LA RESPONSABILIDAD PROACTIVA DE LAS ADMINISTRACIONES PÚBLICAS EN LA PROTECCIÓN DE DATOS PERSONALES

THE PROACTIVE RESPONSIBILITY OF PUBLIC ADMINISTRATIONS IN THE PROTECTION OF PERSONAL DATA

Aritz Romeo Ruiz
Profesor Ayudante Doctor de Derecho Administrativo
Universidad Pública de Navarra
aritz.romeo@unavarra.es
https://orcid.org/0000-0002-8150-458X

Recibido: 22/07/2019 Aceptado: 19/04/2020

Laburpena: Lan honen helburua da administrazio publikoak datu pertsonalen tratamenduan duen erantzukizun proaktiboaren printzipioaren analisia eskaintzea, eta ikuspegi juridikoa ematea praktikan errazago aplikatzeko. Lana lau ataletan egituratuta dago. Lehenengoan, datu pertsonalen babesa arautzen duen esparru berriaren aurkezpen orokorra egiten da; hau da, Datuak Babesteko Erregelamendu Orokorrak (EB) ezartzen duen araudi berria aurkezten da. Bigarren atala erantzukizun proaktiboari buruzkoa da, administrazio publikoek datu pertsonalak tratatzeko oinarrizko printzipio gisa. Hirugarrenak proposatzen ditu administrazio publikoek praktikan erantzukizun proaktiboaren printzipioa betetzeko kontuan har ditzaketen hainbat neurri. Azkenik, laugarren atalak gogoeta egiten du antolamendu-aldaketak egiteko beharrari buruz, Erregelamendu Orokorraren printzipioak betetzen dituztela ziurtatzeko eta herritarrek eskubideak balia ditzaten ziurtatzeko; horrez gain, aipamen berezia egiten dio datuak babesteko ordezkariaren figurari. Ondorioztatzen den ideia nagusia da garrantzitsua dela administrazio publikoek datuak babesteko politika bat diseinatzea, lehenetsita aplikatuko dena, eta ez bakarrik erantzukizun politikoak dituztenei, baizik eta sektore publikoan lan egiten duten pertsona guztiei eragingo diena.

Gako-hitzak: Administrazio Publikoa, Big Data, Teknologia Berriak, Datuen Babesa, Datuen Babeserako Erregelamendu Orokorra, Erantzukizun Proaktiboa.

Resumen: El presente trabajo tiene como objetivo ofrecer un análisis del principio de responsabilidad proactiva en el tratamiento de datos personales por parte de la administración pública, y pretende aportar una visión jurídica para facilitar su aplicación en la práctica. El trabajo está estructurado en cuatro apartados. En el primero de ellos se presenta, en términos generales, el nuevo marco regulador de la protección de datos personales, que es consecuencia del Reglamento (UE) General de Protección de Datos. El segundo apartado está dedicado a la responsabilidad proactiva como principio básico del tratamiento de datos personales por las administraciones públicas. El tercero propone una serie de medidas que las administraciones públicas pueden tener en cuenta para cumplir con el principio de responsabilidad proactiva en la práctica. Finalmente, el apartado cuarto aporta una reflexión sobre la necesidad de introducir cambios organizacionales para asegurar el cumplimiento de los principios del Reglamento General de Protección de datos y del ejercicio de derechos por la ciudadanía, con una especial mención a la figura del delegado o delegada de protección de datos. La principal idea que se concluye es la importancia de que las administraciones públicas diseñen una política de protección de datos que se aplique por defecto, e implique, no sólo a quienes ejercen responsabilidades políticas, sino a todas las personas que trabajan en el sector público.
Palabras clave: Administración Pública, Big Data, Nuevas Tecnologías, Protección de Datos, Reglamento General de Protección de Datos, Responsabilidad Proactiva.

Abstract: The present work aims to offer an analysis of the principle of proactive responsibility in the treatment of personal data by the public administration, and aims to provide a legal vision to facilitate its practical implementation . The work is structured in four sections. The first of these presents, in general terms, the new regulatory framework for the protection of personal data, which is a consequence of the General Data Protection Regulation (EU). The second section is dedicated to proactive responsibility as a basic principle of the processing of personal data by public administrations. The third proposes a series of measures that public administrations can take into account to comply with the principle of proactive responsibility in practice. Finally, the fourth section provides a reflection on the need to introduce organizational changes to ensure compliance with the principles of the General Data Protection Regulation and the exercise of rights by citizens, with special reference to the figure of the Data Protection Officer . The main idea that is concluded is the importance for public administrations to design a data protection policy that is applied by default, and involves not only those who exercise political responsibilities, but also all those who work in the public sector.
Keywords: Public Administration, Big Data, New Technologies, Data Protection, General Data Protection Regulation, Proactive Liability.

Sumario

1. Apertura de una nueva época para la protección de datos

1.1. Una nueva regulación: un Reglamento de la Unión Europea

El 25 de mayo de 2018 ha entrado en vigor 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 y por el que se deroga la Directiva 95/46/CE (RGPD, en adelante), que incorpora un importante cambio de paradigma en materia de protección de datos, para sujetos públicos y privados, y que, por tanto, las administraciones públicas deben tener en cuenta, puesto que actúan de forma relevante y continuada como responsables de tratamiento respecto a los datos personales.

El Reglamento deroga la Directiva 95/46, después de 17 años de vida jurídica, supera la protección que ofrece a los datos personales y cambia la visión que han de tener las organizaciones responsables de tratamiento en relación con la protección de datos, si bien parte de los objetivos y principios de la directiva «siguen siendo válidos», tal y como se establece en el considerando 9.º RGPD.

Además del Reglamento, recientemente se ha aprobado la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD). La LOPDGDD está estructurada en diez Títulos y responde a un doble objeto, por un lado, la adaptación al ordenamiento jurídico español del RGPD, estableciendo que el derecho fundamental a la protección de datos, contenido en el artículo 18.4 CE se ejercerá con arreglo a dicho Reglamento. Y, en segundo lugar, busca garantizar los derechos digitales de la ciudadanía, que quedan regulados en el Título X de esta ley orgánica.

Debe tenerse en cuenta que a nivel de España la protección de datos personales es un derecho fundamental de los comprendidos en la Sección Primera del Capítulo Segundo del Título Primero de la Constitución, recogido en el artículo 18.4 (García, 2018). Y que el Tribunal Constitucional, en su Sentencia (STC) 94/1998, de 4 de mayo, dejó sentado que el artículo 18.4 de la Carta Magna instituye un derecho fundamental a la protección de datos, que se concreta en la facultad de las personas de oponerse a un uso de sus propios datos de carácter personal distinto de aquel para el que fueron cedidos. En definitiva, el derecho fundamental a la protección de datos garantiza el control sobre el uso y el destino de los datos personales de cada persona (Boix, 2015, p. 16). Además del resto de garantías que la Constitución establece para los derechos fundamentales, constituye un derecho subjetivo exigible frente a otros individuos y frente a los poderes públicos, que puede ser invocado ante los tribunales, siendo objeto de recurso de amparo ante el Tribunal Constitucional. La protección de datos es una manifestación del derecho a la autodeterminación informativa, y está dirigida a preservar la intimidad, y un aspecto de ésta como es la privacidad, por lo que su objetivo último es la salvaguarda de un valor jurídico tan primigenio como la dignidad de la persona.

Y la protección de datos es una construcción jurídica, protegida bajo el manto de los derechos fundamentales, que tiene por objetivo la salvaguarda, frente al uso de la tecnología, de la libertad y la dignidad humana, aplicadas el estadio de la privacidad, la cual garantiza, en la era de Internet, el disfrute de un marco de autonomía propia frente a inmisiones de terceros (Barrio, 2018:89).

La naturaleza de derecho fundamental se encuentra también recogida en la Carta Europea de Derechos Fundamentales de la Unión Europea, que en su artículo 8 proclama la protección de datos como un derecho fundamental de los ciudadanos europeos (Lattanzi, 2015, p. 103).

El derecho europeo de protección de datos parte del Convenio 108 de 28 de enero 1981, del Consejo de Europa, que supuso una primera extensión de la protección de datos personales (Rallo, 2017).

