Universidad Internacional de La Rioja
Facultad de Derecho

Máster Universitario en Derecho Digital

La eliminación y conservación de datos en las Administraciones Públicas por aplicación de la normativa de protección de datos.

Trabajo fin de estudio presentado por:	Beatriz Fernández Delgado
Tipo de trabajo:	Trabajo fin de máster
Utilizar si se necesita alguna tipología más:	
Director/a:	Victor Cazurro Barahona
Fecha:	19 de febrero de 2025

Resumen

Este trabajo aborda los retos que enfrentan las Administraciones Públicas en la gestión de la eliminación y conservación de datos personales, en un contexto normativo que combina la normativa de protección de datos con disposiciones específicas de archivos, transparencia y patrimonio documental. El objetivo principal es examinar cómo estas normativas impactan en la aplicación del derecho de supresión y el principio de limitación del plazo de conservación por parte del sector público, diferenciando su tratamiento respecto al sector privado.

La metodología se ha centrado, principalmente, en el análisis detallado de la normativa aplicable y las consideraciones que al respecto ha emitido la AEPD, y de casos prácticos para comprender cómo las Administraciones Públicas gestionan la conservación y eliminación de datos en un marco normativo complejo. Se concluye que, aunque la eliminación de datos en el sector público está mucho más restringida que en el sector privado debido a sus obligaciones legales específicas, pueden implementarse medidas como el derecho al olvido, el derecho de oposición o la digitalización, entre otros, para reforzar la protección de los derechos de los ciudadanos. Este trabajo subraya la importancia de adoptar soluciones que equilibren las necesidades de conservación documental con el respeto a la privacidad.

Palabras clave: Protección de datos, Administraciones Públicas, Supresión de datos, Conservación de datos, Conservación del patrimonio documental.

Abstract

This study addresses the challenges faced by Public Administrations in managing the deletion and retention of personal data within a regulatory framework that combines data protection regulations with specific provisions related to files, transparency, and documentary heritage. The primary objective is to examine how these regulations affect the application of the right to erasure and the principle of storage limitation in the public sector, highlighting the differences compared to the private sector.

The methodology primarily focused on a detailed analysis of the applicable regulations and the considerations issued by the Spanish Data Protection Agency (AEPD), as well as practical case studies to understand how Public Administrations handle data retention and deletion within a complex regulatory framework. The study concludes that, although data deletion in the public sector is significantly more restricted than in the private sector due to specific legal obligations, measures such as the right to be forgotten, the right to object, and digitalization, among others, can be implemented to strengthen the protection of citizens' rights. This research emphasizes the importance of adopting solutions that balance the need for documentary preservation respect for privacy.

Keywords: Data protection, Public Administrations, Data erasure, Data retention, Preservation of documentary heritage.

Índice de contenidos

Índice de figuras

1. Introducción.

1.1.Justificación del tema elegido.

La normativa en materia de protección de datos recoge, entre las obligaciones del responsable del tratamiento, la necesidad de tomar decisiones y gestionar la eliminación y conservación de los documentos que contienen datos personales. Esto se debe, fundamentalmente, al cumplimiento de determinados principios y responsabilidades contenidos en el RGPD, en concreto:

- Dar respuesta a los ejercicios de derechos de supresión ejercitados por los interesados, de acuerdo con el artículo 17 del RGPD, suprimiendo sin dilación indebida los datos personales cuando concurra alguna de las circunstancias previstas en la norma.
- Cumplir el principio de limitación del plazo de conservación, recogido en el artículo 5.1 letra e) del RGPD, que establece que los datos serán eliminados cuando han dejado de ser necesarios para los fines para los que fueron recabados, aunque podrán conservarse durante plazos más amplios si se cumplen determinadas circunstancias.

En ambos casos, la conservación y/o eliminación, se encuentra vinculada directamente a la finalidad para la cual los datos fueros recogidos y tratados, ya que, los datos deben recogerse con fines determinados, explícitos y legítimos, y no ser tratados posteriormente para fines incompatibles para los que fueron recabados.

En el ámbito de las Administraciones Públicas, estas obligaciones encuentran condicionantes específicos que las distinguen del sector privado. Entre estos se incluyen:

- ✓ Las causas de licitud habituales de las entidades públicas, muy diferentes del ámbito privado.
- ✓ El valor histórico y administrativo de los documentos públicos y la necesidad de conservación del patrimonio documental, así como la traza documental de la Administración Pública.
- ✓ Las obligaciones en materia de transparencia de las entidades públicas.

Dichos factores hacen que surjan especialidades que no existen en el sector privado, así como excepciones, limitaciones y problemas a la hora decidir sobre la eliminación o conservación de los documentos públicos que contienen datos de carácter personal.

Todo ello puede llevar a plantearse si realmente la normativa de protección de datos permite al ciudadano, en relación con las Administraciones Públicas, disponer del control sobre la supresión de sus datos o saber, con cierta exactitud, cuándo van a eliminarse por el responsable del tratamiento.

1.2. Problema y finalidad del trabajo.

En la actualidad, las solicitudes de ejercicio de derechos que llegan a los responsables del tratamiento han aumentado significativamente. Entre estas solicitudes, los derechos de oposición y supresión son los más frecuentemente ejercidos por los ciudadanos[1].

Las Administraciones Públicas no son ajenas a este fenómeno donde el ejercicio de derechos por parte de los ciudadanos es cada vez mayor, especialmente solicitando la supresión de datos y la retirada de contenidos publicados lícitamente en páginas web.

Esto sugiere una creciente preocupación de los ciudadanos por su privacidad, en particular, desean que sus datos sean eliminados de aquellos tratamientos que consideran innecesarios y, especialmente, que no sean fácilmente accesibles para cualquier internauta que busque su nombre en un buscador online.

En este contexto, en la mayoría de las ocasiones, una Administración Pública no podrá suprimir esos datos o incluso tendrá la obligación de hacerlos públicos a través de una página web por razones de transparencia.

Teniendo en cuenta la normativa vigente es posible preguntarse si, realmente, en el sector público, puede llevarse a cabo la supresión de datos derivada de la normativa de protección de datos y qué soluciones hay en estos casos para proteger la privacidad de los ciudadanos.

[1] Las resoluciones de la AEPD en materia de derechos son en su mayoría relativas a los derechos de supresión y oposición.

1.3. Objetivos.

Este trabajo tiene los siguientes objetivos:

- Analizar la normativa aplicable a la supresión de datos personales en el ámbito público, en especial el Reglamento General de Protección de Datos (RGPD) y la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD). Se estudiará tanto la supresión derivada de las solicitudes realizadas por los ciudadanos, como la asociada al cumplimiento del principio de limitación del plazo de conservación por parte de los responsables del tratamiento.
- Examinar la viabilidad de la supresión de datos personales en las Administraciones Públicas, identificando los condicionantes específicos derivados de normativas sectoriales relacionadas con transparencia, patrimonio documental e interés público, así como las problemáticas prácticas que dificultan su implementación.
- Evaluar las medidas técnicas y organizativas necesarias para garantizar la protección de los datos personales que deben conservarse, asegurando que los derechos y libertades de las personas físicas no se vean afectados por la *hiperaccesibilidad* o el uso indebido de los mismos. Esto incluye la implementación de soluciones como el derecho al olvido frente a motores de búsqueda.
- Explorar posibles soluciones integrales para armonizar el cumplimiento de la normativa en materia de protección de datos personales con las obligaciones legales específicas del sector público, incluyendo la creación de un marco normativo más coherente que permita equilibrar las necesidades de conservación documental con el derecho de supresión y la privacidad de los ciudadanos.
- Examinar si el marco normativo vigente en materia de protección de datos personales es suficiente y provee las herramientas necesarias para garantizar la adecuada implementación de la supresión de datos en el ámbito público, evaluando su efectividad en la práctica y su capacidad para adaptarse a los desafíos tecnológicos, organizativos y legales actuales.

