Protección de Datos.
[84] DAVARA RODRÍGUEZ, M.Á., *El Delegado de Protección de Datos en los ficheros y/o tratamientos de la Administración en consonancia con el Reglamento Europeo de Protección de Datos*. Actualidad Administrativa, nº 1, Ed. Wolters Kluwer, Madrid, 2017, pp. 5-6.

respecto, se prevén mecanismos voluntarios de certificación para demostrar que cumplen con la cualificación adecuada[85].

A pesar de que las funciones de los Delegados están reguladas, no existe una definición para esta figura motivo por el cual sería interesante que contarán con un estatuto jurídico íntegro a fin de evitar posibles conflictos de intereses que podrían suscitarse, por ejemplo, con el responsable del tratamiento.

Entre las particularidades que presenta el DPD destaca su posición especial en la entidad para la que desarrolle sus funciones[86]. Esto se traduce en que no podrá ser despedido ni sancionado como consecuencia del ejercicio de sus funciones; sólo responderá frente al más alto nivel jerárquico y actuará con plena independencia y autonomía[87]; y, por último, se encargará de comunicar a los órganos de administración la existencia de cualquier vulneración o incidencia en protección de datos[88]. El DPD también actúa como interlocutor ante autoridad de control y, por consiguiente, cuando la vulneración fuera relevante deberá ponerlo en conocimiento de la AEPD.

Respecto al hecho de que los Delegados no puedan ser sancionados ni removidos de su cargo como resultado del desempeño de sus funciones, no implicará que pueda ser destituido por razones distintas a su actividad como puede ser la comisión de infracciones del orden laboral o incumplimiento contractual[89]. Por otro lado, su posición de independencia es incompatible con funciones y tareas que puedan dar lugar a conflictos de intereses, lo cual se traduce en que no podrá ocupar un cargo en la organización por el que se determinen los fines y medios de un tratamiento de datos -funciones propias de los responsables-[90].

[85] *Ex* artículo 35 de la LOPDGDD.
[86] *Ex* artículo 36 de la LOPDGDD acerca de la posición del delegado de protección de datos.
[87] Implica que no podrá recibir instrucciones en el desempeño de sus funciones.
[88] MARTOS, N., *El Delegado de Protección de Datos: ¿figura interna, externa o mixta?,* Actualidad Jurídica Aranzadi, núm. 936/2017, Ed. Aranzadi, S.A.U., Cizur Menor, 2017, pp. 1-2.
[89] RALLO LOMBARTE, A., (coord.). *El delegado de protección de datos.* «Tratado de protección de datos: actualizado con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales», 1ª edición, Ed. Tirant lo blanch, Valencia, 2019, p. 446.
[90] RALLO LOMBARTE, A., (coord.). *Capítulo XII – El delegado de protección de datos…* op. cit., p. 447.

En teoría sería más adecuado que el Delegado fuera externo a fin de evitar cualquier injerencia en el desarrollo de su actividad. A este respecto, cuando el responsable externalice las funciones del DPD, éste pasará a tener la consideración de encargado del tratamiento y, por consiguiente, deberá formalizarse la relación mediante contrato[91].

El Delegado puede desempeñar sus funciones con ayuda de un equipo si fuera necesario en orden a comunicarse de forma eficaz con los interesados y para cooperar con las autoridades de control[92]. En este mismo sentido y en relación con las Corporaciones Locales existen distinciones respecto al volumen de población, en concreto, los ayuntamientos con población inferior a 20.000 habitantes podrán designar a un Delegado o bien compartir al profesional designado en la Diputación Provincial o la Comunidad Autónoma[93]. Cuando su población sea superior a 20.000 habitantes el Delegado podrá contar con un departamento de apoyo y, en el caso de tratarse de empresas municipales, se podrá designar en función de los tratamientos que realicen[94].

En la práctica el nombramiento de un único Delegado para toda una administración podría presentar riesgos si no se le facilitan los recursos y soporte técnico adecuado para el desempeño de sus funciones.

En el desarrollo de su actividad, los Delegados deberán velar por el cumplimiento del deber de secreto profesional y el deber de confidencialidad, además de acometer sus obligaciones con la máxima diligencia en atención a los riesgos asociados con los tratamientos de datos[95]. Por lo expuesto, se presume que el contar con un Delegado asegura el cumplimiento del principio de responsabilidad proactiva ya que estos se encargarán de adoptar todas aquellas medidas preventivas para el

[91] *Directrices para la elaboración de contratos entre responsables y encargados del tratamiento* de publicado el 16 de mayo de 2018 por la Agencia Española de Protección de Datos.
[92] AA.VV., MOSCOSO DEL PRADO MUÑOZ, J., (coord.), *El delegado de protección de datos en la administración local.* «La administración local ante la gestión de la protección de datos», 1ª edición, Ed. Aranzadi, Cizur Menor, 2019, p. 329.
[93] En el caso de Canarias, los Cabildos también tienen la obligación de designar a un DPD.
[94] AA.VV., MOSCOSO DEL PRADO MUÑOZ, J., (coord.), *El delegado de protección de datos en la administración local…* op. cit., p. 329.
[95] RODRÍGUEZ AYUSO, J.F., *El delegado de protección de datos en el ámbito de la Administración Pública.* Actualidad Administrativa, nº 7-8, Ed. Wolters Kluwer, Madrid, 2019, pp. 3-4.

cumplimiento de la legislación en protección de datos. En contraposición, esto podría ocasionar que los responsables adopten una actitud laxa al confiar al DPD obligaciones que en principio no les corresponden de forma directa.

Entre las funciones también se encuentra la adopción de medidas de seguridad, la realización de evaluaciones de impacto en la protección de datos o la confección del registro de actividades del tratamiento de datos.

5.2.- El registro de actividades del tratamiento de datos.

El registro de actividades del tratamiento de datos -también denominado inventario de actividades- conforma una obligación que atañe a los responsables y encargados del tratamiento según las previsiones del artículo 30 del RGPD y 31 de la LOPDGDD. Consistirá en la elaboración de un registro que contendrá su identificación y datos de contacto y, en su caso, los del corresponsable, representante del responsable y del Delegado; los fines del tratamiento, una descripción de las categorías de interesados y de sus datos personales; cuando se comuniquen los datos se reflejarán las categorías de destinatarios y, además, deberá indicarse si se realizan transferencias de datos a terceros países u organizaciones internacionales. Asimismo, aunque no sea estrictamente necesario, también se podrán indicar los plazos previstos para la supresión de los datos al igual que una descripción general de las medidas técnicas y organizativas de seguridad[96].