El nuevo RGPD obedece a las necesidades actuales derivadas de la vertiginosa evolución de la tecnología y las infinitas posibilidades que ofrecen las TIC, que han hecho necesario avanzar hacia un marco de mayor protección jurídica. Y es que, no debemos olvidar que vivimos no ya en la era de la revolución tecnológica, sino más allá de eso, en la sociedad del dato. Mostramos nuestra vida a través de internet: subiendo a Facebook las fotos de las vacaciones, compartiendo nuestra opinión en *Twitter*, poniendo *stories* en *Instagram* contando aspectos de lo más variado de nuestra actividad diaria, compartiendo contenido profesional en *LinkedIn*, y, en general, dando muestras de cómo acontece nuestra cotidianeidad, a través de las más variadas redes sociales. Pero, además, trabajamos a través de internet, a través de sistemas como el *cloud computing* almacenamos en la nube una no desdeñable cantidad de datos personales de nuestros clientes en servidores que, en muchos casos, ni siquiera se encuentran en la Unión Europea[1]. A todo ello hay que añadir el volumen de transferencia de datos que se produce a través del denominado «internet de las cosas», por medio del cual nuestros dispositivos y electrodomésticos de uso cotidiano están conectados a la RED y a través de esta son localizados y controlados (Troncoso, 2012, p.35).

En la era de lo que Bauman ha llamado la «modernidad líquida» (Bauman, 2017), a través del *Big data* se puede saber aspectos fundamentales de nuestra esfera más íntima como dónde estamos en cada momento, a qué nos dedicamos, cuales son nuestros gustos musicales, cómo vestimos, dónde compramos, con quién pasamos nuestro tiempo libre o cuales son nuestras preferencias políticas. Así, nuestra vida privada es predecible, es identificable (Garriga, 2016:65).

Toda esa cantidad inabarcable de datos es objeto de tráfico económico. Las grandes compañías comercian con nuestros datos (Navas, 2017) a través del *Big Deal* (Sancho, 2019:4), tratándolos como paquetes a explotar económicamente (Han, 2014:98), en un mercado francamente rentable, pues la materia prima objeto de transacción para los denominados *Data Brokers* es cedida gratuitamente por sus propietarios y propietarias (Martínez y Sancho, 2018:20), es decir, por las personas usuarias de redes sociales, y aplicaciones informáticas en general. Así, puede afirmarse que hemos transitado del internet de las cosas al internet de las corporaciones (Del Fresno, 2014:107).

Ante esta situación, el derecho debía dar una respuesta para prevenir la vulneración de la privacidad, a través del fortalecimiento del marco jurídico de protección de datos personales (Jiménez, 2018.ª, p. 16). No obstante, la eficacia del derecho se va a topar con un obstáculo importante como es la evolución frenética de la tecnología, o lo que algún autor ha denominado «*efecto Hotel California*», ya que resulta prácticamente imposible un borrado total de la información y los datos que han sido depositados en la red (Troncoso, 2010, p. 47).

Por eso, era necesario superar y reforzar el marco de protección de la privacidad en este contexto de la «sociedad de dato», para salvaguardar derechos fundamentales como la dignidad de la persona y la privacidad (Cotino, 2019, p.15).

El nuevo Reglamento encuentra justificación en esta nueva realidad. Y además, esta nueva regulación europea se realiza bajo la veste de Reglamento, y no de Directiva, para que sea de aplicación directa en todos los Estados de la Unión Europea (Razquin, 2019, p. 143). El Reglamento tiene alcance general, y debe ser aplicado en todo el territorio de la Unión Europea (UE) integrándose de manera directa en el ordenamiento interno de los Estados, sin necesidad de que éstos realicen acto previo de transposición (García, 2018, p. 71).

Se cumple de esta manera el objetivo de superar la aplicación fragmentada del régimen de protección de datos, según la normativa interna de cada Estado, lo que generaba una inseguridad jurídica, fundamentalmente en las actividades *online*, y dificultaba la libre circulación de los datos, por lo que resultaba esencial garantizar un mismo marco jurídico de protección de datos personales en el ámbito de la UE según el considerando 9.º RGPD.

1.2. **Los aspectos fundamentales del nuevo RGPD**

Además de constituir una norma de aplicación directa sin necesidad de transposición, lo que supone que en todo el ámbito europeo a partir de ahora existe una única e igual regulación en materia de protección de datos personales, el RGPD aporta seguridad jurídica y transparencia a los operadores que realicen actividades de tratamiento de datos, dando un mismo nivel de protección y, por tanto, de exigencia, en todo el ámbito de la UE (considerando 13.º RGDP).

Además, incorpora un nuevo ámbito de aplicación recogiendo la doctrina del Tribunal de Justicia de la Unión Europea (TJUE) en la importante sentencia en el asunto de Mario Costeja contra Google Spain y que recoge el RGPD[2]: se aplica a las actividades de tratamiento realizadas por entidades con establecimiento en la UE, aunque el tratamiento se haya desarrollado fuera de la Unión Europea.

También, el Reglamento amplía los derechos de la ciudadanía, de manera que el anterior marco constituido por los denominados «Derechos ARCO» (acceso, rectificación, cancelación y oposición), queda superado por los nuevos derechos: derecho de acceso, derecho de rectificación, derecho de oposición, derecho de supresión («al olvido»), derecho a la limitación del tratamiento, derecho a la portabilidad, derecho a no ser objeto de decisiones individuales automatizadas y derecho de información.

Además, el Reglamento establece los siguientes principios, en los que todo tratamiento debe basarse (Puyol, 2016):

- Principio de licitud, lealtad y transparencia: los responsables de tratamiento deben ser transparentes en cuanto a lo que hacen con los datos que la ciudadanía les ha confiado, deben tratarlos lícitamente y con lealtad.
- Principio de limitación de finalidad: los datos deben ser tratados para el fin para el que han sido recabados, pero no para objetivos diferentes. En este sentido debe hacerse referencia al importante cambio que se ha producido con respecto al consentimiento, que deja de ser un principio para pasar a considerarse una base jurídica del tratamiento, recogida en el artículo 6 RGPD[3]. En aplicación del RGPD el consentimiento pasa a ser «*toda manifestación de voluntad libre, específica, informada e inequívoca, por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen*». Esto exige una acción positiva de la persona afectada que deberá realizar esa manifestación de que es su voluntad consentir que sus datos vayan a ser tratados, para los fines de los que ha tenido que ser previamente informado. Por tanto, sólo habrá consentimiento si la persona afectada realiza un acto afirmativo libre, específico, informado e inequívoco.
- Principio de minimización: el tratamiento de datos debe limitarse a lo estrictamente necesario. Y además solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios.
- Principio de exactitud (LOPD): los datos deben ser exactos y estar actualizados. Las personas responsables del tratamiento deberán adoptar las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan, tal y como establece el artículo 5.1.d RGPD.
- Principio de limitación del plazo de conservación, contenido en el artículo 5.1.d) RGPD, que establece que los datos serán mantenidos de manera que permitan la identificación de las personas interesadas durante el tiempo que resulte necesario para cumplir los fines del tratamiento. No obstante, se permiten tratamientos de mayor duración cuando se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, aunque estableciendo medidas que garanticen la protección de los derechos del interesado o interesada.
- Principio de integridad y confidencialidad. El artículo 5.1.f) RGDP establece que los datos serán «*tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas*». Así, este principio queda directamente relacionado con el principio de responsabilidad proactiva, pues exige que las personas responsables del tratamiento establezcan medidas que garanticen tanto la seguridad de la información y la confidencialidad en cada tratamiento de datos.

2. La responsabilidad proactiva: principio básico del tratamiento de datos por las Administraciones públicas

Con todo, probablemente el principio que mejor define el cambio de paradigma que incorpora el Reglamento, es el principio de responsabilidad proactiva. El art. 5.2 RGPD lo recoge en estos términos: *«El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo ("responsabilidad proactiva")»*.

El sistema precedente se basaba en el cumplimiento de los imperativos legales, y, por ejemplo, bajo el

marco de la Directiva y la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), se limitaba a la creación de unos ficheros de la Agencia Española de Protección de Datos (en adelante, AEPD) y la incorporación de los datos a los ficheros, y a seguir las demás prescripciones de la Ley Orgánica.

Este nuevo concepto se trae del Grupo de Trabajo del artículo 29 (sustituido desde la entrada en vigor del RGPD por el Comité Europeo de Protección de Datos), que desarrolló, en su Dictamen 3/2010, de 13 de julio, el concepto de responsabilidad proactiva, basado, como ya se ha señalado en la *accountability*. Como señala el Dictamen, *«un principio reglamentario de responsabilidad requeriría expresamente que los responsables del tratamiento de datos aplicaran medidas adecuadas y eficaces para poner en práctica los principios y obligaciones de la Directiva y demostrar este extremo cuando se les solicitara»*. Y para ello, aconseja el acometimiento de una serie de medidas de responsabilidad proactiva, como la puesta en marcha de procedimientos internos de cumplimiento, evaluaciones sobre el impacto del tratamiento de los datos sobre la privacidad, la adopción de normas para tratamientos nuevos o establecimientos de mecanismos de control para garantizar el cumplimiento efectivo de las medidas (apartado 41.º del Dictamen) (Nogueira, 2018:1).