2. La eliminación de los datos a solicitud del interesado.

Un primer motivo para la eliminación de los datos personales de un tratamiento por parte de su responsable, es el que surge como consecuencia de que un interesado ejerza su derecho de supresión.

El derecho de supresión es el derecho que tiene el interesado a exigir al responsable que excluya del tratamiento sus datos de carácter personal si se cumplen una serie de requisitos que posteriormente se analizarán.

La supresión podrá ejercerse respecto de todos los datos o solo de alguno de ellos. Por lo tanto, esto supondrá, o bien la extinción completa del tratamiento, o bien, el tratamiento continuará respecto de los datos que no se hayan suprimido.

Es un derecho que el interesado puede ejercer ante cualquier responsable del tratamiento, ya sea una entidad pública o privada, si bien, las Administraciones Públicas tienen una serie de particularidades en materia de protección de datos que harán que la gestión de este derecho sea diferente.

Estas particularidades serán estudiadas a lo largo de este epígrafe.

2.1. El derecho de supresión como derecho de los interesados.

El derecho de supresión se recoge en el artículo 17 del RGPD. El interesado tendrá derecho a obtener, sin dilación indebida del responsable del tratamiento, la supresión de los datos personales que le conciernan, que estará obligado a suprimir los mismos cuando concurran ciertas circunstancias, es decir, está delimitado en cuanto a su alcance, ya que solo podrá llevarse a cabo en los supuestos a que se refiere el apartado 1 de este mismo artículo y que más adelante se estudiarán.

Este derecho se encuadra dentro de los derechos de los interesados, que se regulan en el capítulo III del RGPD, tradicionalmente conocidos con el acrónimo ARCO (acceso, rectificación, cancelación y oposición), incorporando otros derechos más novedosos, algunos de reconocimiento jurisprudencial y otros que pretenden dar respuesta a la propagación de las nuevas tecnologías, como la inteligencia artificial, blockchain, internet of things (IoT) o big data entre otras.

En la actualidad, los derechos que se recogen en el RGPD son: acceso, rectificación, supresión, limitación del tratamiento, portabilidad, oposición y a no ser objeto de decisiones individuales automatizadas, y son conocidos con las siglas ARCO+, ARSOPOL, ARSULIPO, etc… aunque la denominación «derechos ARCO» nunca ha dejado de utilizarse.

Todos ellos se configuran como herramientas fundamentales para hacer efectivos los principios que rigen el tratamiento de datos de carácter personal y que están recogidos en el artículo 5 del RGPD.

Así, el derecho de acceso hace efectiva la transparencia; el de rectificación garantiza la calidad de la información; y los de supresión y oposición permiten la capacidad de control del interesado sobre sus datos personales.

El derecho de supresión de datos podrá ejercerse en las circunstancias previstas en el artículo 17.1 del RGPD. Este derecho es aplicable cuando los datos personales ya no son necesarios para los fines para los que fueron recabados o tratados, cuando el interesado retire su consentimiento y no exista otro fundamento jurídico para el tratamiento, cuando el interesado se oponga al tratamiento y no haya motivos legítimos para mantenerlo, cuando los datos hayan sido tratados de manera ilícita, cuando sea necesario cumplir con una obligación legal que exija su eliminación, o cuando los datos hayan sido obtenidos en relación con la oferta de servicios de la sociedad de la información.

No obstante, incluso cuando se dan estos supuestos, el derecho de supresión no siempre puede llevarse a cabo, ya que existen excepciones que fija el apartado 3 del mismo artículo 17 y que se analizarán con detenimiento en el apartado siguiente.

2.2. Excepciones y particularidades del derecho de supresión en entidades públicas.

2.2.1. Excepciones al derecho de supresión.

El derecho de supresión, además de estar delimitado respecto a su alcance, como se ha visto en el apartado anterior, solo podrá llevarse a cabo cuando no se aplique ninguna de las excepciones contempladas en el artículo 17.3 del RGPD.

En el considerando 65 del RGPD se establece que, si bien los interesados deben tener el derecho a la supresión de sus datos personales y a que estos dejen de ser tratados en

determinadas circunstancias, la conservación ulterior de los mismos es legítima siempre que se cumplan una serie de requisitos. Estos requisitos, definidos en el considerando, se desarrollan posteriormente en los artículos del Reglamento.

Aclara la AEPD, en su informe 00148/2019 de 9 de diciembre de 2020 que, en estos casos, la retención ulterior de dichos datos es lícita. Esto es, no concurriría un derecho del interesado a la supresión de los datos personales.

Estas excepciones persiguen diversas finalidades, siendo especialmente relevante el equilibrio entre el derecho de supresión y los intereses públicos legítimos. Según el tercer apartado del artículo 17 del RGPD, la supresión no procederá en los siguientes casos:

a) Cuando el tratamiento sea necesario para ejercer el derecho a la libertad de expresión e información.
b) Cuando sea necesario para el cumplimiento de una obligación legal, de acuerdo con la legislación de la Unión Europea o de los Estados miembros aplicable al responsable del tratamiento, o para llevar a cabo una misión en interés público o el ejercicio de poderes públicos asignados al responsable.
c) Cuando sea necesario por razones de interés público en el ámbito de la salud pública.
d) Cuando el tratamiento se realice con fines de archivo en interés público, investigación científica o histórica, o fines estadísticos.
e) Cuando sea necesario para la formulación, ejercicio o defensa de reclamaciones.

Entre estas excepciones interesa especialmente resaltar la del apartado b), y es que la supresión no se llevará a cabo cuando el tratamiento tenga determinadas causas de licitud.

Esto debe enlazarse con el artículo 6 del RGPD, que introduce uno de los principios más importantes en materia de datos de carácter personal, la «licitud del tratamiento». Este artículo establece que cualquier tratamiento que se lleve a cabo, deberá cumplir al menos una entre las 6 causas de legitimación que recoge: consentimiento, ejecución de un contrato, cumplimiento de una obligación legal, proteger intereses vitales del interesado, cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos o satisfacción de intereses legítimos.

De acuerdo el artículo 17.3 letra b) del RGPD, no podrá aplicarse el derecho de supresión a cualquier tratamiento cuya causa de licitud se base en el cumplimiento de una obligación legal o de una misión realizada en interés público.

2.2.2. Estudio de las causas de licitud del tratamiento de datos personales en la Administración Pública.

Para que los tratamientos de datos sean legítimos, es imprescindible que los fines perseguidos se identifiquen con una base jurídica adecuada. Según el artículo 6 del RGPD, el tratamiento de datos personales solo será lícito si se cumple al menos una de las siguientes condiciones:

a. Consentimiento del interesado.
b. Es necesario para la ejecución de un contrato.
c. Es necesario para cumplir una obligación legal.
d. Es necesario para proteger intereses vitales del interesado o de un tercero.
e. Es necesario por razones de interés público.
f. Es necesario para la satisfacción de intereses legítimos.

Las bases de licitud en el sector público presentan particularidades que no se encuentran en el ámbito privado. Por este motivo, resulta esencial analizar cada una de estas bases para determinar si tienen cabida en la Administración Pública y, de ser así, de qué manera se aplican en este contexto. Una de las principales diferencias entre ambos sectores radica en las causas de licitud que afectan a las Administraciones Públicas. Mientras que en el ámbito privado la licitud suele basarse principalmente en el consentimiento del interesado, la relación contractual o el interés legítimo, en el sector público, son comúnmente el ejercicio de competencias públicas, lo que condiciona de forma significativa la aplicación del derecho de supresión.