Respecto al cumplimiento de esta obligación, se exige la publicación del referido registro a las entidades públicas, sin embargo, puede comprobarse que no todas cumplen, especialmente, en el caso de las corporaciones locales. A ese respecto, cobra especial importancia la figura del Delegado que deberá elaborar el registro conforme a los fines y medios del tratamiento establecidos por el responsable.

[96] CAMPOS ACUÑA, C., *Impacto de la nueva Ley Orgánica de protección de datos personales y garantía de los derechos digitales en el ámbito local*. Revista digital CEMCI, nº 40, Granada, 2018, p. 8.

5.3.- Las evaluaciones de impacto en la protección de datos.

La evaluación de impacto en protección de datos (en adelante «EIPD»)[97] es una herramienta que permite identificar, evaluar y gestionar los riesgos que pueden suscitarse en las actividades de tratamiento que realicen los responsables[98]. El principal objetivo de estas evaluaciones es garantizar los derechos y libertades de los afectados, así como determinar el nivel de riesgo que entrañe un tratamiento y, por consiguiente, adoptar medidas de control adecuadas para reducir los riesgos. El momento idóneo para realizar la EIPD será antes de realizar un tratamiento o bien cuando se produzcan modificaciones en los fines, las técnicas utilizadas, etc.

La EIPD será obligatoria cuando el tratamiento de datos entrañe un alto riesgo para los derechos y libertades de los afectados[99] en función de su naturaleza, alcance, contexto o fines del tratamiento[100]. Asimismo, será necesaria la EIPD en los siguientes supuestos:

1º. *«Evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar».*

2º. *«Tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9.1 o de los datos personales relativos a condenas e infracciones penales del artículo 10».*

3º. *«Observación sistemática a gran escala de una zona de acceso público»*[101].

[97] Se regula en el artículo 35 del RGPD. La LOPDGDD sólo menciona los supuestos en que será obligatoria la EIPD remitiéndose a la Sección 3 del Capítulo IV del RGPD.
[98] Guía sectorial de *Protección de Datos y Administración Local* publicada en fecha 16 de mayo de 2018 por la Agencia Española de Protección, pp. 22-23.
[99] Considerando nº 84 del RGPD.
[100] Con el objeto de aclarar los supuestos en que resulte necesaria la EIPD la Agencia Española de Protección de Datos ha publicado un documento con una lista de tipos de tratamientos que requieren evaluación de impacto.
[101] Guía sectorial de *Protección de Datos y Administración Local,* op. cit., pp. 22-23.

La EIPD contendrá, como mínimo, una descripción sistemática de las operaciones previstas y de los fines del tratamiento incluyéndose el interés legítimo, por ende, las entidades públicas difícilmente se encontrarán exentas de realizar la evaluación[102]. También contendrá una evaluación de la necesidad y proporcionalidad de las operaciones de tratamiento con respecto a su finalidad; una evaluación de los riesgos para los derechos y libertades de los interesados y, por último, las medidas previstas para afrontar los riesgos, como las garantías, medidas de seguridad y mecanismos destinados a garantizar la protección de datos[103] [104].

Por otro lado, cuando la EIPD refleje que el tratamiento analizado pudiera entrañar un alto riesgo el responsable deberá elevar una consulta previa a la autoridad de control y ésta se encargará de asesorar al responsable acerca de cómo proceder[105].

Esta obligación no es una cuestión baladí ya que su incumplimiento es constitutivo de infracción grave en atención al artículo 77.t) de la LOPDGDD. Una vez más la figura del DPD será clave para realizar la EIPD pues, a pesar de que la obligación corresponda al responsable, si éste hubiera designado a un Delegado, podrá valerse de su asesoramiento.

5.4.- La seguridad en el tratamiento de datos personales.

En este epígrafe se tratarán tres aspectos: el análisis de riesgos, las medidas de seguridad y la comunicación de quiebras de seguridad de los datos personales.

El análisis de riesgos supone valorar los riesgos de los tratamientos que los responsables realicen, constituyendo una obligación prevista en el RGPD e

[102] DÍAZ DÍAZ, E., *El nuevo Reglamento General de Protección de Datos de la Unión Europea y sus consecuencias jurídicas para las instituciones*, Revista Aranzadi Doctrinal núm. 6/2015, Ed. Aranzadi, Cizur Menor, 2016, pp. 31-32.
[103] Se identifica con el principio de responsabilidad proactiva.
[104] *Guía práctica para las evaluaciones de impacto en la protección de los datos sujetas al RGPD* publicado el 17 de enero de 2018 de la Agencia Española de Protección de Datos.
[105] *Ex* artículo 36 del RGPD.

independiente de la EIPD vista anteriormente. El referido análisis de riesgo resulta crucial para determinar las medidas de seguridad a aplicar.

En el caso de los Ayuntamientos que cuenten con una población inferior a 20.000 habitantes podrán utilizar el soporte que corresponda a la Diputación Provincial -en el caso de Canarias los Cabildos- para realizar el análisis[106].

Por lo que respecta a las medidas de seguridad, se identifican principalmente con las medidas técnicas y organizativas apropiadas para garantizar la seguridad en atención a los riesgos detectados. Aunque el RGPD no establece medidas concretas si se cuenta con un catálogo de medidas previsto en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS). Este texto legal contiene los principios básicos y requisitos mínimos para la adecuada protección de la información cuyo objetivo es su aplicación por las Administraciones Públicas *«para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias»*[107].

La comunicación de quiebras o incidentes de seguridad[108] de los datos personales resulta fundamental para controlar el cumplimento y establecer medidas correctoras. Respecto a los incidentes, se definen como una situación o circunstancia que ponga en riesgo la seguridad de los datos de cualquier tipo y no deberán confundirse con las quiebras o brechas de seguridad que suponen una violación de los datos afectando a la confidencialidad, la disponibilidad o la integridad de dichos datos [109].

[106] Guía sectorial de *Protección de Datos y Administración Local* publicada en fecha 16 de mayo de 2018 por la Agencia Española de Protección, p. 19.
[107] *Ex* artículo 1.2 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
[108] La comunicación de una violación de la seguridad de los datos se encuentra regulada en el artículo 34 del RGPD.
[109] AA.VV., MOSCOSO DEL PRADO MUÑOZ, J., (coord.), *La gestión de riesgos y la seguridad en el tratamiento de los datos.* «La administración local ante la gestión de la protección de datos», 1ª edición, Ed. Aranzadi, Cizur Menor, 2019, p. 384.