Ahora se produce un cambio radical de una lógica de actuación basada en la comunicación de actuaciones previas, a una exigencia de actuación proactiva (Gudín, 2018:85), basada en el concepto anglosajón de *accountability* (Glavey, 2000:134). Así, el principio de responsabilidad proactiva supone el basamento del nuevo paradigma introducido por el RGPD (Jiménez, 2019, p. 125).

En definitiva, el Reglamento ha incorporado una nueva visión a la protección de datos, desde una perspectiva garantista del derecho a la privacidad y de la autodeterminación informativa. Esta pretende servir de elemento de preservación frente a los riesgos que entraña el mal uso, el abuso y el uso descontrolado y desregulado de la tecnología, en el contexto de la sociedad del dato.

En todo caso, lo relevante es que las administraciones públicas tienen el deber de mantener una actitud activa en la preservación de los datos personales de sus administrados y administradas pues, es el primer quehacer de los poderes públicos garantizar la libertad y la dignidad de la ciudadanía.

El RGPD, en su considerando 85, alerta sobre la necesidad de tomar «a tiempo» las medidas de protección, anticipándose a las posibles vulneraciones de la privacidad que puedan acontecer como consecuencia de los tratamientos, con base en el principio de responsabilidad proactiva.

Principio que proclama su artículo 24 y que se materializa en el conjunto de medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el RGPD, que debe adoptar la persona responsable del tratamiento de los datos.

En consecuencia, en virtud del principio de responsabilidad proactiva, las personas responsables del tratamiento deben asumir activamente el cumplimiento de los principios del tratamiento, y asegurarse de que los mismos se han cumplido. Y, además de ello han de poder acreditar su cumplimiento[4].

Todo ello exige medidas que permitan una anticipación a las incidencias o incidentes que puedan surgir, para evitar una vulneración del derecho a la privacidad de la ciudadanía que ha cedido sus datos.

Por tanto, la acción de la administración debe dirigirse, de inicio, a la protección de datos personales. Y debe hacerse desde una vertiente activa.

Eso requiere considerar el parámetro de la protección de datos desde el diseño de las actividades que se vayan a desarrollar y puedan entrañar tratamiento de datos. Es decir, el llevar a cabo una serie de medidas concretas, que se basen en una metodología de cumplimiento de los principios y obligaciones que establecen tanto el RGPD como la LOPDGDD.

Las administraciones públicas deben, por lo tanto, contar con un Programa de Cumplimiento, o una Política de Seguridad de la Información, en la que se especifique qué medidas se van a tomar en cada caso, en cada situación que sea previsible, de acuerdo con el Reglamento y con el Esquema Nacional de Seguridad[5].

Y debe comprender, además, medidas adecuadas desde el punto de vista técnico y desde el punto de vista administrativo, así como medidas a adoptar por defecto, como pueden ser, por ejemplo, la disociación de datos en determinados supuestos, o la alteración aleatoria de los caracteres alfanuméricos del documento de identificación al publicar en Boletines Oficiales.

Se establece un nuevo modelo en el que la necesidad de cumplimiento de los principios establecidos por el RGPD y la necesidad de acreditar en cada momento que efectivamente se está cumpliendo, exige la puesta en marcha de una serie de medidas concretas basadas en una política de *compliance* (Jiménez, 2018.ª, p. 30) que va a requerir, además, la introducción de nuevas figuras relacionadas con el control y la gestión de los tratamientos de datos personales en las organizaciones de las administraciones públicas.

El nuevo marco requiere el cumplimiento de una serie de obligaciones por parte de los poderes públicos. El Reglamento exige que las administraciones públicas, en cuanto titulares del tratamiento, asuman de manera proactiva su responsabilidad. Pero ¿cómo puede ser proactiva una administración?, ¿qué medidas han de implementarse?

3. Medidas para la proactividad en las Administraciones Públicas

La Agencia Española de Protección de Datos (AEPD) ha destacado la necesidad de que las personas responsables del tratamiento adopten «*una actitud consciente, diligente y proactiva por parte de las organizaciones frente a todos los tratamientos de datos personales que lleven a cabo*»[6]. De esta forma, la Agencia establece, como ejemplos de medidas que pueden encuadrarse dentro del principio de responsabilidad proactiva, las siguientes[7]:

— Contar con un delegado o delegada de protección de datos en la organización.
— Llevar un registro de las actividades de tratamiento.
— Adoptar medidas de protección de datos desde el diseño de una política específica que se aplique por defecto.
— Realizar un análisis de riesgos y acometer medidas de seguridad basadas en el mismo.
— Notificar las quiebras que pudieran suceder en la seguridad.
— Realizar evaluaciones de impacto.
— Promover la adhesión por parte de personas responsables y encargadas de tratamiento a códigos de conducta, mecanismos de certificación, sellos y marcas de protección de datos.

Además de esas recomendaciones generales, la AEPD ha establecido una serie de medidas que las administraciones públicas deberán aplicar para cumplir de manera adecuada con el principio de responsabilidad proactiva, a la hora de adaptar su actuación al RGPD[8]. También la Agencia Vasca de Protección de Datos (AVPD) ha publicado la «Guía en ocho pasos», para facilitar la adecuación de las administraciones públicas al RGPD[9].

Las medidas a adoptar pueden encuadrarse en diferentes apartados:

3.1. Identificar la finalidad y la base jurídica del tratamiento

En primer lugar, se resalta la necesidad de identificar de manera precisa la finalidad y la base jurídica de la actividad de tratamiento, que adquiere una especial relevancia en el nuevo RGPD.

El considerando 40 RGPD, y el artículo 6.1 de mismo, prevén que, para que el tratamiento sea lícito, deberá estar basado o bien en el consentimiento de la persona titular de los datos, o bien en una de las causas legales que legitiman ese tratamiento, de manera que el tratamiento será lícito si se encuadra en alguna de las siguientes causas (Gudín, 2018:90).

Cuando la necesidad del tratamiento se derive de un contrato que haya suscrito la persona afectada, o que sea necesario realizar el tratamiento para la realización de actuaciones precontractuales en el marco de un contrato.

En los casos en que el tratamiento resulte necesario para el cumplimiento de una obligación legal por parte de la persona responsable del tratamiento.

En supuestos en que exista necesidad de realizar el tratamiento para proteger intereses vitales o bien de la persona interesada o bien de cualquier otra persona física.

Cuando la necesidad del tratamiento esté fundamentada en el cumplimiento de una misión basada en el interés público o en ejercicio de poderes públicos por parte del tratamiento.

Que el tratamiento sea necesario para responder a intereses legítimos, salvo que prevalezcan los derechos y libertades fundamentales de la persona interesada en materia de protección de datos personales, y muy especialmente cuando ésta sea menor de edad. Debe mencionarse que dicho interés legítimo puede ser tanto de la persona responsable del tratamiento como de una tercera persona, si bien, en el caso de las administraciones públicas, estas no pueden invocar un interés propio, sino que, el interés que legitima el tratamiento de datos por parte de la administración es el interés público. No obstante, sí podría apreciarse por parte de una administración pública el interés legítimo de una tercera persona.

La LOPDGDD, en su artículo 8, refuerza la necesidad de que el tratamiento se fundamente sobre una norma de rango legal o en el cumplimiento de fines de interés público, remitiéndose al artículo 6.1 RGDP, y recalca que cuando se base en el cumplimiento de fines de interés público, los mismos deberán derivarse de cumplimiento de una norma con rango legal.

En el caso de las administraciones públicas, en la mayoría de los supuestos, el tratamiento estará basado en el interés general y en el cumplimiento de normas de rango legal, prestando especial interés a los datos especialmente protegidos.

La AEPD, en su Informe Jurídico 175/2018, ha analizado la base del tratamiento de datos por parte de administraciones públicas. Según este informe, en aquellas relaciones jurídicas en las que no se dé un equilibrio entre la persona responsable del tratamiento y la persona titular de los datos (como sucede en los casos en los que una administración pública es responsable del tratamiento), la base jurídica del tratamiento no estará amparada en el consentimiento sino en el cumplimiento de una obligación legal y en el interés público. En este caso, por obligación legal, debe entenderse el mandato contenido en una norma con rango de ley.