A continuación, se analizarán cada una de las causas de licitud mencionadas, detallando su aplicación específica en el sector público. Este análisis se fundamenta, entre otras fuentes, en las consideraciones de la Agencia Española de Protección de Datos recogidas en el Informe núm. 2018-0175 de 19 de noviembre de 2018, ampliación del Informe emitido en los expedientes 108/2018 (ref. 181577/2018) y 155/2018 (ref. 200012/2018).

2.2.2.1. Consentimiento del interesado.

El RGPD supone un cambio de perspectiva en relación con las causas de licitud, en concreto, en lo relativo al "principio de consentimiento" que, anteriormente, se articulaba como el eje central del derecho a la protección de datos.

Establece la AEPD en su informe núm. 022147/2019 de 20 de febrero de 2020 que, con el RGPD, se modifica sustancialmente este aspecto, ya que, con la LOPD del año 1999, el consentimiento era la regla básica para legitimar cualquier tratamiento, y con la regulación que surge a partir de 2016 el consentimiento es solo una de las 6 posibles causas de legitimación, sin que tenga mayor importancia que las demás.

No solo eso, sino que, además, en la Administración Pública se considera que no se da el requisito de libertad del interesado, haciendo del consentimiento una base legitimadora prácticamente residual, casi nula.

El considerando 43 del RGPD establece que para garantizar que el consentimiento sea libre, no puede existir un desequilibrio entre responsable de tratamiento e interesado, especialmente cuando el responsable es una autoridad pública y sea improbable que el consentimiento se haya dado libremente en todas las circunstancias debido a la situación particular.

En los mismos términos se pronuncia la propia Agencia Española de Protección de datos en su Informe núm. 2018-0175 de 19 de noviembre de 2018, ampliación del Informe emitido en los expedientes 108/2018 (ref. 181577/2018) y 155/2018 (ref. 200012/2018):

«Con carácter general, la base jurídica del tratamiento en las relaciones con la Administración, en aquellos supuestos en que existe una relación en la que no puede razonablemente predicarse que exista una situación de equilibrio entre el responsable del tratamiento (la Administración), y el interesado (el administrado) no sería el consentimiento (art. 6.1.a) RGPD), sino, según los casos, el cumplimiento de una obligación legal (art. 6.1.c) RGPD) o el cumplimiento de una misión de interés público o en el ejercicio de poderes públicos (art. 6.1.e) RGPD).»

Por otro lado, el considerando 42 del RGPD señala que el consentimiento no se considera válido si la persona interesada no tiene una verdadera o libre elección al otorgarlo, o si no puede retirarlo o denegarlo sin sufrir consecuencias negativas.

En base a ello, la Agencia, en el citado informe considera que el consentimiento no puede ser considerado un «fundamento jurídico válido» en la Administración, dado que, como requiere el RGPD, no se garantiza que se dé con libertad. Y el consentimiento debe ser libre, como establece el artículo 4.11 del RGPD.

La Agencia, para ejemplificar esta falta de libertad en el consentimiento hace referencia al tratamiento de datos para obtener el carnet de conducir, gestionado por la Dirección General de Tráfico. En este caso, no se puede considerar que el consentimiento otorgado por un interesado sea verdaderamente "libre" en el sentido que establece el RGPD. Si la persona decidiera retirar su consentimiento, y si este fuera la única base legal para el tratamiento de sus datos, se vería claramente afectada, ya que no existiría una alternativa viable a la obtención del carnet de conducir.

En conclusión, como norma general, no cabe considerar el consentimiento como base jurídica válida del tratamiento de datos en las Administraciones Públicas.

2.2.2.2. Ejecución de un contrato.

Conforme al considerando 44 del RGPD el tratamiento debe ser lícito cuando sea necesario en el contexto de un contrato o de la intención de concluir un contrato.

Es evidente que la Administración Pública puede contratar, si bien, esta potestad de contratación viene dada por una norma con rango de ley. Así lo establece la AEPD:

«Nadie discute que la Administración puede entrar en contratos, bien de derecho público o de derecho privado. En ambos casos dicha potestad de contratar ha de venir establecida por ley, en cuanto que regula la competencia y las facultades del órgano para contratar, pero nada impide que en estos casos el tratamiento pueda basarse en una base jurídica distinta, como es la del art. 6.1.b) RGPD, esto es, que el tratamiento sea necesario para la ejecución de un contrato, por cuanto el art. 6.1, primer inciso, establece que será suficiente para un tratamiento de datos lícito el que concurra al menos una (luego puede haber más de una) de las condiciones que el precepto regula.»

Por lo tanto, en aquellos supuestos en los que existe un tratamiento de datos público cuya licitud se base en un contrato, siempre habrá también como causa de legitimación del tratamiento una competencia pública, ya que la capacidad para contratar se la otorga una norma con rango de ley.

2.2.2.3. Obligación legal e interés público.

Estas dos causas de licitud, recogidas en las letras c y e del artículo 6.1 del RGPD son las que el artículo 17 del RGPD considera excepciones al derecho de supresión, y a la vez son, con carácter general, la causa de licitud habitual que utiliza la Administración Pública, tal y como dice la AEPD y se ha venido adelantando en puntos anteriores.

Establece además la AEPD, en el informe (núm. 2018-0175) al que venimos haciendo referencia, que se infringiría el "principio de minimización de datos" del artículo 5.1 letra c) del RGPD si un tratamiento de la Administración Pública no es "necesario" para el ejercicio de los poderes públicos conferidos por el ordenamiento, careciendo dicho tratamiento de base jurídica suficiente.

Recalca la Agencia la vinculación de la Administración Pública al principio de legalidad, conforme a los artículos 9.1 y 103.1 de la Constitución Española, sujeta a la Constitución y al resto del ordenamiento jurídico, con sometimiento pleno a la ley y al Derecho. Conforme a este principio, y a diferencia de los particulares, la Administración solo puede realizar aquellas actuaciones que el ordenamiento jurídico le permite. Es decir, la Administración solo puede actuar si una norma le da competencia para hacerlo, es lo que se conoce como vinculación positiva de la Administración: la Administración sólo podría realizar lo que la ley le permita (GARCÍA DE ENTERRÍA, 1994).

La Agencia Española de Protección de Datos señala que, para que la Administración pueda llevar a cabo cualquier actuación, debe contar con una habilitación legal previa, entendida esta como una autorización normativa. Esto se aplica tanto en el ámbito del derecho público como en el derecho privado. Así, incluso cuando la Administración actúa en el ámbito privado, similar a los particulares, requiere una norma que le permita intervenir. Un ejemplo de esto es el caso en el que el Estado actúa como heredero, según lo dispuesto en la Ley 33/2003, del Patrimonio de las Administraciones Públicas. Aunque el Estado ocupa la misma posición que otros herederos, la aceptación de la herencia está regulada por esta ley, estableciendo que

debe hacerse a beneficio de inventario. Los tratamientos de datos que la Administración necesite realizar en este contexto se basarían en el artículo 6.1.e) del RGPD, es decir, que el tratamiento debe ser necesario para cumplir con una misión de interés público. Esto se debe a que la Administración está sujeta a la ley y no puede actuar sin su amparo; por esta razón, toda su actuación, aunque sea en el ámbito privado, está orientada por el interés público.

La AEPD, tras analizar la situación, llega a la conclusión de que «cabe considerar, en principio, que, dado que la Administración ha de actuar siempre vinculada a la ley y al derecho, su actuación tanto en el campo del derecho público como del derecho privado vendría amparado por el concepto de "interés público" previsto en el art. 6.1.e) RGPD).»

Dentro de estas causas de legitimación pueden nombrarse dos leyes que atribuyen a la Administración obligaciones relativas a la conservación y publicación de datos por razones de trasparencia, estas normas son:

- Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español.
- Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.