Cuando se trate de una quiebra de seguridad, supondrá una destrucción, pérdida o alteración accidental o ilícita de datos personales. Por su importancia, está previsto que sean comunicadas en el plazo máximo de 72 horas a la AEPD cuyo contenido mínimo expresará la naturaleza de la quiebra, las categorías de afectados, los datos de contacto del DPD, las posibles consecuencias y las medidas adoptadas o propuestas para remediar los perjuicios ocasionados[110]. Asimismo, las quiebras también deberán comunicarse a los afectados como regla general salvo excepciones[111].

Por otro lado, los encargados no se encuentran ajenos ante la comunicación de quiebras o incidencias, aunque su obligación será frente al responsable, cobrando especial importancia el contrato o acto jurídico entre responsables y encargados a la hora de establecer los medios para realizar la comunicación.

Respecto a las entidades públicas, comportaría ventajas la elaboración de un plan de contingencias con el objeto de mitigar los daños y también mantener un registro con los incidentes de seguridad producidos, al igual que requerir al Delegado de Protección de Datos su asesoramiento en cuanto a medidas preventivas.

Como se ha expuesto en la introducción de este documento, la protección de datos forma parte del ámbito de la seguridad pública, motivo por el cual, recientemente, se ha reforzado su cumplimiento mediante la regulación de medidas concretas a través del Real Decreto-ley 14/2019, de 31 de octubre. A este respecto, destaca el ámbito de la contratación pública sobre el que se advierte que *«los contratistas del sector público manejan en ocasiones, para la ejecución de los respectivos contratos, un ingente volumen de datos personales, cuyo uso inadecuado puede, a su vez, plantear riesgos para la seguridad pública. Por ello, resulta necesario asegurar normativamente su sometimiento a ciertas obligaciones específicas que*

[110] Guía sectorial de *Protección de Datos y Administración Local* publicada en fecha 16 de mayo de 2018 por la Agencia Española de Protección, p. 21.

[111] Las excepciones están previstas en el artículo 34.3 del RGPD y son las siguientes:
1º. Cuando se hubieran adoptado y aplicado medidas sobre los datos personales afectados, particularmente aquellas que hagan ininteligibles los datos para cualquier persona que no esté autorizada a acceder a ellos (por ejemplo: el cifrado los datos personales).
2º. Que el responsable hubiera adoptado medidas ulteriores que garanticen que ya no existe un alto riesgo para los derechos y libertades.
3º. Que esta comunicación fuese un esfuerzo desproporcionado, optándose por una comunicación pública o medida semejante por la que se informe de forma efectiva a los afectados.

garanticen tanto el cumplimiento de la normativa en materia de protección de datos personales como la protección de la seguridad pública[112]».

Por otro lado, resulta frecuente que las entidades públicas no cumplan con las exigencias de la legislación de protección de datos a la hora de practicar notificaciones por medio de anuncios y publicaciones de actos administrativos. A fin de garantizar una mayor protección, la Disposición Adicional 7ª de la LOPDGDD establece una medida consistente en realizar la publicación identificando al interesado «*mediante su nombre y apellidos, añadiendo cuatro cifras numéricas aleatorias del documento nacional de identidad»* o análogo de forma que no se faciliten todos sus datos. A pesar de que el procedimiento pueda parecer sencillo, la AEPD recibió numerosas consultas lo cual motivó la publicación de orientaciones para la aplicación provisional de la disposición séptima de la LOPDGDD.

Por último, cabe señalar que la obligación de comunicar este tipo de quiebras o incidencias que afectan a la protección de datos se encuentra relacionado con la exigencia de proveer información a la ciudadanía, así como la debida transparencia en la actuación de los poderes públicos.

6.- Derecho a la información, publicidad y transparencia en la actuación de la Administración desde la perspectiva de la protección de datos.

Como no podría ser de otra forma, desde Europa se realizan esfuerzos para la consecución del fin de transparencia de las autoridades públicas dentro de una sociedad democrática y pluralista tal y como se refleja en el Convenio del Consejo de Europa sobre el Acceso a los Documentos Públicos de 18 de junio de 2009[113].

[112] Preámbulo del Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.

[113] Según el Convenio *«el ejercicio del derecho de acceso a los documentos públicos:*
i) Proporciona una fuente de información para el público;
ii) Ayuda al público a formarse una opinión sobre el estado de la sociedad y sobre las autoridades públicas;
iii) Fomenta la integridad, la eficacia, la eficiencia y la responsabilidad de autoridades públicas, ayudando así a que se afirme su legitimidad».

Actualmente, el principio de transparencia adquiere especial importancia ante la complejidad tecnológica puesto que propicia que cada vez sea más difícil saber y comprender por parte de los ciudadanos si sus datos han sido recabados y tratados. Por esta razón se exige a los responsables el cumplimiento del principio de publicidad de forma que faciliten cualquier información concerniente a los tratamientos que realicen.

El derecho de acceso a la información pública se encuentra regulado en el capítulo III de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno (en adelante «Ley de transparencia»). Este derecho a la transparencia no presenta la condición de derecho fundamental, así se ha pronunciado la jurisprudencia del Tribunal Supremo y, en concreto, señala que no podrá formularse *«pretensión que pueda tener cabida en el limitado objeto del especial proceso contencioso-administrativo al que acudió el recurrente puesto que ni tal derecho de acceso a la información contenida en los archivos y registros constituye, en sí mismo, un derecho fundamental de los que se pueden hacer valer en dicho proceso»*[114].

El meritado derecho y el derecho a la protección de datos puede colisionar y no resulta fácil de determinar cuál de ellos debe prevalecer. A este respecto, puede afirmarse que no dará lugar a la prohibición del derecho de acceso cuando la información pública contenga datos personales[115], no obstante, se tratará de adoptar medidas como la seudonimización[116] de los datos a fin de garantizar que no puedan asociarse directamente a las personas físicas a las que afecten.

[114] Sentencia de la Sala de lo Contencioso-Administrativo, Sección 7ª del Tribunal Supremo de 19 de junio de 2012 (RJ 2012/7459). Fundamento Jurídico 2º.

[115] AA.VV., MOSCOSO DEL PRADO MUÑOZ, J., (coord.). *La protección de datos y la administración local*. «La administración local ante la gestión de la protección de datos», 1ª edición, Ed. Aranzadi, Cizur Menor, 2019, p. 88-89.

[116] En atención al RGPD, la «seudonimización» implica un tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.