La Agencia afirma en el mismo informe que el hecho de que el tratamiento se legitime sobre la base del cumplimiento de una obligación legal, no lo convierte en ilimitado. Las administraciones públicas están igualmente sujetas a los principios del derecho de protección de datos y, por tanto, deben realizar sus tratamientos con base en el principio de minimización. Lo cual significa que cualquier tratamiento de datos realizado por una administración pública, para ser lícito, debe ser adecuado, pertinente y ha de estar limitado, de manera estricta, al fin que se busque a través de dicho tratamiento.

Debe recordarse, como lo hace la AEPD, que la administración pública, al contrario de los particulares, está vinculada con el Derecho a través del principio de vinculación positiva. Es decir, para que la administración pueda actuar necesitará una previa habilitación del ordenamiento jurídico. Así, para poder realizar un tratamiento, la administración, habitualmente, se basará en el artículo 6.1.e) RGPD, y, por tanto, el interés público será la base legitimadora más frecuente (Campos, 2018, p. 99), aunque no la única, del tratamiento de datos por parte de una administración pública.

De esta manera, en todo tratamiento de datos que se realice, las administraciones públicas deberán prestar especial atención en justificar adecuadamente los fines en los que dicho tratamiento se base, y en evitar el uso de los datos para fines distintos.

En este sentido, una de las cuestiones que deberá realizar el órgano administrativo competente será el de informar a las personas interesadas de los fines del tratamiento, de manera que puedan conocer para qué se van a usar sus datos, y bajo qué justificación la administración necesita hacer uso de ellos, y, también, incorporarlos al registro de actividades de tratamiento. Esto debe ponerse en relación con el principio de transparencia, contenido en el artículo 12 RGDP (Campos, 2018, p.103), por lo que la información que se facilite a los administrados en relación con el tratamiento que se vaya a realizar, por escrito o por otros medios, de manera «*concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo*», especialmente cuando se dirija a menores de edad.

3.2. **El consentimiento**

Si bien en la mayoría de los casos, la base jurídica del tratamiento en el caso de administraciones públicas esté amparada en el cumplimiento de una norma de rango legal y en el interés público, también debe ponerse especial atención en el consentimiento que habrán de prestar las personas interesadas (Trujillo, 2017, p. 67).

El consentimiento tiene que ser informado, expreso, libre e inequívoco, y debe prestarse para el fin concreto del tratamiento. Siendo el derecho a la protección de datos una potestad de disposición de los particulares sobre todo dato personal cuyo uso o tratamiento pueda afectar al libre ejercicio de sus derechos y libertades básicas, como la privacidad o el derecho al honor y la propia imagen, el consentimiento, de acuerdo con las Sentencias del Tribunal Constitucional 254/1993 y 292/2000, forma parte del contenido esencial del derecho fundamental del artículo 18.4 CE, junto con el control sobre la información, los derechos de acceso, rectificación, cancelación, oposición, limitación, olvido y portabilidad, y el derecho a ser informado o informada (Plaza, 2017, p. 26).

El RGPD define el consentimiento en su artículo 4.11, como «*toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen*».

Esas características encuentran su plasmación en el artículo 7 RGPD, que regula las condiciones para el consentimiento y exige que la persona responsable deberá poder probar la existencia del mismo, lo cual obliga a recabar tal consentimiento a través de medios que dejen clara constancia de que se ha producido y en qué términos se ha producido.

Por otro lado, el consentimiento debe darse en relación con cada tratamiento de datos. El artículo 7.2 establece que, si el consentimiento se prestara por escrito para distintos tratamientos, deberá constar claramente cada uno de los tratamientos en qué va a consistir, cual es la finalidad, y su fundamento. Y deberá hacerse utilizando un lenguaje claro y sencillo, para que el consentimiento sea realmente informado.

Además, el consentimiento podrá retirarse en cualquier momento, sin que ello afecte a la licitud del tratamiento efectuada con base en el consentimiento previamente otorgado y posteriormente retirado.

3.3. **Facilitar el ejercicio de derechos**

Las administraciones públicas deben establecer medios visibles, sencillos y accesibles para que las personas puedan ejercer sus derechos, presentando especial atención a la verificación de la identidad de los particulares cuando se trate de procedimientos electrónicos. Eso conlleva, además, crear procedimientos ágiles, siguiendo los plazos que el Reglamento impone para el ejercicio de derechos.

A este respecto, resulta de plena aplicación a las administraciones públicas lo dispuesto por la AEPD en su Guía para Responsables de Protección de Datos[10], en relación con las obligaciones que los y responsables del tratamiento deben cumplir para garantizar el ejercicio de derechos por parte de la ciudadanía.

Las administraciones públicas deben emplear todos los medios a su alcance para facilitar a las personas interesadas el ejercicio de sus derechos relacionados con la protección de datos personales, y para ello habrán de adoptar las siguientes medidas, tal y como recomienda dicha Guía:

- Crear procedimientos de ejercicio de derechos que sean simples, accesibles, sencillos, y a los que se les dé plena transparencia, para que puedan conocerse con facilidad, a través de las sedes tanto electrónicas como físicas de las administraciones. Los procedimientos han de contemplar los medios para que las personas interesadas puedan acreditar que han ejercido sus derechos. Además, deberán ser gratuitos, de acuerdo con el principio de gratuidad del procedimiento administrativo[11].
- Activar plataformas telemáticas para posibilitar la presentación de los correspondientes escritos para el ejercicio del derecho a través de medios electrónicos, fundamentalmente cuando el tratamiento de datos se haya dado por estos medios.
- Articular procedimientos que permitan fácilmente que las personas interesadas puedan acreditar que han ejercido sus derechos por medios electrónicos (cuando sea viable técnicamente).
- Las administraciones públicas han de facilitar toda la información necesaria para que las personas interesadas puedan conocer las actuaciones que se hayan derivado de su solicitud en el plazo de un mes, y, si se tratara de supuestos especialmente complejos, en el plazo de dos meses.
- En caso de que la solicitud de la persona interesada resulte desestimada, habrá de notificarle la desestimación de manera motivada, en el plazo de un mes.
- Deberán implementarse medidas para verificar la identidad de quienes soliciten acceso y de quienes ejerzan los restantes derechos acceso, rectificación, cancelación, oposición, limitación, olvido y portabilidad.

3.4. **Adecuar los contratos públicos al RGPD y a la LOPDGDD**

Es importante, además, adecuar los contratos que se tengan suscritos a las previsiones del Reglamento y adaptar los pliegos al mismo.

A este respecto, la disposición adicional vigesimoquinta de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público (LCSP), si bien referenciada a la derogada Ley Orgánica 15/1999, establece la plena aplicación de la normativa en materia de protección de datos en el ámbito de la contratación pública.

Además, debe tenerse en cuenta que, según el artículo 28 RGPD, «*el tratamiento por el encargado se regirá por un contrato u otro acto jurídico*», y, por tanto, cuando el contratista, en ejercicio de la prestación objeto del contrato, deba realizar tratamiento de datos personales, ese tratamiento debe estar basado en un contrato o acto jurídico, especialmente cuando se trate de la gestión indirecta de un servicio público.

A este respecto, el pliego de cláusulas administrativas deberá contener una previsión específica sobre la sujeción al RGPD y a la LOPDGDD de todo tratamiento de datos que se realiza durante la ejecución del contrato, así como, en caso de que el objeto del contrato así lo exigiera, cualesquiera condiciones que fueran necesarias para tal tratamiento de datos (Mayor, 2019 y Díaz-Romeral, 2018).

Y más recientemente el Real Decreto Ley 14/2019, de 31 de octubre, ha modificado varios preceptos de la LCSP para enfatizar en la protección de datos de carácter personal.

3.5. **Realizar un análisis de los tratamientos de datos**

Debe realizarse un análisis de todos los tratamientos de datos que se desarrollen previendo los posibles

riesgos que pudieran entrañar para los derechos y libertades de los ciudadanos. Las medidas de cumplimiento dependen del nivel de riesgo de cada tratamiento.

El análisis debe dirigirse, fundamentalmente, a parámetros de la seguridad de la información. Se trata de una evaluación de riesgos que no va dirigida a analizar las amenazas que pudiera causar en la organización, sino que debe centrar el foco en la prevención de posibles vulneraciones los derechos y libertades de los ciudadanos y ciudadanas.

A este respecto, resulta de utilidad la Guía publicada por la AEPD para el análisis de riesgos[12].

El análisis, que debe orientarse a la visión de protección de los derechos y libertades de los ciudadanos, comprende tres fases: la identificación de riesgo, su evaluación y, finalmente, su tratamiento.