Estas normas serán estudiadas con detenimiento más adelante. Si bien cabe dejar constancia de que, en ocasiones, la licitud del tratamiento vendrá dada por alguna de ellas, y ambas obligan a que los datos sean tratados de una determinada manera, haciendo que el ciudadano no pueda decidir sobre el destino de sus datos.

2.2.2.4. Proteger intereses vitales del interesado o de un tercero.

Estamos ante una causa de licitud excepcional, que se utiliza para casos muy concretos en los que se encuentra en juego la vida de una persona.

Únicamente podría acudirse a esta causa de licitud si no es posible salvar la vida de una persona sin realizar el tratamiento de datos, es decir, debe ser absolutamente necesario. Si fuese posible salvaguardar la vida del individuo de manera menos intrusiva, esta causa de legitimación no se aplicaría.

Es una causa de licitud limitada a cuestiones de vida o muerte, que encontraremos en un porcentaje muy pequeño de tratamientos, tanto en el ámbito público como privado.

Por ejemplo, en el caso de la Administración Pública se puede encontrar esta causa de licitud en hospitales públicos, para atender una urgencia que requiere acceder al historial clínico sin valorar si existen otras causas de licitud para ello.

También podríamos pensar en tratamientos masivos públicos de datos por cuestiones de salud. Esto se resuelve en el Dictamen 6/2014 del Grupo de Trabajo del Artículo 29, señalando que, en último término, existiría una obligación legal o una competencia Pública.:

«Esto también limitaría la aplicación de esta disposición a un análisis caso por caso y no puede normalmente utilizarse para legitimar cualquier recopilación o tratamiento masivos de datos personales. En caso de que esto resultara necesario, las letras c) o e) del artículo 7 serían motivos de legitimación más apropiados para el tratamiento».

En conclusión, el tratamiento público de datos en base a esta legitimación será mínimo y, en ocasiones, reconducible a una obligación legal o un interés público.

2.2.2.5. Satisfacción de intereses legítimos.

El propio artículo 6.1 RGPD, en su último párrafo, establece que esta causa de legitimación «no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones».

Podría plantearse en este apartado si, el tratamiento de datos llevado a cabo por autoridades públicas al margen del «ejercicio de sus funciones», podría tener su causa de licitud en la satisfacción de intereses legítimos.

Esta cuestión ha sido resuelta por la propia AEPD, en base a lo establecido en el Dictamen 6/2014 del Grupo de Trabajo del Artículo 29 antes citado, interpretando esta disposición de forma amplia, señalando que cualquier Administración Pública está excluida de utilizar el interés legítimo como causa de licitud de su tratamiento.

Concluye la AEPD, al igual que defendía el Grupo de trabajo del artículo 29, que la Administración no puede recurrir al interés legítimo como base jurídica para el tratamiento de datos, tal como se establece en el propio RGPD. En cambio, debe entenderse que el apartado e), "misión de interés público", debe interpretarse de manera amplia, lo que permite a las Administraciones realizar tratamientos de datos personales, incluso en el ámbito del

Derecho Privado, siempre que sean necesarios para cumplir con las finalidades legítimas que el ordenamiento jurídico les otorga o autoriza.

Es cierto que, las autoridades nacionales de otros países, podrían hacer una interpretación distinta. Por ejemplo, la autoridad británica permite el interés legítimo a las autoridades públicas cuando actúan por motivos distintos del ejercicio de su autoridad pública, como llevar a cabo actuaciones comerciales. La Information Commissioner's Office (ICO) establece lo siguiente en su página web: «Public authorities can only rely on legitimate interests if they are processing for a legitimate reason other than performing their tasks as a public authority».

Tras el estudio de todas las causas del artículo 6 del RGPD y el análisis de cómo se aplican en la Administración Pública, podemos afirmar que casi la totalidad de sus tratamientos se basarán en una obligación legal o el ejercicio de competencias públicas. Como se ha indicado, existen algunas excepciones, pero el porcentaje de tratamientos que se legitiman en base a otras causas es totalmente residual.

Para tener una visión de lo que sucede en la realidad de las Administraciones Públicas españolas, se van a analizar a continuación los tratamientos de algunas de ellas, seleccionando una muestra de diferentes organizaciones pertenecientes a la Administración General del Estado, Administración Autonómica, Administración Local y una autoridad administrativa independiente.

Se analizará cuántos tratamientos tienen como causa de licitud una obligación legal o competencia pública, independientemente que puedan tener más causas añadidas[2].

- Centro de Sistemas y Tecnologías de la Información y las Comunicaciones del Ministerio de Defensa.

  Con un total de 9 tratamientos, el 100% tiene al menos una de las siguientes causas de legitimación: obligación legal y/o competencia pública (en algunos tratamientos concurren otras causas diferentes junto con las anteriores).

[2] La información ha sido extraída de los "registros de actividades de tratamiento" que son públicos en las páginas oficiales de los organismos que se mencionan.

- Consejería de Digitalización de la Comunidad de Madrid.

  Con un total de 90 tratamientos, 89 de ellos (es decir, el 98.8888888889%) tiene al menos una de las siguientes causas de legitimación: obligación legal y/o competencia pública (en algunos tratamientos concurren otras causas diferentes junto con las anteriores).

  Existe solo un tratamiento (Contratación) que tiene como causa de legitimación única la ejecución de un contrato.

- Servicio de Información y Administración Electrónica del Ayuntamiento de Valladolid.

  Con un total de 9 tratamientos, el 100% tiene al menos una de las siguientes causas de legitimación: obligación legal y/o competencia pública (en algunos tratamientos concurren otras causas diferentes junto con las anteriores).

- Agencia Española de Protección de Datos.

  Con un total de 22 tratamientos, 20 de ellos (es decir, el 90,90%) tiene al menos una de las siguientes causas de legitimación: obligación legal y/o competencia pública (en algunos tratamientos concurren otras causas diferentes junto con las anteriores).

  Existen solo dos tratamientos (Gestión y control de la biblioteca y Régimen interior) que tienen como causa de legitimación la ejecución de un contrato.

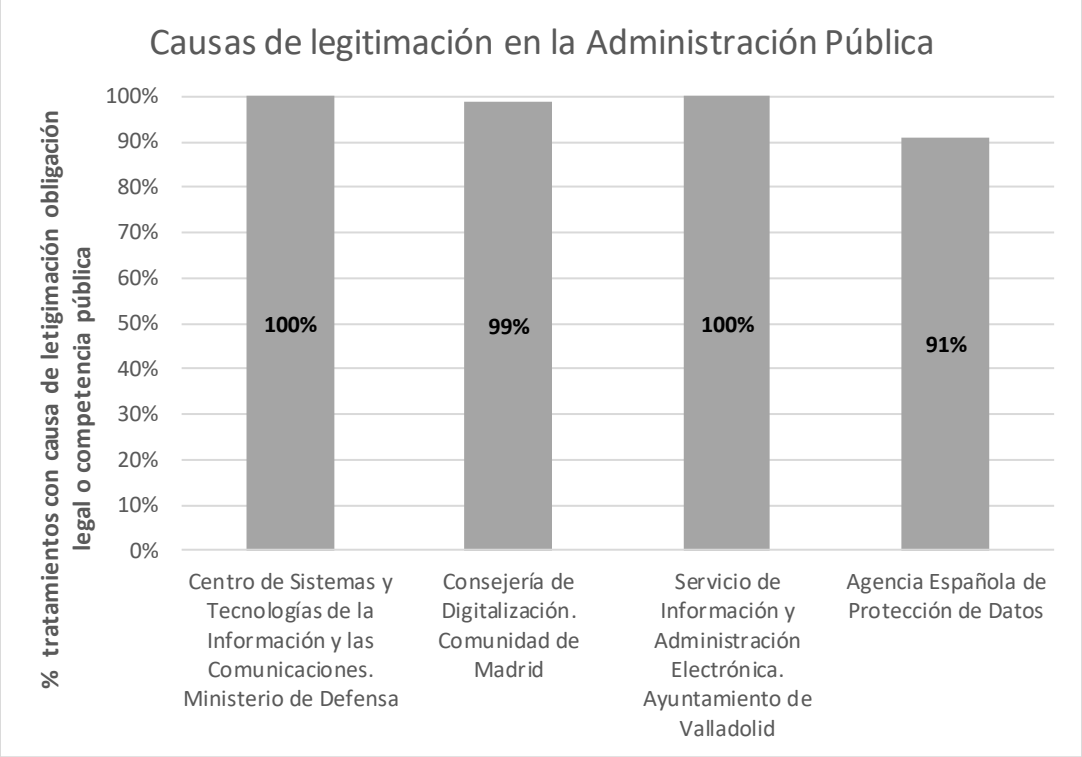

Figura 1: Causas de legitimación en la Administración Pública. Fuente: elaboración propia.