En otros casos, no será necesario la adopción de estas medidas, verbigracia, cuando se solicite información al amparo de la Ley de transparencia respecto a las retribuciones percibidas por los Alcaldes de los ayuntamientos por tratarse de información del ámbito de la actividad pública que deberá ser objeto de publicación periódica y actualizada[117]. En este sentido se pronunció el Consejo de Transparencia y Buen Gobierno (CTBG)[118] en su resolución de 21 de junio de 2018 (JUR 2018/221978).

Por otro lado, el Consejo de Transparencia y Buen Gobierno no se encarga únicamente de resolver a este tipo de reclamaciones ya que también deberá controlar y evaluar el desempeño de las instituciones públicas y de sus entidades dependientes en lo que respecta al cumplimiento de las obligaciones de publicidad activa[119].

La publicidad activa también comprende la obligación de compartir y actualizar la información en los respectivos espacios webs de los organismos públicos, sin embargo, el grado de cumplimiento no es el adecuado como se desprende de estudios realizados para determinar el *índice de transparencia*[120]. En el caso de Canarias ha mejorado en los últimos ejercicios, aunque queda un largo camino por recorrer hasta alcanzar un nivel adecuado de transparencia.

A continuación, se expondrá el procedimiento a seguir ante la conculcación de principios, derechos, obligaciones y deberes en materia de protección de datos, así como el régimen sancionador.

---

[117] Artículo 5.1 de la Ley 19/2013, de 9 de diciembre.

[118] Consejo de Transparencia y Buen Gobierno es un organismo independiente con personalidad jurídica propia y plena capacidad de obrar pública y privada. Se encarga de promover la transparencia de la actividad pública, velar por el cumplimiento de las obligaciones de publicidad, salvaguardar el ejercicio del derecho de acceso a la información pública y garantizar la observancia de las disposiciones de buen gobierno.

[119] El CTBG confeccionó la *Metodología de Evaluación y Seguimiento de la Transparencia de la Actividad pública (MESTA)* con el objetivo de establecer un método de evaluación que fuera único y común.

[120] TRONCOSO REIGADA, A. (coord.). *Proceso de evaluación del cumplimiento de la Ley 12/2014, de 26 de diciembre, de transparencia de Canarias: Modelo y resultados del Índice de Transparencia de Canarias (ITCanarias).* «Trasparencia pública y Comunidades Autónomas», Ed. Tirant lo blanch, Valencia, 2019, pp. 1-5.

7.- Los procedimientos ante la vulneración de la normativa de protección de datos y el régimen sancionador.

Existen dos tipos de procedimientos, aquellos que tienen por objeto atender debidamente las reclamaciones de un afectado en el ejercicio de sus derechos y los procedimientos que deriven de la investigación de una posible infracción en materia de protección de datos. Ambos procedimientos se encuentran regulados entre los preceptos 63 a 78 de la LOPDGDD.

Está previsto que el Gobierno regule mediante Real Decreto los procedimientos[121], sin embargo, el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal aún no se ha adaptado a la nueva LOPDGDD. Este texto legal aún hace referencia al procedimiento de inscripción de la creación, modificación o supresión de ficheros en relación con la obligación de inscripción de ficheros por parte de los responsables que ha desaparecido.

Los procedimientos que encajan con la actual regulación serán los del Título IX – Capítulo I a III, en concreto, el procedimiento referido a la falta de atención de los derechos de los afectados y, por otro lado, el procedimiento relativo al ejercicio de la potestad sancionadora.

7.1.- El procedimiento referido a la falta de atención de los derechos establecidos en los artículos 15 a 22 del RGPD.

En el Real Decreto 1720/2007 se encuentra bajo la denominación de *«procedimiento de tutela los derechos de acceso, rectificación y oposición»,* pero tras la nueva regulación ahora resulta de aplicación al resto de derechos que introduce el RGPD.

[121] *Ex* artículo 63.3 de la LOPDGDD.

Este tipo de procedimiento se iniciará a instancia de los afectados a través de una reclamación que señale los preceptos de la LOPDGDD que considere vulnerados[122]. Cuando la AEPD reciba la reclamación dará traslado al responsable para que en el plazo de quince días formule las oportunas alegaciones e independientemente que la AEPD reciba tales alegaciones o transcurra el plazo deberá resolver conforme a los informes, actuaciones previas y otros actos de instrucción que se hubieran practicado. Como se trata de un procedimiento que se inspira en el procedimiento administrativo, entre los actos de instrucción se prevé la audiencia al afectado y al responsable del tratamiento.

El plazo máximo de resolución que dispone la AEPD es de nueve meses y, en el supuesto que el afectado no tuviera noticias en tres meses desde la admisión a trámite o en seis meses de la notificación con admisión a trámite, operará el silencio administrativo positivo. Cuando reciba resolución expresa y esta fuera estimatoria se requerirá al responsable del tratamiento para que en el plazo de diez días procediera a cumplir con el ejercicio del derecho objeto de tutela. Además, deberá comunicar el cumplimiento a la AEPD también en el plazo de diez días.

7.2.- El procedimiento relativo al ejercicio de la potestad sancionadora.

La Agencia Española de Protección de Datos es la autoridad que ostenta el ejercicio de la potestad sancionadora, así como las autoridades autonómicas en su ámbito territorial[123]. El ejercicio de este poder sancionador deberá respetar las debidas garantías procesales de acuerdo con el Derecho de la Unión y el de ámbito nacional[124], así como los principios comunes de los procedimientos administrativos[125].

La norma que rige en estos procedimientos sancionadores es el Real Decreto 1720/2007 y supletoriamente la LPAC tal y como prevé el propio Estatuto de la AEPD

[122] *Ex* artículo 117 del Real Decreto 1720/2007, de 21 de diciembre.
[123] *Ex* artículo 57 de la LOPDGDD.
[124] AA.VV., MOSCOSO DEL PRADO MUÑOZ, J., (coord.), *Régimen sancionador en materia de protección de datos*. «La administración local ante la gestión de la protección de datos», 1ª edición, Ed. Aranzadi, Cizur Menor, 2019, p. 415.
[125] REBOLLO PUIG, M., *El procedimiento sancionador y las actuaciones previas ante la Agencia Española de Protección de Datos*. «La potestad sancionadora de la Agencia Española de Protección de Datos». Ed. Aranzadi, Pamplona, 2008, p. 306.

en su artículo 2.c). Además, la AEPD no sólo podrá sancionar las infracciones de la LOPDGDD ya que también se incluyen las previstas en la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (en adelante «LSSI»)[126].