Así, debe protocolizarse un sistema que paute, desde su inicio, cómo va a tratarse cada una de las amenazas que puedan poner en riesgo una adecuada política de protección, y que articule qué respuesta se va a producir ante eventuales accesos ilegítimos a datos personales, modificaciones no autorizadas de los mismos o supuestos de eliminación de datos, que son los tres supuestos contemplados en el artículo 32.2 RGPD.

Una vez identificados cuales de estos tres tipos de riesgo pueden darse, ha de realizarse una valoración de las posibilidades de que sucedan y el impacto que puedan tener, viendo los posibles daños que pudieran generarse en los derechos y libertades de la ciudadanía, para posteriormente tratar dichos riesgos con el objetivo de disminuir los mismos o, al menos, los posibles daños que pudieran causar en caso de suceder.

Así, la gestión de la protección de datos debe realizarse desde el diseño, y teniendo en cuenta el artículo 25 RGPD, que, en su apartado 1 establece que los responsables del tratamiento deberán aplicar «*medidas técnicas y organizativas adecuadas*» como podría ser, en su caso, la disociación, para «*aplicar los principios de la protección de datos*», entre otros, la minimización, teniendo en cuenta el «*estado de la técnica, el coste y la naturaleza ámbito, contexto y los fines del tratamiento*».

Asimismo, el artículo 25.2 compele al responsable del tratamiento a aplicar las medidas necesarias, desde el punto de vista tanto técnico como organizativo con el objetivo de «*garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento*».

En desarrollo de lo anterior, el artículo 32.1 RGPD establece que deberán aplicarse medidas técnicas y organizativas adecuadas para evitar o reducir los riesgos, entre las que cita, a modo enunciativo, las siguientes:

— «La seudonimización y el cifrado de datos personales.
— La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
— La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico.
— Un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento».

Todo ello, como se ha señalado ha de quedar debidamente sistematizado en un protocolo de gestión de datos, que parta de la identificación, gestión y tratamiento de riesgos.

3.6. **Revisión de las medidas de seguridad**

Como consecuencia del análisis de riesgos, deben revisarse las medidas de seguridad que tienen que estar determinadas según las características de los tratamientos, sus riesgos, el contexto en que se desarrollan, las posibilidades técnicas y los costes que entrañen. Pero, fundamentalmente han de ser una consecuencia del análisis de riesgos y deberán adecuarse al Esquema Nacional de Seguridad (ENS).

El ENS parte de la idea de que en la seguridad informática no operan únicamente componentes tecnológicos, sino que también afecta a conductas personales. Basándose en esto, el ENS es un protocolo de ciberseguridad que unifica criterios y medidas, y afecta a todo el sector público (Amutio, 2018, p. 97).

El ENS se contempló en la ya derogada Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, y quedó regulado 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. También la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, tiene en cuenta el Esquema Nacional de Seguridad en su artículo 156.2. Finalmente, se ha producido una modificación del ENS a través del Real Decreto 951/2015, de 23 de octubre, de modificación 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.

Este instrumento trata de garantizar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, en las informaciones y servicios tratados por las administraciones públicas, y por lo ciudadanos ante éstas, a través de medios electrónicos. Todo ello para generar la confianza para que el uso de medios electrónicos por parte de las administraciones públicas y los ciudadanos se haga en términos de seguridad y garantía de los derechos y libertades de éstos últimos.

Para ello se homogeneizan los sistemas, las terminologías y las medidas a aplicar por todas las entidades del sector público.

Tal y como ha establecido el Centro de Transferencia de Tecnología[13], para su adaptación, las administraciones públicas deben:

- Elaborar y aprobar la política de seguridad, que ha de distribuir los roles y las responsabilidades de cada órgano.
- Categorizar los sistemas teniendo en cuenta qué información se maneja y qué servicios se prestan.
- Realizar el análisis de riesgos, teniendo en cuenta la evaluación de las medidas de seguridad ya existentes.
- Elaborar y aprobar la Declaración de aplicabilidad de las medidas del Anexo II del ENS.
- Partiendo de los problemas detectados, debe elaborarse un plan de adecuación para la mejora de la seguridad.
- Las medidas de seguridad deben ser implantadas, operadas y monitorizadas llevando a efecto una gestión continuada de la seguridad.
- Auditar la seguridad.
- Informar sobre el estado de la seguridad.

Para ello, el ENS consta de 75 medidas, que se dividen en diferentes estadios: el marco organizativo, el marco operativo y el marco de protección.

3.7. **Registro de las actividades de tratamiento**

Ha de establecerse un registro de actividades de tratamiento, que hay que mantener actualizado y siempre a disposición de las autoridades de control competentes en materia de protección de datos, tal y como contempla el artículo 30.1 RGPD. Debe tenerse en cuenta que el artículo 6 bis de la Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno, que fue introducido por la disposición final undécima de la LOPDGDD, obliga a las administraciones públicas a publicar el registro de actividades de tratamiento, haciéndolo accesible por medios electrónicos.

El mismo artículo establece qué contenido ha de tener el registro:

- El nombre y los datos de contacto de la persona responsable y, en su caso, del corresponsable, del representante del responsable, y de la persona delegada de protección de datos.
- Los fines del tratamiento.
- Una descripción de las categorías de interesados e interesadas y de las categorías de datos personales.
- Las categorías de personas destinatarias a quienes se comunicaron o comunicarán los datos personales, incluidas las que se encuentren en terceros países u organizaciones internacionales.
- En su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas.
- Cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos.
- Cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 32, apartado 1.

El registro de actividades de tratamiento es un elemento esencial para el cumplimiento de principio de responsabilidad proactiva, puesto que va a ser el instrumento que va a permitir poder demostrar en cada momento el cumplimiento efectivo de los principios del RGPD (Sanz, 2018:251).

3.8. **Identificación eficaz de las violaciones de seguridad**

Tienen que establecerse protocolos para poder identificar con premura las violaciones de seguridad de los datos, y una escala de actuación, según la gravedad y afección de esas violaciones de seguridad, para poder reaccionar con celeridad.

Tendrá que basarse en el riesgo que cada nivel de vulneración entrañe para los derechos y deberes de

Núm. 18 zk./2020. Págs. 138-153 or.
ISSN: 2173-6405 e-ISSN: 2531-2103

las personas afectadas. Además, aquellas vulneraciones que alcancen cierto grado de gravedad (es decir, que llegue a la categoría de «incidente de seguridad») han de ser puestas en conocimiento de las Autoridades competentes en materia de protección de datos. Todo esto debe recogerse en un registro de incidentes de seguridad, se haya o no notificado a la Autoridad competente.

3.9. Evaluación de impacto de los tratamientos de datos

Por otro lado, habrá de valorarse si los tratamientos que se realizan deben someterse a una Evaluación de Impacto, en virtud del riesgo que puedan entrañar para los derechos y libertades de los afectados, y especialmente cuando el tratamiento se realice por medios tecnológicos. En concreto, el artículo 35 RGPD, requiere la realización de la evaluación en impacto en los siguientes casos:

— Cuando se trate de una «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».
— En casos de «tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10».
— En supuestos de «observación sistemática a gran escala de una zona de acceso público».

3.10. Transferencias internacionales de datos[14]

En el caso de que se realicen transferencias internacionales de datos personales, estas deben adaptarse a las previsiones del Reglamento. Con las nuevas formas de trabajo «en la nube», las transferencias internacionales de datos cobran relevancia, dado que, en ocasiones, al depositar cierta información a través de este sistema, pueden estar transfiriéndose datos personales a terceros países.

Es fundamental establecer un programa de cumplimiento, o una política de protección de datos, que tiene que ir unida a una política de seguridad informática, que aborde todas estas cuestiones, y que se base en el Esquema Nacional de Seguridad.

4. Cambios en la organización: algunas notas sobre la figura del delegado o delegada de protección de datos

La correcta implementación de las acciones y políticas que se derivan del nuevo paradigma exige, además, introducir cambios en la organización de las administraciones públicas.

El cambio fundamental, y obligatorio en el caso de las administraciones públicas, consiste en el nombramiento de un Delegado o Delegada de Protección de Datos (DPD), que puede ser parte de la Entidad, pero que ha de desempeñar su función con independencia. Por lo que no podrá recibir instrucciones de los superiores jerárquicos. Deberá tener la formación y cualificación adecuadas, y podrá estar certificado como DPD[15].

Las funciones del DPD son las de informar y asesorar al responsable y encargado (actividad documentada); supervisar la puesta en práctica de las políticas de protección de datos, información y auditorías; supervisar la aplicación del Reglamento; asesorar en la evaluación de impacto; así como cooperar y actuar como punto de contacto con la autoridad de control (art. 39 RGPD).