Tras el estudio de las causas de legitimación de la Administración Pública puede concluirse que, en casi la práctica totalidad de los tratamientos de las Administraciones Públicas, cuando el sujeto ejerza su derecho de supresión, este se denegará por aplicación del artículo 17.3 letra b) del RGPD.

Además, en ese porcentaje tan discreto que tiene causas de legitimación diferentes, cabe la posibilidad de que apliquen otras excepciones del artículo 17.3: ejercer el derecho a la libertad de expresión e información, por razones de interés público en el ámbito de la salud pública, con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos o para la formulación, el ejercicio o la defensa de reclamaciones. Entre estas excepciones hay varias que son muy habituales en la Administración Pública.

Ello hace plantearse si en el ámbito público realmente existe la capacidad de control del interesado sobre sus datos personales, ya que lo habitual será denegarle este derecho. La importancia de esto recae en cómo proteger la privacidad de los interesados que, en la mayoría de los casos, lo que buscan es que sus datos no sean accesibles o, mejor dicho, *hiperaccesibles* por cualquiera que busque información sobre ellos.

Ello lleva a buscar soluciones para que, a pesar de que los datos no sean suprimidos, el interesado vea protegido sus derechos e intereses.

2.3. Diferencia entre el derecho de supresión y el derecho al olvido.

En el epígrafe anterior se ha analizado el derecho de supresión del artículo 17 del RGPD, derecho que se viene utilizando como sinónimo del "derecho al olvido", y así lo hace el propio RGPD en su considerando 65.

También se hace esta analogía en el propio artículo 17 del RGPD, que tiene como título: «Derecho de supresión («el derecho al olvido»)».

Pero derecho de supresión y derecho al olvido no son sinónimos. La Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala) de 13 de mayo de 2014 en el asunto C-131/12 (Google Spain, S.L. y Google Inc. contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González), consagra un derecho con un significado diferente del que recoge el artículo 17 RGPD: el derecho al olvido frente a los motores de búsqueda.

Javier APARICIO SALOM (2019, p.381), ex jefe de la asesoría jurídica de la AEPD, recoge que:

«Bajo el mismo nombre de derecho al olvido, se consagra en esta sentencia un derecho radicalmente diferente, como es exigir que, el motor de búsqueda no incluya en la lista de resultados de búsqueda por su nombre, ni la referencia ni el enlace a los contenidos que incluyen información que no les conviene. La sentencia no consagra el derecho al olvido como una extensión del derecho de supresión, de hecho, ni siquiera obliga al editor a suprimir los datos objeto de olvido, sino que, manteniendo esos datos publicados, simplemente obliga a dificultar su localización al prohibir al motor de búsqueda que los indexe. El derecho reconocido en la sentencia es más bien una aplicación concreta del derecho de oposición que regula el artículo 21 RGPD y no del de supresión del artículo 17 RGPD».

Es decir, con el derecho al olvido la información no se suprimirá de las bases de datos del responsable, si no que dejarán de ser accesibles a través de los motores de búsqueda.

Este derecho puede ejercitarse de dos formas diferenciadas con unas consecuencias idénticas, de acuerdo con lo establecido en la sentencia citada:

- Acudiendo al editor de la página web. Los editores tienen la facultad de indicar a los motores de búsqueda, con la ayuda, concretamente, de protocolos de exclusión como «robot.txt», o de códigos como «noindex» o «noarchive», que desean que una información determinada, publicada en su sitio, sea excluida total o parcialmente de los índices automáticos de los motores. Esto no implica eliminar la información de ningún sitio, simplemente añadir unas etiquetas para que los motores no indexen la información, de manera que encontrarla se haga muy difícil, es decir, dejaría de ser *hiperaccesible*.
- Acudiendo directamente al motor de búsqueda, de manera que, si se cumplen los requisitos, estaría obligado a eliminar de la lista de resultados obtenidos a partir de una búsqueda por nombre, los vínculos a páginas web, publicados por terceros que contengan información relativa a esa persona, aunque la publicación sea lícita. Esto tampoco implica la supresión del contenido de la web, solo dejará de ser indexada por el motor de búsqueda. Acudir a esta solución es una opción muy válida y normalmente muy eficaz. Por ejemplo, Google, ha puesto a disposición de todos los internautas un «Formulario de solicitud de retirada de datos personales» donde ejercitar el derecho al olvido. Si bien, el objeto de este trabajo es dar visibilidad y soluciones a lo que está en manos de la Administración Pública como editor de muchos de los contenidos que se encuentran en la red.

En el apartado siguiente se analiza qué deben hacer las entidades públicas con los datos que no pueden ser suprimidos para garantizar la protección de los datos de los ciudadanos y su privacidad.

2.4. Soluciones para garantizar la privacidad de los datos conservados en la Administración Pública.

Lo dicho hasta ahora pone de manifiesto el escaso control que tiene el interesado cuando se trata de eliminar sus datos personales en manos de las entidades públicas. Queda claro que las Administraciones actúan en cumplimiento de la legalidad vigente y este trabajo no pretende juzgar las excepciones que recoge el legislador, ya que, sin duda, tienen una función nada reprochable.

A pesar de ello, es necesario que estos datos que no pueden eliminarse y, que en ocasiones deben ser publicados en páginas web, se traten de manera que se proteja la privacidad y protección de datos de los interesados.

Así, a continuación, se recogen una serie de soluciones que están en manos de las Administraciones Públicas para que los datos de los interesados no sean *hiperaccesibles*, a pesar de sus obligaciones de conservación y publicación por razones de transparencia.

2.4.1. Supresión de los datos cuando la normativa lo permita.

Es manifiesto que los casos en los que se podrán suprimir los datos serán muy pocos, si bien, existen algunos supuestos en los que la supresión deberá llevarse a cabo. Para aquellos casos en los que la causa de licitud del tratamiento no es una obligación legal o una competencia pública y se cumplan los requisitos del artículo 17 del RGPD los datos deberán ser eliminados.

En este caso, lo habitual será la "supresión por bloqueo", que no implica automáticamente su borrado físico.

El bloqueo de datos se recoge en el artículo 32 de la LOPDGDD, que establece que el responsable del tratamiento debe proceder al bloqueo de los datos cuando proceda a su rectificación o eliminación. De acuerdo con la normativa, este bloqueo implica la identificación y reserva de los datos, adoptando medidas técnicas y organizativas para evitar su tratamiento, incluida su visualización, salvo en los casos en los que los datos deban ser puestos a disposición de las autoridades competentes, como los jueces, tribunales, Ministerio Fiscal, Administraciones Públicas o las autoridades de protección de datos, para la exigencia de responsabilidades derivadas del tratamiento. Este bloqueo deberá mantenerse únicamente durante el plazo de prescripción de las posibles responsabilidades. Una vez transcurrido este plazo, los datos deberán ser destruidos.