Respecto a los sujetos responsables se encuentran enumerados en el artículo 70 de la LOPDGDD formando parte de esta lista los responsables y encargados de los tratamientos; los representantes de los responsables o encargados de los tratamientos no establecidos en el territorio de la Unión Europea; las entidades de certificación y las entidades acreditadas de supervisión de los códigos de conducta[127]. Por el contrario, se encuentra expresamente excluido del ámbito sancionador el Delegado de Protección de Datos, aunque podría cuestionarse si está totalmente exento de responsabilidad ante una mala praxis en el ejercicio de sus funciones por parte de la entidad pública que lo hubiera designado.

Las infracciones se encuentran reguladas entre los artículos 71 a 74 de la LOPDGDD y se clasifican en leves, graves y muy graves siendo su plazo de prescripción de uno, dos y tres años, respectivamente[128]. Entre las infracciones que pueden cometer los citados sujetos se encuentra la vulneración de los principios y garantías en los tratamientos que efectúen, la no concurrencia de una base para que el tratamiento sea lícito, tratamiento de datos expresamente prohibidos, la falta de atención de las solicitudes y reclamaciones de los ciudadanos, etc.

Por lo que refiere a las sanciones se regulan en el artículo 76 de la LOPDGDD y, en síntesis, las sanciones de multa para las infracciones muy graves pueden llegar hasta 20 millones de euros o bien una cuantía equivalente al 4% como

[126] REBOLLO PUIG, M., *El procedimiento sancionador y las actuaciones previas ante la Agencia Española de Protección de Datos*. «La potestad sancionadora de la Agencia Española de Protección de Datos». Ed. Aranzadi, Pamplona, 2008, p. 303-304.
[127] Los códigos de conducta contienen reglas comunes para realizar tratamientos de datos y la adhesión y respeto a estos códigos de conducta por parte de los responsables sirve para demostrar el cumplimiento de las garantías que el RGPD considera suficientes a la hora de realizar tratamientos de datos (considerando nº 98 del RGPD y artículo 38 y 39 de la LOPDGDD).
[128] En el caso de las infracciones de la LSSI los plazos de prescripción son idénticos excepto para las infracciones leves que será de seis meses.

máximo del volumen de negocio total anual global del ejercicio financiero anterior[129]. Sin embargo, las sanciones no serán sólo pecuniarias debido a que podrán imponerse de manera adicional o sustituirse por las siguientes medidas correctivas[130]:

«1º. Advertencias previas a la infracción.

2º. Apercibimiento una vez producida la infracción.

3º. Requerimiento de atención de los ejercicios de derechos, para que los tratamientos se realicen de determinada manera y dentro de un plazo, de comunicación al interesado de las violaciones de seguridad de sus datos.

4º. Limitación temporal o definitiva del tratamiento, incluida su prohibición.

5º. Ordenar la rectificación o supresión de datos o la limitación del tratamiento; y en su caso su notificación al interesado.

6º. Sobre certificaciones: ordenar rectificarla, retirarla o su no emisión.

7º. Ordenar la suspensión de una transferencia internacional de datos»[131].

Ciertos responsables o encargados cuentan con un régimen sancionador especial como es el caso de la Administración Pública. La principal particularidad radica en que no se prevén sanciones pecuniarias cuando estos sujetos cometan infracciones, sustituyéndose por la sanción de apercibimiento.

Por lo que respecta al procedimiento sancionador cuenta con tres vías para ser iniciado: previa denuncia de una persona física o jurídica; mediante petición razonada de una entidad pública; o bien de oficio por la autoridad de control cuando tenga sospechas de la comisión de una infracción[132].

La forma de inicio del procedimiento será mediante acuerdo adoptado por propia iniciativa de la AEPD y cuando se trate de una reclamación a instancia de un interesado decidirá previamente su admisión a trámite. En ambos casos existirá una

[129] AA.VV., MOSCOSO DEL PRADO MUÑOZ, J., (coord.), *Régimen sancionador en materia de protección de datos*. «La administración local ante la gestión de la protección de datos», 1ª edición, Ed. Aranzadi, Cizur Menor, 2019, p. 417.
[130] Se ha extraído de la obra citada debido a que la LOPDGDD no prevé estas sanciones de forma expresa, aunque si las aplica en la práctica.
[131] AA.VV., MOSCOSO DEL PRADO MUÑOZ, J., (coord.), *Régimen sancionador…* op. cit., p. 418.
[132] MARTÍNEZ ROMÁN, E. *El procedimiento sancionador en la Agencia Española de Protección de Datos*. Economist & Jurist, vol.:22 iss:180, 2014, p. 21.

fase de actuaciones previas[133] de investigación cuyo objeto será determinar los hechos y circunstancias que justifican la tramitación del procedimiento. Esta fase no tendrá una duración superior a doce meses a contar desde la fecha del acuerdo de admisión a trámite o decisión de iniciación de la AEPD.

Tras finalizar la fase de actuaciones previas y siempre que concurran indicios suficientes, la Presidencia de la AEPD dictará el correspondiente acuerdo de inicio de procedimiento sancionador que contendrá la relación de hechos, la identificación del sujeto, la infracción que presuntamente se hubiera cometido y la posible sanción[134]. Asimismo, para salvaguardar el derecho fundamental a la protección de datos se podrán acordar medidas provisionales y de garantía de los derechos[135] como el bloqueo cautelar de los datos[136].

Por otro lado, con el fin de dar a conocer la reclamación al supuesto sujeto infractor, la AEPD podrá remitirla al Delegado de Protección de Datos o al encargado de supervisión de códigos de conducta antes de admitirla a trámite. Cuando no se hubiere designado a un DPD ni se hubiera adherido a un código de conducta, podrá ser remitida al responsable o encargado del tratamiento que tendrá plazo de un mes para responder a dicha reclamación.

El procedimiento sancionador también contendrá un periodo de práctica de prueba y de audiencia a los presuntos infractores resultando de aplicación las normas de la LPAC. Tras el plazo genérico de quince días para presentar alegaciones y proponer prueba, la AEPD acordará la apertura del periodo de prueba en un plazo que no podrá ser superior a treinta días ni inferior a diez y mediante resolución motivada estimará o desestimará las pruebas propuestas.