Y para su cumplimiento se exige que la persona que asuma esas funciones tenga conocimientos tanto jurídicos como prácticos en materia de protección de datos (artículo 37.5 RGPD), incluso pudiéndose exigir certificación de tales conocimientos (art. 35 LOPDGDD).

Con todo, el DPD es una figura que, si bien se inserta en la organización, al ser su papel controlar que ésta cumple con los principios del RGPD, requiere un estatus que le garantice actuar con independencia de la entidad en la que desempeña sus funciones (Jiménez, 2018b: 12).

La designación del DPD no está exenta de complejidad ya que, para su integración en la organización administrativa, caben diferentes posibilidades.

El artículo 37 RGPD prevé tres posibilidades: que el DPD sea parte de la plantilla, o realice su función a través de un contrato de servicios; que exista un mismo delegado o delegada para varios organismos, siempre en virtud del tamaño y estructura de los mismos; que quien ejerce de DPD dentro de la organización o bien se dedique exclusivamente a esas funciones, o

bien las realice de manera simultánea con otras, siempre que estas últimas no afecten a su independencia o generen un conflicto de intereses dentro de la organización (Balín, 2018: 97).

En el caso en que el DPD se provea a través de un contrato de servicios, habrá que estar a lo regulado en el derecho de contratos públicos y, en particular a los dispuesto en la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público (LCSP), así como en la legislación autonómica, en el caso de aquellas CCAA que tengan competencia sobre la materia, como es el caso de Navarra, con la Ley Foral 2/2018, de 13 de abril, de contratos públicos.

En caso de que se determine que el DPD ha de ser parte de la organización, surgen varias cuestiones. En primer lugar, surge la cuestión sobre si el DPD ha se ser una sola persona o pueden existir varios dentro de una misma organización.

Esta es una cuestión que se plantea en organizaciones complejas con estructuras departamentales. Así, disponer de un DPD por cada departamento facilita el trabajo de control por parte de la persona que realice las funciones, así como la rendición de cuentas, permitiendo, además el conocimiento especializada de la protección de datos aplicado a la materia correspondiente a cada departamento. Sin embargo, en caso de contar con un solo DPD para toda la organización, se dificulta el control y la especialización en cuanto al ejercicio de sus funciones (Valín, 2018, p. 98).

En todo caso, ha de considerarse que, además de la doble especialización (en relación con la protección de datos, y en relación con la materia general de la que se ocupe la organización), las funciones del DPD requieren una interlocución fluida con los responsables del tratamiento de su organización, con la Autoridad en materia de protección de datos y con las personas interesadas, por lo que, en estructuras departamentales, la existencia de varios DPD, posibilita en mayor medida esa accesibilidad y la labor del mismo como cauce para el ejercicio de derechos (Jiménez, 2018b, p. 13)[16].

Además de lo anterior, surgen otras consideraciones en torno a cómo debe insertarse esta figura en la organización. Si se crea un órgano administrativo que se encargue de ejercer las funciones del DPD o si las mismas son asumidas por una persona física.

El primero de los supuestos hay que contemplarlo con cautela, ya que el RGPD en sus artículos 37-39, en todo momento se refieren al DPD como el *delegado* por lo que parece estar pensando en una persona física que en un órgano colegiado. No obstante, no existe una prohibición expresa de que las funciones de DPD se asuman colegiadamente (Valín, 2018, p. 98).

En el caso de que el DPD sea una persona física, de la propia organización, caben dos posibilidades: que se trate de un nuevo puesto creado en la plantilla de la entidad, o que a un puesto ya existente se le atribuyan las funciones propias del DPD. En el primer caso, además, se plantea el problema de la forma de provisión de esa plaza, que podría ser cubierta por un sistema de libre designación, o cubrirse mediante una oposición o concurso-oposición, o podría recurrirse al concurso de méritos entre personal funcionario.

Con todo, lo relevante es, tanto en cómo se integra el DPD en la organización, como en su forma de provisión, que se garanticen las características del puesto, que requiere salvaguardar su independencia como órgano de garantía en el ejercicio de derechos y pieza clave en el sistema de control interno.

En todo caso, debe destacarse que el DPD no es el responsable de la política de protección de datos. Quien asume la responsabilidad será la persona Responsable del tratamiento, es decir, la administración pública, y el DPD va a ser una figura clave para el cumplimiento de los principios de protección de datos y para el ejercicio de derechos por parte de los particulares. Aunque la aplicación de la política de protección de datos debe realizarse por todas las personas y órganos que forman parte de la administración.

Con todo, es preciso ahondar más aún en el marco de protección de la normativa de protección de datos, y fijar de manera concisa cuales han de ser las consecuencias del incumplimiento de ésta en materias como la privacidad, el principio de minimización, la evaluación de impacto y análisis de riesgo y las medidas de seguridad en los tratamientos de información[17].

5. Conclusiones

El RGPD ha introducido un nuevo paradigma en la protección de datos personales, la responsabilidad proactiva, un concepto difuso, pero no por ello menos obligado de cumplimiento, lo que exige a las administraciones públicas implementar importantes cambios tanto de visión como de organización.

Núm. 18 zk./2020. Págs. 138-153 or.
ISSN: 2173-6405 e-ISSN: 2531-2103

Ya no pueden limitarse al simple cumplimiento legal, sino que se han convertido, por obra del RGPD, en garantes de los derechos de los de los ciudadanos y ciudadanas. Para ello deben poner en marcha un sistema de cumplimiento orientado a la prevención. La prevención exige la adopción de instrumentos que aseguren la protección de datos por defecto, de modo que los procedimientos administrativos y los archivos públicos (electrónicos o no) deben incorporar garantías que se cumplan en el día a día de la actividad administrativa. Esta esencial tarea preventiva requiere la elaboración previa de una evaluación de impacto de todas las actividades de tratamiento de datos.

El principio de responsabilidad proactiva requiere un diseño previo de cómo ha de ser esa «hoja de ruta» de la protección de datos en el seno de cada organización pública. Y todo eso debe contemplarse en el registro de actividades de tratamiento e incorporarse a todo el catálogo de procedimientos administrativos que desarrolle la administración pública de que se trate.

También se extiende a la necesidad de operar cambios a nivel organizativo, de todo tipo. Uno de ellos es la incorporación del DPD, a quien debe garantizársele independencia para poder cumplir sus funciones como instrumento de control interno, además de interlocución con la Autoridad en materia de protección de datos y de órgano de garantía en el ejercicio de derechos por parte de los administrados y administradas.

El principio de responsabilidad proactiva exige que todas las personas que trabajan en la organización estén implicadas, no es una tarea sólo de quienes ostentan responsabilidades políticas o del personal directivo, sino de todo el personal del Sector Público. Para ello, éstos deberán ser debidamente formados y sensibilizados con la importancia que la política de protección de datos y de seguridad informática ha adquirido en la gestión pública. Por eso, las administraciones deberán establecer un plan de formación continua sobre esta materia que garantice al personal adquirir los conocimientos necesarios, en virtud del grado de responsabilidad que, por las funciones que desempeñan, adquieran en el tratamiento de datos personales.

La proactividad significa poder acreditar en todo momento que se está cumpliendo con la política de seguridad y protección de datos. Por eso, la política de protección de datos debe estar sometida a un plan de mejora continua. En consecuencia, han de articularse medios de auditoría interna y externa que permitan garantizar que en cada administración pública se está cumpliendo adecuadamente con el RGPD y el ENS.

6. Referencias

Alamillo Domingo, I. (2019). Esquema nacional de seguridad. La Administración electrónica y la seguridad de la información. En Campos Acuña, M.C. (dir.), *Aplicación práctica y adaptación de la protección de datos en el ámbito local: novedades tras el RGPD y la LOPDGDD* (pp. 607-639). Las Rozas (Madrid): Wolters Kluwer.

Amutio Gómez, M.A. (2018). El Esquema Nacional de Seguridad, al servicio de la ciberseguridad del Sector Público. *Economía Industrial*, n.º 410, 97-109.

Azurmendi López, A. (2015). Por un derecho al olvido para los europeos: aportaciones jurisprudenciales de la sentencia del Tribunal de Justicia europeo del caso Google Spain y su recepción por la sentencia de la Audiencia Nacional de 29 de diciembre de 2014. UNED. *Revista de Derecho Político*, n.º 92, enero-abril, 273-310.

Barrio Andrés, M. (2018). *Ciberderecho. Bases estructurales, modelos de regulación e instituciones de gobernanza de Internet*. Valencia: Tirant lo Blanch.

Bauman, Z. (2017). *Modernidad líquida*. Madrid: Fondo de Cultura Económica.