Así lo dispone la AEPD en algunas de sus resoluciones, en las que hace referencia a la necesidad de esta modalidad de supresión. Dice la AEPD en la Resolución núm. R/00750/2022 de 8 de agosto de 2022 que, cuando la causa de licitud no está basada en los artículos 6.1 letras c y e, se debe proceder a la supresión mediante el bloqueo conforme a lo establecido en la normativa de protección de datos:

«La modalidad de bloqueo de los datos de carácter personal sometidos a tratamiento que, salvo en las circunstancias recogidas en el citado artículo 17.3 b) y e), no implicará automáticamente su borrado físico. Esta actuación está sometida a determinadas condiciones con las que se pretende asegurar y garantizar el derecho del afectado a la protección de sus datos de carácter personal, de modo que el responsable del tratamiento no puede disponer de tales datos.

Los datos bloqueados quedarán a disposición exclusiva de los Tribunales, el Ministerio Fiscal u otras Administraciones públicas competentes, en particular las autoridades de protección de datos, para las exigencias de posibles responsabilidades derivadas del tratamiento y por el plazo de prescripción de estas. Los datos bloqueados no podrán ser tratados para ninguna finalidad distintas a las señaladas.»

La AEPD, en su Informe N/REF: 00148/2019, señala que, en todo caso, debe recordarse que el mantenimiento de los datos en estado bloqueado constituye una excepción al borrado físico de los mismos, que representa, en última instancia, el objetivo final de la cancelación. Esto se encuentra alineado con lo dispuesto en el artículo 16.3, que establece que, «cumplido el citado plazo deberá procederse a la supresión».

2.4.1.1. Nuevas tecnologías y supresión de datos.

En el contexto de la supresión de datos, un tema relevante y actual son las nuevas tecnologías, entre las que destaca el blockchain debido a su impacto y potencial en la gestión de datos personales. En este sentido, la AEPD publicó recientemente en noviembre de 2024 una nota técnica que explora la posibilidad de cumplir con el RGPD en infraestructuras blockchain, particularmente en lo que respecta al ejercicio del derecho de supresión. Este análisis demuestra cómo las tecnologías innovadoras pueden adaptarse a los requisitos del RGPD, lo que plantea nuevos desafíos y soluciones para garantizar la privacidad de los datos de los ciudadanos.

En su nota técnica, la AEPD aclara que la inmutabilidad del blockchain no es un concepto absoluto. Bajo ciertas condiciones, es posible modificar la cadena mediante un acuerdo entre usuarios, lo que permitiría eliminar bloques o transacciones. Aunque esta modificación puede generar inconsistencias, no es posible recuperar los datos eliminados, asegurando así la irreversibilidad de la supresión.

Por su parte, el Comité Europeo de Protección de Datos ha dejado claro que no se puede alegar la imposibilidad técnica para justificar el incumplimiento del RGPD. Es fundamental implementar medidas jurídicas, organizativas y técnicas adecuadas para garantizar la conformidad con la normativa y la protección de los derechos de los ciudadanos, incluso con el uso de tecnologías como el blockchain.

2.4.2. Derecho al olvido como editor.

Como ya se ha comentado, el derecho de supresión y el derecho al olvido no son lo mismo. El hecho de que la Administración no suprima los datos y que los publique en una determinada página web no es óbice para que esa información publicada esté *hiperaccesible* a cualquier internauta que lleve a cabo una búsqueda sobre el interesado y puede desempeñar un papel decisivo para la difusión de esta información, pudiendo constituir una gran injerencia en el derecho fundamental al respeto de la vida privada (Sentencia Mario Costeja, de 13 de mayo de 2014).

Para evitar esto, la Administración puede hacer uso de los ya mencionados protocolos de exclusión, de manera que, aunque la información no se elimine de la web, los motores no indexarán la información, y se hará muy complicada su búsqueda.

2.4.3. Informar a los interesados sobre la posibilidad de acudir al motor de búsqueda.

Una de las acciones que puede llevar a cabo la Administración para ayudar a que los datos de los interesados no sean *hiperaccesibles*, es informar, cuando el interesado solicita la eliminación de una información publicada en internet, sobre la posibilidad que tiene de acudir directamente al motor de búsqueda para pedir que retire la indexación de los contenidos.

Por supuesto esta medida no excluye las obligaciones que, como editor, pueda tener el responsable del tratamiento, y tampoco es de carácter obligatorio, si bien, es una medida complementaria para ayudar al interesado cuyos datos están *hiperaccesibles*, de forma simultánea a las acciones que realice la Administración.

2.4.4. Derecho de oposición.

Cuando la causa de licitud del tratamiento sea una misión de interés público, el interesado podrá oponerse en cualquier momento, por motivos relacionados con su situación particular, conforme al artículo 21.1 del RGPD.

En este caso, el responsable del tratamiento deberá cesar el tratamiento de los datos personales, a menos que pueda demostrar la existencia de motivos legítimos y de carácter imperioso que justifiquen el tratamiento, los cuales deben prevalecer sobre los intereses, derechos y libertades del interesado, o bien para la formulación, ejercicio o defensa de reclamaciones.

Así pues, aunque los datos no sean eliminados, el interesado podrá oponerse a tratamientos concretos de datos.

Esta opción es muy común, por ejemplo, en la publicación de listados de aprobados y suspensos en las diferentes páginas web de la Administración, donde el interesado puede oponerse a la publicación, aunque los datos no sean eliminados como tal.

2.4.5. Imposición de medidas técnicas y organizativas adecuadas.

La conservación de los datos de la Administración pública deberá llevarse a cabo bajo la implementación de medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, tal y como se recoge en los artículos 24 y 32 del RGPD.

En este sentido, el responsable del tratamiento debe aplicar las medidas necesarias considerando la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos potenciales para los derechos y libertades de las personas físicas, con el fin de garantizar y demostrar que el tratamiento cumple con lo estipulado en la normativa vigente.

En relación con las medidas de seguridad en el ámbito del sector público, ha de acudirse a la disposición adicional primera de la LOPDGDD. Esta norma indica que el Esquema Nacional de Seguridad establecerá las medidas necesarias para proteger los datos personales en el caso de su tratamiento, con el fin de prevenir su pérdida, alteración o acceso no autorizado. Estas medidas deberán estar alineadas con los criterios para la evaluación del riesgo en el tratamiento de datos, conforme a lo establecido en el artículo 32 del RGPD. Los responsables mencionados en el artículo 77.1 de la LOPDGDD deberán aplicar las medidas previstas en el ENS a los tratamientos de datos que realicen. Además, deberán fomentar la implementación de medidas equivalentes en las empresas o fundaciones vinculadas a ellos que estén sometidas al Derecho privado.

Es decir, todas las entidades de la Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local, los organismos públicos y entidades de Derecho público vinculadas o dependientes de las Administraciones Públicas, las autoridades administrativas independientes, corporaciones de Derecho público, fundaciones del sector público, universidades públicas, etc… estarán obligadas a cumplir el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. Esta norma establece una serie de medidas para garantizar una protección adecuada de la información tratada y los servicios prestados. El objetivo de estas medidas es asegurar aspectos clave como el acceso, la confidencialidad, la integridad, la trazabilidad, la autenticidad, la disponibilidad y la conservación de los datos, la información y los servicios gestionados por medios electrónicos en el ejercicio de sus competencias.

2.4.6. Digitalización de la documentación.

En el contexto de las soluciones para garantizar la privacidad de los datos conservados en la Administración Pública, la digitalización se presenta como una herramienta útil y eficaz. su implementación facilita la gestión eficiente de grandes volúmenes de información al reducir la dependencia de soportes físicos, optimizando los procesos asociados a los plazos de conservación y eliminación de datos. Las Administraciones Públicas enfrentan importantes retos derivados de la acumulación de documentos en soporte físico, que implican elevados costos logísticos y administrativos. La transición hacia sistemas electrónicos permite un control más preciso y automatizado, asegurando que los datos se eliminen en determinados plazos, optimizar recursos, reducir costes y mejorar la eficacia administrativa.