Una vez concluido el periodo de prueba, el procedimiento terminará con resolución expresa de la AEPD que deberá emitirse en el plazo de seis meses desde la

[133] *Ex* artículo 67 de la LOPDGDD.
[134] En contraposición, de no hallarse indicios suficientes para sustentar la apertura del procedimiento sancionador, se procederá al archivo de las actuaciones.
[135] *Ex* artículo 69 de la LOPDGDD.
[136] El bloqueo de datos consiste en la identificación y reserva de los datos, así como la adopción de medidas técnicas y organizativas con el fin de impedir su tratamiento (*ex* artículo 32 de la LOPDGDD).

notificación al reclamante del acuerdo de admisión a trámite. En el supuesto que no se notifique resolución el silencio será estimatorio[137]. Asimismo, operará la caducidad del procedimiento cuando transcurra el plazo de nueve meses desde el acuerdo de inicio y, por consiguiente, se procederá al archivo de actuaciones. Este plazo se ha visto ampliado en comparativa con la anterior Ley Orgánica de Protección de Datos cuyo plazo de caducidad era de seis meses.

Respecto a las resoluciones de la AEPD, se advierte que agotan la vía administrativa por lo que sólo podrá interponerse recurso potestativo de reposición[138] o bien acudir a la vía jurisdiccional mediante la interposición de recurso contencioso-administrativo[139] ante la Audiencia Nacional. A este respecto, cabe señalar que la legitimación activa para recurrir no la ostenta quien denuncia hechos constitutivos de infracción. Así lo ha reconocido la jurisprudencia y, en concreto, conviene traer a colación la resolución de la Sala de lo Contencioso-Administrativo del Tribunal Supremo de fecha 6 de octubre de 2009:

«*quien denuncia hechos que considera constitutivos de infracción de la legislación de protección de datos carece de legitimación activa para impugnar en vía jurisdiccional lo que resuelva la Agencia […]. La razón es, en sustancia, que el denunciante carece de la condición de interesado en el procedimiento sancionador que se puede incoar a resultas de su denuncia. Ni la Ley Orgánica de Protección de Datos ni su Reglamento de desarrollo le reconocen esa condición. Y por lo que se refiere a los principios generales del derecho administrativo sancionador, aunque en algunas ocasiones esta Sala ha dicho que el denunciante puede impugnar el archivo de la denuncia por la Administración, no se admite que el denunciante pueda impugnar la resolución administrativa final. El argumento crucial en esta materia es que el denunciante, incluso cuando se considere a sí mismo "víctima" de la infracción denunciada, no tiene un derecho subjetivo ni un interés legítimo a que el denunciado sea sancionado*»[140].

[137] Artículo 64.1 de la LOPDGDD.
[138] El recurso potestativo de reposición podrá interponerse ante el mismo órgano que dictó la resolución en el plazo de un mes.
[139] El recurso contencioso-administrativo podrá interponerse ante la Audiencia Nacional en el plazo de dos meses.
[140] Sentencia de la Sala de lo Contencioso-Administrativo, Sección 6ª del Tribunal Supremo de 6 de octubre de 2009 (RJ 2010/966). Fundamento Jurídico 6º.

Se concluye que sólo la AEPD ostenta interés legítimo en que los infractores sean sancionados como consecuencia de que la potestad sancionadora corresponda a la Administración.

Por otro lado, cuando el infractor sea un órgano público ya se enunciaba que las sanciones que se impondrán serán de apercibimiento y, además, la resolución que se dicte contendrá medidas con el objeto de que cese la conducta o se corrijan los efectos que hubiera ocasionado la infracción[141]. Asimismo, cuando existan indicios suficientes, la autoridad de control propondrá la iniciación de actuaciones disciplinarias tal y como señala el artículo 77.3 de la LOPDGDD que se remite a la legislación que resulte de aplicación sobre régimen disciplinario o sancionador. Será habitual que las actuaciones disciplinarias se dirijan frente a funcionarios públicos y el personal laboral a servicio de las entidades públicas, de ahí que resulte de aplicación las disposiciones previstas en el Título VII del Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público.

En el supuesto de que las infracciones fueran imputadas a autoridades y directivos y, además, se acredite la existencia de informes técnicos o recomendaciones para el tratamiento que éstos no hubieran atendido, la sanción incluirá una amonestación con identificación del cargo responsable y se ordenará su publicación en el Boletín Oficial del Estado (BOE) o autonómico que corresponda[142].

Asimismo, la resolución que se dicte tras finalizar el procedimiento disciplinario deberá ser comunicada a la AEPD que se encargará de dar publicidad en su página web de la referida resolución. En su caso, también se comunicará a las autoridades autonómicas en protección de datos que estarán a lo dispuesto en su normativa específica y lo mismo se aplica al Defensor del Pueblo o instituciones análogas de las comunidades autónomas.

[141] AA.VV., MOSCOSO DEL PRADO MUÑOZ, J., (coord.), *Régimen sancionador en materia de protección de datos.* «La administración local ante la gestión de la protección de datos», 1ª edición, Ed. Aranzadi, Cizur Menor, 2019, pp. 423-424.
[142] Ex artículo 77.3 de la LOPDGDD.

A pesar de que pueda parecer que los procedimientos analizados se encuentran desligados entre sí, lo cierto es que la falta de atención de los derechos de los interesados puede tener trascendencia sancionadora para los responsables, ya que es constitutivo de infracción[143]. En esos casos, la AEPD procederá de oficio a incoar procedimiento sancionador cuando no se atiendan las solicitudes de los interesados.

Conviene advertir que entre los sujetos infractores no está previsto que la responsabilidad sea extensible a otro tipo de personas que intervengan en cualquier fase del tratamiento. A este respecto, dado que existe un deber de confidencialidad entre cualquier sujeto que intervenga en un tratamiento y los responsables, resulta paradójico su falta de inclusión como sujetos infractores, lo cual se traduce en que quedará al arbitrio del responsable la iniciación de un procedimiento disciplinario.

Entre los sujetos exentos de responsabilidad destaca el Delegado de protección de datos que se encuentra expresamente excluido, a pesar de que debería estar sujeto al régimen sancionador pues en su actividad tendrá que respetar el referido deber de confidencialidad. Además, la negligencia del Delegado puede perjudicar gravemente al responsable del tratamiento al igual que poner en riesgo la seguridad de los datos, por ende, resulta un error que no esté incluido entre los sujetos infractores.

Seguidamente se efectuará un análisis de las resoluciones emitidas en esta materia por la autoridad de control, en este caso, la Agencia Española de Protección de Datos.

[143] RALLO LOMBARTE, A., (coord.), *Procedimientos por vulneración de la normativa de protección de datos: tramitación de denuncias*. «Tratado de protección de datos: actualizado con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales», 1ª edición, Ed. Tirant lo blanch, Valencia, 2019, p. 552.