Boix Palop, A. (2015). El equilibrio entre los derechos del artículo 18 de la Constitución, el Derecho al Olvido y las libertades informativas tras la Sentencia Google. *Revista General de Derecho Administrativo*, n.º 38.

Buisán García, N. (2014). El derecho al olvido: el nuevo contenido de un derecho antiguo. *El Cronista de Estado Social y Democrático de Derecho*, n.º 46, 22-35.

Campos Acuña, C. (2018). Finalidades y bases jurídicas de los tratamientos de datos por parte de las Entidades Locales. En Campos Acuña, C. (dir.), *Aplicación práctica y adaptación a la protección de datos en el ámbito local. Novedades tras el Reglamento europeo* (pp. 85-115). Las Rozas: Wolters Kluwer.

Cotino Hueso, L. (2015). El conflicto entre las libertades de expresión e información en internet y el derecho a la protección de datos. Un falso derecho a juzgar por un falso tribunal. En Bel Mallén, J.I. y Corredoira y Alfonso, L. (dirs.), *Derecho de la información: el ejercicio del derecho a la información y su jurisprudencia* (pp. 387-430). Madrid: Centro de Estudios Políticos y Constitucionales.

Cotino Hueso, L. (2019). Riesgos e impactos del Big Data, la inteligencia artificial y la robótica. Enfoques, modelos y principios de la respuesta del Derecho. *Revista General de Derecho Administrativo*, n.º 50, 15-18.

Del Fresno García, M. (2014). Internet como macromedio: la cohabitación entre los medios sociales y medios profesionales. *Revista de Pensamiento sobre Comunicación, Tecnología y Sociedad*, n.º 99, 107-110.

Díaz-Romeral Gómez, A. (2018). Protección de datos y contratación pública. En I. Gallego Corcoles, y E. Gamero

Casado (dirs.), *Tratado de Contratos del Sector Público* (pp. 422-466). Valencia: Tirant lo Blanch.

García Mahamut, R. (2018). El derecho fundamental a la protección de datos: El Reglamento (UE) 2016/679 como elemento definidor del contenido esencial del artículo 18.4 de la Constitución. *Anuario de Derecho Parlamentario*, núm. Extra 31, 59-80.

Garriga Domínguez, A. (2016). *Nuevos retos para la protección de datos personales en la era del Big Data y de la computación ubicua*. Madrid: Dykinson.

Glavey, F. (2000). Accountability, the Right to Privacy and Third Pillar Arrangements. En Regan, E. (ed.), *The new Third Pillar. Cooperation against crime in the European Union* (pp. 134 y ss). Dublín: Institute of European Affairs.

Gudín Martínez-Magariños, F. (2018). *Nuevo Reglamento europeo de Protección de Datos versus Big Data*. Valencia: Tirant lo Blanch.

Han, B. (2014). *Psicopolítica,* Barcelona: Herder.

Jiménez Asensio, R. (2018a). *La aplicación del Reglamento (UE) de Protección de Datos Personales en la Administración Pública: especial referencia a los entes locales*. Oñati: Instituto Vasco de Administración Pública.

Jiménez Asensio, R. (20 de marzo de 2018b). La figura del delegado de protección de datos en las organizaciones públicas. [Entrada blog]. Recuperado de https://rafaeljimenezasensio.com/2018/03/

Jiménez Asensio, R. (2019). *Introducción al nuevo marco normativo de la protección de datos personales en el sector público*. Oñati: Instituto Vasco de Administración Pública.

Lattanzi, R. (2015). Diritto alla protezione dei dati di carattere personale: appunti di un viaggio non ancora concluso. En Rallo Lombarte, A. y García Mahamut, R. (eds.), *Hacia un nuevo derecho europeo de protección de datos* (pp. 103-142). Valencia: Tirant lo Blanch.

Lubián Rueda, M.A. (2018). Transferencia internacional de datos y su impacto en la administración local. En Campos Acuña, C. (dir.), *Aplicación práctica y adaptación a la protección de datos en el ámbito local. Novedades tras el Reglamento europeo*, (pp. 203-231). Las Rozas: Wolters Kluwer.

Martínez Velencoso, L. M. y Sancho López, M. (2018). El nuevo concepto de onerosidad en el mercado digital. ¿Realmente es gratis la App?. *InDret, Revista para el análisis del Derecho*, n.º 1/2018.

Mayor Gómez, R. (2019). La protección de datos personales en la Ley 9/2017, de 8 de noviembre, de Contratos del sector público. *Gabilex: Revista del Gabinete Jurídico de Castilla-La Mancha,* n.º extra 2/2019, 673-688.

Murga Fernández, J.P. (2017). La protección de datos y los motores de búsqueda en internet: cuestiones actuales y perspectivas de futuro acerca del derecho al olvido. *Revista de Derecho Civil*, n.º 4, 181-209.

Navas Navarro, S. (2017). Datos personales y mercado. En Navas Navarro, S. (dir.), *Inteligencia artificial, tecnología, Derecho* (pp. 259-272). Valencia: Tirant lo Blanch.

Nogueira Blanco, J. (2018). Reglamento General de Protección de Datos (RGPD) y BIG DATA. *Actualidad Civil,* Wolters Kluwer n.º 5.

Plaza Penadés, J. (2017). El nuevo modelo de protección de datos personales europeo y el modo de obtener un consentimiento lícito. *Revista Aranzadi de Derecho y Nuevas Tecnologías*, n.º 44.

Puyol Montero F.J.(2016). Los principios del derecho a la protección de datos. En Álvarez Caro, M., Recio Gayo, M. (Coords.) y Piñar Mañas, J.L. (dir.), *Reglamento general de protección de datos hacia un nuevo modelo europeo de privacidad*, (pp 135-150). Madrid: Reus.

Rallo Lombarte, A. (2014). *El derecho al olvido en internet. Google versus España*. Madrid: Centro de Estudios Políticos y Constitucionales.

Rallo Lombarte, A. (2017). De la «libertad informática» a la constitucionalización de nuevos derechos digitales (1978-2018). UNED. *Revista de Derecho Político*, n.º 100, 639-669.

Razquin Lizarraga, M.M. (2019). El necesario equilibrio entre transparencia y protección de datos personales. En Zegarra Valdivia, D. (coord.), *La proyección del Derecho Administrativo peruano. Estudios por el Centenario de la Facultad de Derecho de la PUCP* (pp. 137-162). Lima: Palestra.

Romeo Ruiz, A. (2019). El derecho al olvido en las administraciones públicas. *Revista Española de Derecho Administrativo,* n.º 198, 215-242.

Sancho López, M. (2019). Estrategias legales para garantizar los derechos fundamentales frente a los desafíos del Big Data. *Revista General de Derecho Administrativo*, n.º 50.

Sanz Marco, L. (2018). Medidas organizativas para la implantación del marco legal de protección de datos personales. El registro de actividades de tratamiento. En Campos Acuña, C. (dir.), *Aplicación práctica y adaptación a la protección de datos en el ámbito local. Novedades tras el Reglamento europeo* (pp. 321-341). Las Rozas: Wolters Kluwer.

Troncoso Reigada, A. (2010). *La protección de datos personales. En busca del equilibrio*. Valencia: Tirant lo Blanch.

Troncoso Reigada, A. (2012). Hacia un nuevo marco jurídico europeo de la protección de datos personales. *Revista Española de Derecho Europeo*, núm. 43, 35-36.

Trujillo Cabrera, C. (2017). Aproximación a la regulación del consentimiento en el Reglamento General de Protección de Datos. *Anales de la Facultad de Derecho*. Universidad de la Laguna, n.º 34, 67-75.

Valín López, M. (2018). Apuntes sobre el delegado de protección de datos y la Administración General de Euskadi. *Revista Vasca de Gestión de Personas y Organizaciones Públicas,* n.º 14, 92-105.