Un ejemplo práctico es el uso de sistemas automatizados para aplicar plazos de conservación y eliminación. Estas herramientas permiten programar alertas y ejecutar supresiones cuando se alcanzan los plazos legales, evitando errores humanos y garantizando un cumplimiento más consistente con el principio de limitación del plazo de conservación.

Además, la digitalización facilita la implementación de medidas técnicas como el bloqueo de datos, asegurando que la información sea inaccesible para usos no autorizados mientras se conserva para fines legales.

El Real Decreto 4/2010, de 8 de enero, que regula el Esquema Nacional de Interoperabilidad (ENI), promueve la digitalización de la actividad de la Administración Pública como uno de sus

objetivos principales. En su artículo 21.1, letra h), establece que las Administraciones deben adoptar medidas destinadas a asegurar la conservación de los documentos electrónicos a lo largo de su ciclo de vida. Estas medidas deben garantizar que los documentos sean recuperables durante el plazo mínimo de conservación determinado por las normas administrativas y las obligaciones jurídicas.

Asimismo, el ENI subraya la necesidad de preservar los documentos a largo plazo, asegurando su valor probatorio y su fiabilidad como evidencia electrónica de las actividades y procedimientos administrativos. Estas disposiciones buscan garantizar no solo la transparencia y la traza documental, sino también la correcta identificación de los órganos de las Administraciones Públicas y de las Entidades de Derecho Público vinculadas o dependientes de estas, que ejercen la competencia sobre el documento o expediente.

Finalmente, es fundamental señalar el Real Decreto 311/2022, de 3 de mayo, que regula el Esquema Nacional de Seguridad (ENS), el cual resulta esencial en el contexto de la digitalización de la Administración Pública. La digitalización debe ir acompañada de un enfoque robusto en cuanto a la seguridad de la información, y el ENS desempeña un papel clave al establecer los requisitos mínimos de seguridad para los sistemas de información que gestionan los datos. Esta norma exige la implementación de medidas técnicas y organizativas que protejan los datos contra accesos no autorizados, alteraciones y destrucción indebida. Al seguir las directrices del ENS, las Administraciones pueden garantizar la integridad y confidencialidad de los datos a lo largo de su ciclo de vida, especialmente cuando se emplean sistemas automatizados para el control y eliminación de documentos conforme a los plazos legales establecidos.

2.4.7. Establecer plazos de conservación de los datos adecuadas y no excesivas

El hecho de que, como norma general, el derecho de supresión ejercido por el interesado se deniegue en virtud de la excepción prevista en el artículo 17.3 del RGPD, no implica que las Administraciones Públicas nunca eliminen los datos que obran en su poder. Estas entidades tienen la capacidad de establecer plazos de conservación para los datos, siempre que lo hagan respetando las normativas específicas que les son aplicables. No obstante, dichas normativas suelen ser complejas y, en muchos casos, presentan ambigüedades que dificultan su correcta aplicación.

Esta cuestión será analizada en profundidad en el apartado 3, donde se examinan los criterios y procedimientos relacionados con la conservación y eliminación de datos en el sector público.

3. La eliminación de los datos derivada de la limitación de los plazos de conservación por el responsable del tratamiento.

En segundo lugar, la supresión de los datos en la Administración Pública por aplicación de la normativa de protección de datos, viene dada como consecuencia de la aplicación de uno de los principios recogidos en el artículo 5 del RGPD, el «principio de limitación del plazo de conservación», que supone que los datos solo podrán ser mantenidos permitiendo la identificación del interesado, durante el tiempo estrictamente necesario para cumplir los fines del tratamiento.

Este principio se recoge en el apartado 1 letra e) del artículo 5 y está en íntima relación con el principio de minimización de datos (artículo 5.1 letra c) del RGPD) y con el de responsabilidad proactiva (artículos 5.2, 24 y 32 del RGPD), de manera que la identificación del afectado se realice durante el mínimo tiempo necesario para que se cumplan los fines del tratamiento.

La responsabilidad proactiva, es una de las mayores novedades que presenta el RGPD, así lo indica la LOPDGDD, y exige que el responsable del tratamiento adopte las medidas que procedan para garantizar la seguridad del mismo, en este caso, serán medidas para garantizar que los datos se mantienen durante el tiempo necesario para la finalidad del tratamiento.

Ello supone que el Responsable del Tratamiento debe fijar unos plazos de supresión periódica de los datos, lo que encuentra un correlato en el derecho de supresión (JUAN CARLOS HERNÁNDEZ PEÑA 2021) analizado en el apartado anterior de este trabajo.

No obstante, el mismo artículo 5.1 letra e), contiene excepciones a la limitación del tratamiento y estableciendo que, los datos personales, podrán mantenerse por períodos más largos, siempre que se utilicen exclusivamente con fines de archivo en interés público, investigación científica o histórica, o para fines estadísticos. No obstante, esto estará condicionado a la implementación de las medidas técnicas y organizativas necesarias, conforme al Reglamento, para garantizar la protección de los derechos y libertades de los interesados.

Estas excepciones deberían interpretarse de modo restringido, no deberían justificar una tendencia a almacenar y conservar datos por periodos prolongados (JUAN CARLOS HERNÁNDEZ PEÑA 2021).

Tal y como establece la AEPD (Informe N/REF: 00148/2019, de 9 de diciembre de 2020), debe procederse a un examen pormenorizado de cada uno de los tratamientos incluidos en el "registro de actividades de tratamiento" (RAT) de cada organización, y deberá determinarse, para cada uno de ellos, el plazo en el que deberán eliminarse los datos. Es más, el propio artículo 30 RGPD, en la información que debe contener el RAT, recoge en su apartado 1, letra f), «los plazos previstos para la supresión de las diferentes categorías de datos», cuando sea posible.

Nos encontramos ante un principio general aplicable tanto al sector público como al privado. Sin embargo, este trabajo se centra en analizar su aplicación específica en el ámbito de las Administraciones Públicas, destacando las particularidades y desafíos que surgen en relación con la limitación del plazo de conservación de los datos.

En comparación con el sector privado, donde la supresión de datos permite una mayor flexibilidad y adaptación a los criterios del RGPD y LOPDGDD, el sector público enfrenta condicionantes adicionales que restringen significativamente este derecho. Las Administraciones Públicas están sujetas a normativas específicas, como las relacionadas con archivos o transparencia entre otras, que imponen la conservación de documentos para garantizar la trazabilidad administrativa, el acceso a la información pública y la protección del patrimonio documental.

Mientras que las empresas privadas pueden eliminar los datos cuando ya no son necesarios para los fines para los que fueron recabados, las AAPP deben armonizar los principios del RGPD con un marco normativo que prioriza los intereses generales sobre los derechos individuales.

Esta diferencia pone de manifiesto que, mientras el sector privado tiende a centrarse en el cumplimiento individualizado de los derechos de los interesados, el sector público debe encontrar un equilibrio entre estos derechos y sus responsabilidades colectivas, lo que plantea retos únicos en la implementación del derecho de supresión.

Para poder analizar este principio en profundidad se estructuran dos apartados diferenciados:

1. En primer lugar, se examinará la normativa sectorial aplicable a la eliminación de datos, identificando las disposiciones normativas que pueden aplicar a este proceso.
2. En segundo lugar, se analizarán los condicionantes específicos de la Administración Pública que diferencian la eliminación de datos en este ámbito respecto al sector privado.