8.- Breve análisis de las resoluciones emitidas por la Agencia Española de Protección de Datos.

Las resoluciones de la Agencia Española de Protección de Datos se publican en su propia página web[144] tal y como está previsto en la Instrucción 1/2004, de 22 de diciembre, de la Agencia Española de Protección de Datos sobre publicación de sus Resoluciones. A través de la publicación de resoluciones cumple con uno de sus principales objetivos como es lograr una mayor transparencia en su actividad, mejor garantía y tutela del derecho fundamental a la protección de datos, así como potenciar el conocimiento de los criterios en la aplicación de la normativa sobre protección de datos[145].

Respecto a las resoluciones objeto de estudio, se ha centrado el campo de análisis desde una perspectiva subjetiva en el que el sujeto infractor fuera una entidad pública. Se advierte que las entidades que en mayor medida incumplen son los Ayuntamientos cuyas infracciones radican en no atender debidamente los derechos de los interesados. Asimismo, el derecho sobre el que se presentan mayor número de reclamaciones es el derecho de acceso seguido del derecho a la supresión de los datos[146].

9.- Conclusiones.

A la vista de lo expuesto en los apartados anteriores, se pueden obtener las siguientes conclusiones:

El Reglamento General de Protección de Datos (RGPD) ha cumplido con su fin de homogeneizar la regulación y aplicación de la normativa de protección de datos en el ámbito de la Unión Europea tras el evidente fracaso de la Directiva

[144] Página web de la AEPD dónde publica sus resoluciones: *«https://www.aepd.es/es/informes-y-resoluciones/resoluciones».*
[145] Exposición de motivos de la Instrucción 1/2004, de 22 de diciembre, de la Agencia Española de Protección de Datos sobre publicación de sus Resoluciones.
[146] La relación de resoluciones objeto de estudio aparece en el epígrafe de resoluciones consultadas.

derogada tras su aprobación. Además, ha supuesto una mayor seguridad jurídica al ser de aplicación directa y, por consiguiente, no requerir de transposición en la norma interna de los Estados miembros.

La originaria Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) dista enormemente de la actual Ley Orgánica de Protección de Datos y garantía de los derechos digitales (LOPDGDD), precisamente, por la introducción de un novedoso elenco de derechos de la era digital. Sin embargo, requiere tener cerca el RGPD debido a sus continuas remisiones a este texto por ser de aplicación directa, lo cual aumenta el esfuerzo de interpretación jurídica de la normativa de protección de datos.

Destaca el enfoque preventivo más que sancionador de la regulación lo cual se traduce en una mayor garantía en la protección de los derechos y libertades fundamentales de los ciudadanos y, en concreto, cuando estos sean afectados por tratamientos de datos.

En cuanto a su aplicación a las entidades públicas como sujetos responsables de los tratamientos, ha supuesto un gran cambio en su actividad como se advierte con la obligación de designar a un Delegado de Protección de Datos; la necesidad de realizar un registro de actividades de tratamiento de datos o las evaluaciones de impacto de protección de datos. Así como, el requisito de analizar los posibles riesgos de un tratamiento y la consecuente adopción de medidas de seguridad.

La obligación de registro de actividades de tratamiento ha supuesto una reducción de la carga burocrática tras sustituir a la inscripción obligatoria de ficheros, sin embargo, el deber de información se traduce en que los formularios que se faciliten a los ciudadanos sean más extensos.

Respecto a la obligación de contar con un Delegado de Protección de Datos en los entes públicos supone una clara ventaja de cara a la atención de solicitudes y reclamaciones de los afectados. Además, prestará asesoramiento y asistirá al responsable y encargado del tratamiento.

Debido a la importancia que presenta el Delegado de Protección de Datos y por su posición especial dentro de la organización que lo designe, resulta necesario que cuente con un estatuto jurídico íntegro que defina su figura y evite los posibles conflictos de intereses en su actuación.

Aun cuando las Administraciones Públicas actúen como responsables en un tratamiento de datos, la realidad es que ostentan una serie de prerrogativas que las distancian respecto al resto de responsables particulares en la aplicación de la normativa de protección de datos. A este respecto, un uso abusivo del interés legítimo para justificar la realización de tratamientos de datos sobre los que debería realizarse una ponderación respecto a los derechos y libertades fundamentales de los ciudadanos conllevaría a la llevanza de tratamientos que, en principio, estarían prohibidos.

Por lo que refiere al régimen sancionador, es bastante detallado y su procedimiento garantista, sin embargo, no se comparte que a las organizaciones públicas infractoras no se les pueda imponer sanciones pecuniarias. A este respecto, los apercibimientos y obligación de publicar la resolución sancionadora en los boletines oficiales correspondientes resultan insuficiente.

En contraposición con el punto anterior, los afectados por una vulneración de las normas de protección de datos no se encuentran legitimados para acudir a la vía jurisdiccional debido a que la potestad sancionadora sólo corresponde a la Agencia Española de Protección de Datos. No obstante, debería ser posible la aplicación análoga de otras figuras jurídicas como las del derecho penal para que los afectados puedan intervenir en el procedimiento.

Por último, el Delegado de Protección de Datos que se encuentra fuera del *numerus clausus* de sujetos infractores, debería incluirse debido a que el desarrollo de su actividad podría dar lugar a la comisión de infracciones sobre las que no le será de aplicación el régimen sancionador.

10.- Resoluciones judiciales y administrativas consultadas.

Resoluciones judiciales.

Tribunal Constitucional

-Sentencia del Pleno del Tribunal Constitucional de 30 de noviembre de 2000 (RJ 2000/292).

Tribunal Supremo

-Sentencia de la Sala de lo Contencioso-Administrativo, Sección 7ª del Tribunal Supremo de 19 de junio de 2012 (RJ 2012/7459).

-Sentencia de la Sala de lo Contencioso-Administrativo, Sección 6ª del Tribunal Supremo de 6 de octubre de 2009 (RJ 2010/966).

Audiencia Nacional

-Sentencia de la Sala de lo Contencioso-Administrativo, Sección 1ª de la Audiencia Nacional de 8 de marzo de 2002 (RJ 2002/143289).

-Sentencia de la Sala de lo Contencioso-Administrativo, Sección 1ª de la Audiencia Nacional de 9 de julio de 2009 (RJ 2009/363726).

Resoluciones administrativas.