Notas

1 En 2019 había en España 25 millones de cuentas de Facebook frente a los 20 millones de 2014, 4´9 millones de cuentas en twitter, en relación con los 3'5 millones que en 2014 tenía esta red y 15 millones de cuentas en Instagram en contraste con los 7'4 millones de 2015. THE SOCIAL MEDIA FAMILY, *Informe de los perfiles de Redes Sociales en España en 2019. https://thesocialmediafamily.com/informe-redes-sociales/#Titulares_destacados_Informe_2019.*

2 Sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014 (asunto C-131/12), caso Google Spain vs. Agencia Española de Protección de Datos y Mario Costeja. Al respecto puede consultarse abundante bibliografía como la que a continuación se relaciona. Azurmendi López, A (2015). «Por un derecho al olvido para los europeos: aportaciones jurisprudenciales de la sentencia del Tribunal de Justicia europeo del caso Google Spain y su recepción por la sentencia de la Audiencia Nacional de 29 de diciembre de 2014», *UNED. Revista de Derecho Político,* nº 92, enero-abril, 273-310; Boix Palop, A. (2015). «El equilibrio entre los derechos del artículo 18 de la Constitución, el Derecho al Olvido y las libertades informativas tras la Sentencia Google», *Revista General de Derecho Administrativo*, nº 38*;* Buisán García, N. (2014). «El derecho al olvido: el nuevo contenido de un derecho antiguo», *El Cronista de Estado Social y Democrático de Derecho,* nº 46, 22-35; Murga Fernández, J.P. (2017). «La protección de datos y los motores de búsqueda en internet: cuestiones actuales y perspectivas de futuro acerca del derecho al olvido», en *Revista de Derecho Civil,* nº 4, 181-209; Cotino Hueso, L. (2015). «El conflicto entre las libertades de expresión e información en internet y el derecho a la protección de datos. Un falso derecho a juzgar por un falso tribunal», en J.I. Bel Mallén, y L. Corredoira y Alfonso, (Dirs.), *Derecho de la información: el ejercicio del derecho a la información y su jurisprudencia,* (pp 387-430). Madrid: Centro de Estudios Políticos y Constitucionales; Rallo Lombarte, A. (2014). *El derecho al olvido en internet. Google versus España,* Madrid: Centro de Estudios Políticos y Constitucionales. Romeo Ruiz, A. (2019). «El derecho al olvido en las administraciones públicas», *Revista Española de Derecho Administrativo,* nº 198, 215-242.

3 Debe reseñarse que, en el caso de tratamientos de datos realizados por administraciones públicas el consentimiento no va a estar entre las bases jurídicas legitimadoras del tratamiento más habituales, sino, que, más bien, constituye una base residual.

4 Además del artículo 5.2 RGPD que prescribe que «*El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo*», el Considerando 74 del Reglamento establece lo siguiente: «*Debe quedar establecida la responsabilidad del responsable del tratamiento por cualquier tratamiento de datos personales realizado por él mismo o por su cuenta. En particular, el responsable debe estar obligado a aplicar medidas oportunas y eficaces y ha de poder demostrar la conformidad de las actividades de tratamiento con el presente Reglamento, incluida la eficacia de las medidas*».

5 Sobre la aplicación del Esquema Nacional de Seguridad en las administraciones públicas y, más en concreto, en la administración local, véase, Alamillo Domingo, I. (2019). «Esquema nacional de seguridad. La Administración electrónica y la seguridad de la información», en M.C. Campos Acuña (dir.), *Aplicación práctica y adaptación de la protección de datos en el ámbito local: novedades tras el RGPD y la LOPDGDD,* (pp. 607-639). Las Rozas (Madrid): Wolters Kluwer.

6 Agencia Española de Protección de Datos, sobre el Principio de Responsabilidad Proactiva, véase la siguiente web: https://www.aepd.es/reglamento/cumplimiento/principio-responsabilidad-proactiva.html.

7 Agencia Española de Protección de Datos (2019), *Medidas de cumplimiento,* documento electrónico, accesible en la siguiente dirección: https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento

8 Agencia Española de Protección de Datos. *Informe sobre el impacto del Reglamento General de Protección de Datos sobre la actividad de las administraciones públicas*.

9 La AVPD, en su *Guía en ocho pasos* ha identificado las siguientes actuaciones a realizar: «*1. Designar un Delegado de Protección de Datos (DPD). 2. Establecer el Registro Interno de Tratamientos. 3. Revisar la legitimación de los tratamientos. 4. Revisar la información que se ofrece a los interesados. 5. Revisar los procedimientos de ejercicio de derechos. 6. Revisar los contratos con Encargados de Tratamiento. 7. Efectuar Análisis de Riesgos y revisar las medidas de seguridad. 8. Determinar la necesidad de efectuar Evaluaciones de Impacto*» Agencia Vasca de Protección de Datos, *Guía en ocho pasos. Adecuación de las administraciones públicas al Reglamento General de Protección de Datos»,* Vitoria-Gasteiz, 2018. Puede accederse al documento a través del siguiente enlace: https://www.avpd.euskadi.eus/contenidos/informacion/publicaciones_avpd/es_def/adjuntos/rgpd_admonpubl_gida_2018_v01-es.pdf

10 AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, *Guía del Reglamento General de Protección de Datos para responsables del tratamiento.* Disponible en web: https://www.aepd.es/media/guias/guia-rgpd-para-responsables-de-tratamiento.pdf.

11 La AEPD admite la posibilidad del cobro de un canon que compense los gastos de gestión en los casos en los que las peticiones sean «manifiestamente infundadas o excesivas, fundamentalmente por repetitivas». Si bien, en este caso, corresponde al responsable del tratamiento acreditar que la solicitud se ajusta a tales características. AGENCIA ESPAÑOLA DE PROTECCIÓN DE

DATOS, *Guía del Reglamento General de Protección de Datos para responsables del tratamiento,* pág. 8.

12 Agencia Española de Protección de Datos, *Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD.* Disponible en web: https://www.aepd.es/media/guias/guia-analisis-de-riesgos-rgpd.pdf

13 Centro de Transferencia de Tecnología, *Esquema Nacional de Seguridad*. Disponible en web: https://administracionelectronica.gob.es/ctt/ens#.XPjrg9NKigR

14 Un análisis detallado en relación con las Transferencias Internacionales de Datos puede encontrarse en Lubián Rueda, M.A. (2018). «Transferencia internacional de datos y su impacto en la administración local», en M.C. Campos Acuña (dir.), *Aplicación práctica y adaptación a la protección de datos en el ámbito local. Novedades tras el Reglamento europeo,* (pp 203-231). Las Rozas: Wolters Kluwer.

15 Sobre el DPD en el ámbito del sector público resulta imprescindible la lectura de Jiménez Asensio, R. (2018b). «La figura del delegado de protección de datos en las organizaciones públicas», ponencia presentada en el Seminario de Actualización de Función Pública organizado por la Federació de Municipis de Catalunya, el día 20 de marzo de 2018, y publicado en el blog del auto. Documento electrónico accesible en el siguiente enlace: https://rafaeljimenezasensio.files.wordpress.com/2018/03/articulo-dpd-4.pdf

16 A pesar de esto, el sistema que se ha seguido en la Administración General de Euskadi es el del nombramiento de una sólo Delegada de Protección de Datos para toda la organización, nombrada a través del DECRETO 83/2018, de 29 de mayo, por el que se nombra Delegada de Protección de Datos de la Administración Pública de la Comunidad Autónoma de Euskadi. En Navarra, el Decreto Foral 20/2019, de 6 de marzo, por el que se aprueba la política de protección de datos y seguridad de la información de la Administración de la Comunidad Foral de Navarra y sus Organismos Públicos, deja abiertas ambas opciones pues, si bien establece que la Administración de la Comunidad Foral de Navarra y sus Organismos Públicos «*cuentan con una delegada de protección de datos de ámbito general*», a continuación añade *«sin perjuicio del posible nombramiento de otras delegadas u otros delegados de protección de datos en ámbitos inferiores, como Departamentos u organismos públicos cuando sus necesidades específicas así lo requieran»* (art. 12), si bien el Decreto Foral 37/2018, de 16 de mayo, por el que se modifica el Decreto Foral 198/2015, de 9 de septiembre, por el que se establece la estructura orgánica del Departamento de Presidencia, Función Pública, Interior y Justicia, creó la figura de una única Delegada de Protección de Datos para el conjunto de la Administración de la Comunidad Foral de Navarra. Esto último llama la atención cuando el artículo 8 del Decreto Foral 20/2019, de 6 de marzo, por el que se aprueba la política de protección de datos y seguridad de la información de la administración de la Comunidad Foral de Navarra y sus Organismos Públicos establece que «*La condición de responsable del tratamiento recae en la Consejera o el Consejero de cada Departamento del Gobierno de Navarra o Gerente de cada organismo público, en los términos establecidos en el artículo 4.7 del RGPD*».

17 Así se ha establecido en el punto 6º de las líneas de trabajo propuestas en el documento de Conclusiones del I Seminario Internacional «Derecho Administrativo e Inteligencia Artificial», celebrado en la Facultad de Derecho de la Universidad de Castilla-la Mancha, el 1 de abril de 2019.

Núm. 18 zk./2020. Págs. 138-153 or.
ISSN: 2173-6405 e-ISSN: 2531-2103