Consejo de Transparencia y Buen Gobierno (CTBG) en su resolución de 21 de junio de 2018 (JUR 2018/221978).

Agencia Española de Protección de Datos

-Resolución de la AEPD nº R/00331/2019 (sujeto infractor: ayuntamiento)

-Resolución de la AEPD nº R/00064/2019 (sujeto infractor: encargado del tratamiento de un ayuntamiento)

-Resolución de la AEPD nº R/01061/2018 (sujeto infractor: ayuntamiento)

-Resolución de la AEPD nº R/01264/2018 (ídem)
-Resolución de la AEPD nº R/00570/2018 (ídem)
-Resolución de la AEPD nº R/01498/2018 (ídem)
-Resolución de la AEPD nº R/00788/2018 (ídem)
-Resolución de la AEPD nº R/00826/2018 (ídem)
-Resolución de la AEPD nº R/00336/2018 (ídem)
-Resolución de la AEPD nº R/00335/2018 (ídem)
-Resolución de la AEPD nº R/00348/2018 (ídem)
-Resolución de la AEPD nº R/01762/2018 (ídem)
-Resolución de la AEPD nº R/01574/2018 (ídem)
-Resolución de la AEPD nº R/01440/2018 (ídem)
-Resolución de la AEPD nº R/01451/2018 (ídem)
-Resolución de la AEPD nº R/01329/2018 (ídem)
-Resolución de la AEPD nº R/01323/2018 (ídem)
-Resolución de la AEPD nº R/00482/2018 (ídem)

11.- Bibliografía.

AA.VV., MOSCOSO DEL PRADO MUÑOZ, J. (coord), «La administración local ante la gestión de la protección de datos», 1ª edición, Ed. Aranzadi, Cizur Menor, 2019.

MARTÍNEZ VILLASECA, M., *El interés legítimo como base legitimadora del tratamiento de datos de carácter personal,* Actualidad administrativa, nº 12, Wolters Kluwer, Madrid, 2019.

CAMPOS ACUÑA, C., *Impacto de la nueva Ley Orgánica de protección de datos personales y garantía de los derechos digitales en el ámbito local*. Revista digital CEMCI, nº 40, Granada, 2018.

DAVARA RODRÍGUEZ, M.Á., *El Delegado de Protección de Datos en los ficheros y/o tratamientos de la Administración en consonancia con el Reglamento Europeo de Protección de Datos*. Actualidad Administrativa, nº 1, Ed. Wolters Kluwer, Madrid, 2017.

MARTOS, N., *El Delegado de Protección de Datos: ¿figura interna, externa o mixta?,* Actualidad Jurídica Aranzadi, núm. 936/2017, Ed. Aranzadi, S.A.U., Cizur Menor, 2017.

RALLO LOMBARTE, A., (coord.). «Tratado de protección de datos: actualizado con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales», 1ª edición, Ed. Tirant lo blanch, Valencia, 2019.

RODRÍGUEZ AYUSO, J.F., *El delegado de protección de datos en el ámbito de la Administración Pública.* Actualidad Administrativa, nº 7-8, Ed. Wolters Kluwer, Madrid, 2019.

DÍAZ, E., *El nuevo Reglamento General de Protección de Datos de la Unión Europea y sus consecuencias jurídicas para las instituciones*, Revista Aranzadi Doctrinal núm. 6/2015, Ed. Aranzadi, Cizur Menor, 2016.

TRONCOSO REIGADA, A. (coord.). *Proceso de evaluación del cumplimiento de la Ley 12/2014, de 26 de diciembre, de transparencia de Canarias: Modelo y resultados del Índice de Transparencia de Canarias (ITCanarias)*. «Trasparencia pública y Comunidades Autónomas», Ed. Tirant lo blanch, Valencia, 2019.

REBOLLO PUIG, M., «La potestad sancionadora de la Agencia Española de Protección de Datos». Ed. Aranzadi, Pamplona, 2008.

MARTÍNEZ ROMÁN, E. *El procedimiento sancionador en la Agencia Española de Protección de Datos*. Economist & Jurist, vol.:22 iss:180, 2014.

12.- Otra documentación consultada.

Guía sectorial de *Protección de Datos y Administración Local* publicada el 16 de mayo de 2018 por la Agencia Española de Protección de Datos.

Guía para el ciudadano publicada el 7 de febrero de 2019 por la Agencia Española de Protección de Datos.

Grupo de trabajo del artículo 29. Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679 de 10 de abril de 2018 (WP 259 y rev.01).

Principio de accountability (Protección de Datos), Guías Jurídicas de Wolters Kluwer, Madrid, última consulta: 10/01/2020.

Grupo de trabajo del artículo 29. Dictamen 3/2010 sobre el principio de responsabilidad de 13 de julio de 2010 (WP173).

Guía general para el cumplimiento del deber de informar publicada el 22 de mayo de 2018 por la Agencia Española de Protección de Datos con colaboración de la Autoridad Catalana de Protección de Datos y la Agencia Vasca de Protección de Datos.

Guía de Privacidad desde el Diseño publicada el 12 de noviembre de 2019 por la Agencia Española de Protección de Datos. En esta Guía la privacidad desde el diseño se define como la suma integral del enfoque al riesgo y la responsabilidad proactiva.

Guía práctica para las Evaluaciones de Impacto en la Protección de los Datos sujetas al RGPD (guía general) publicada el 17 de enero de 2018 por la Agencia Española de Protección de Datos.

Guía general del Reglamento General de Protección de Datos para Responsables de Tratamiento adoptada el 22 de mayo de 2018 por la Agencia Española de Protección de Datos con colaboración de la Autoridad Catalana de Protección de Datos y la Agencia Vasca de Protección de Datos.

Directrices para la elaboración de contratos entre responsables y encargados del tratamiento de publicado el 16 de mayo de 2018 por la Agencia Española de Protección de Datos.

El Impacto del Reglamento General de Protección de Datos sobre la Actividad de las Administraciones Publicas publicado el 25 de mayo de 2018 por la Agencia Española de Protección de Datos.

Estudio del Centro de Investigaciones Sociológicas (CIS) número 3213 realizado entre el 1 al 10 de mayo de 2018.

Memoria anual de actividad del año 2018 de la Agencia Española de Protección de Datos.

El delegado de protección de datos en las administraciones públicas publicado el 1 de octubre de 2019 por la Agencia Española de Protección de Datos.

Guía práctica para las evaluaciones de impacto en la protección de los datos sujetas al RGPD publicado el 17 de enero de 2018 de la Agencia Española de Protección de Datos.