3.1. Normativa sectorial que contiene plazos de eliminación.

Para establecer plazos de eliminación y conservación de los datos, es necesario revisar si existen obligaciones concretas impuestas por la normativa. En ocasiones, es el legislador quien fija plazos de conservación determinados para materias concretas.

Si existiese normativa sectorial que indique plazos, se aplican de forma preferente, así lo dispone el artículo 12.5 LOPDGDD. Cuando las leyes aplicables a ciertos tratamientos impongan un régimen particular que afecte al ejercicio de los derechos establecidos en el Capítulo III del RGPD, se deberá seguir lo dispuesto en dichas leyes.

3.1.1. Ejemplos de normativa sectorial con plazos de conservación y/o eliminación.

A continuación, se realizará un breve repaso de las normativas más relevantes que establecen plazos de eliminación o conservación de datos en determinadas materias, especialmente en aquellas de uso más frecuente. Este análisis no tiene carácter exhaustivo ni pretende ofrecer una enumeración completa de todos los casos existentes, ya que dicho objetivo excede el alcance de este trabajo.

1. Videovigilancia.

   De acuerdo con la LOPDGDD, los datos deberán ser eliminados en el plazo de un mes desde que fueron captados, salvo que deban conservarse para acreditar la comisión de determinados actos delictivos. En ese caso serán puestos a disposición de las autoridades competentes en el plazo de 72 horas.

2. Documentación clínica.

   La Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica,

establece la obligación de los centros sanitarios de conservar la documentación clínica durante el tiempo necesario y adecuado en cada caso y, como mínimo, 5 años.

También existirá obligación de conservación en los siguientes casos: efectos judiciales, razones epidemiológicas, de investigación o de organización y funcionamiento del Sistema Nacional de Salud.

La ley establece un plazo mínimo, 5 años, pero además habrá que tener en cuenta la normativa autonómica, ya que muchas comunidades autónomas han fijado criterios de conservación diferente relacionados con la documentación clínica, siempre y cuando el mínimo sea 5 años.

Por ejemplo, la Comunidad autónoma de Cataluña, en la Ley 21/2000, de 29 de diciembre, sobre los derechos de información concernientes a la salud y la autonomía del paciente, y la documentación clínica, dedica su artículo 12 a la conservación de la historia clínica, indicando que debe conservarse como mínimo hasta veinte años después de la muerte del paciente. No obstante, se pueden seleccionar y destruir los documentos que no son relevantes para la asistencia, transcurridos diez años desde la última atención al paciente.

Otras comunidades autónomas han hecho algo similar estableciendo plazos diferentes. Cantabria, 15 años; Valencia, 5 años, etc…

Esto pone de manifiesto la disparidad que existe en la legislación española y la falta de criterios generales.

3. Investigación biomédica.

La Ley 14/2007, de 3 de julio, de Investigación biomédica establece un plazo de conservación mínimo de 5 años, transcurrido el cual el interesado podrá solicitar la cancelación.

Si el interesado no los cancelase, se conservarán el tiempo necesario para preservar la salud de las personas afectadas.

4. Comunicaciones electrónicas.

   De acuerdo con la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, los datos deberán conservarse 12 meses. Reglamentariamente, se podrá ampliar o reducir este plazo para determinados datos con máximo de 2 años y mínimo de 6 meses.

5. Blanqueo de capitales y financiación del terrorismo.

   La Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo, establece un plazo de conservación de 10 años a los sujetos obligados por la ley.

Por otro lado, han de tenerse en cuenta en este sentido los plazos de prescripción, ya que los datos deberán conservarse, en ocasiones bloqueados, tal y como indica el artículo 32.2 de la LOPDGDD, para la «exigencia de posibles responsabilidades derivadas del tratamiento durante el plazo de prescripción de las mismas». Es decir, los datos no podrán eliminarse definitivamente hasta que no haya trascurrido el plazo pertinente en cada caso para la exigencia de responsabilidades.

En este sentido, ha de tenerse en cuenta la normativa que existe de prescripción de determinadas acciones y delitos, entre las más comunes para las organizaciones podemos citar las siguientes:

1. Documentos tributarios.

   Se conservarán durante un plazo de 4 años que corresponde con el plazo de prescripción de las deudas tributarias de acuerdo con la Ley 58/2003, de 17 de diciembre, General Tributaria.

2. Acciones derivadas del contrato de trabajo.

   De acuerdo con el Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores, estas acciones, cuando no tengan previsto un plazo de prescripción específico, prescribirán al año.

3. Responsabilidades penales.

   Habrá que estar a lo establecido en la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal y atender al delito concreto, siendo el máximo de 20 años[3].

4. Acciones personales sin plazo especial.

   En este sentido debe acudirse al Código Civil de 1889, que en su artículo 1964 establece que «las acciones personales que no tengan plazo especial prescriben a los cinco años». Este plazo, que anteriormente era de 15 años, se reduce a 5 en virtud de la Disposición final primera de la Ley 42/2015, de 5 de octubre, de reforma de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.

5. Tratamiento de datos personales.

   También tienen plazo de prescripción las responsabilidades relacionadas con el tratamiento de datos personales, para ello habrá que estar al artículo 78 de la LOPDGDD que establece el plazo de prescripción de sus infracciones:

   a) Las sanciones de hasta 40.000 euros prescriben en un plazo de un año.
   b) Las sanciones entre 40.001 y 300.000 euros prescriben en un plazo de dos años.
   c) Las sanciones superiores a 300.000 euros prescriben en un plazo de tres años.

Deberá ser el responsable del tratamiento el que, teniendo en cuenta toda la normativa existente que aplica al tratamiento concreto, incluyendo las normas sectoriales aplicables a su actividad, decidir cuál será el plazo de conservación y eliminación de los datos.

Así el responsable del tratamiento deberá revisar todo su Registro de Actividades estableciendo plazos individualizados para su conservación, eliminación o, en su caso, mantenerse bloqueados como estadio previo a su destrucción y borrado físico.

[3] No prescriben los delitos de lesa humanidad y de genocidio y los delitos contra las personas y bienes protegidos en caso de conflicto armado, tampoco los delitos de terrorismo si hubieren causado la muerte de una persona.

En muchos casos, como se ha observado, es el legislador quien establece plazos concretos para la conservación o eliminación de datos en actividades, sectores o supuestos específicos. Sin embargo, en otros casos, determinar dichos plazos no es tan sencillo, lo que lleva a decisiones que carecen de criterios objetivos o una base legal sólida. Esto puede derivar en inconsistencias, como la aplicación de plazos muy dispares para tratamientos similares, generando posibles problemas tanto legales como organizativos.

Esta situación evidencia la necesidad de una regulación más clara que oriente estas decisiones. Aunque el responsable del tratamiento tiene la obligación de definir plazos, estas decisiones deberían fundamentarse en criterios objetivos, uniformes y ajustados a las normativas aplicables.

Si bien esta problemática afecta tanto a organizaciones públicas como privadas, en las Administraciones Públicas la situación es aún más compleja debido a la mayor cantidad de normativas aplicables y a condicionantes específicos, como la transparencia, la conservación del patrimonio documental y las obligaciones de acceso a la información pública.

Por tanto, cada organización, considerando las normas sectoriales aplicables, así como los plazos de prescripción, fiscalización y las posibles responsabilidades derivadas, debe establecer plazos claros y coherentes para la conservación y eliminación de datos, garantizando el cumplimiento normativo y la coherencia en su gestión documental.

Antes de abordar la normativa específica aplicable a las Administraciones Públicas, se presenta un ejemplo práctico sobre la gestión de los plazos de conservación documental, extraído de «El consultor de los Ayuntamientos». En este caso, el Ayuntamiento de Girona utiliza un sistema de superposición o concatenación de plazos, que permite determinar con precisión el periodo final de retención de un documento. Este enfoque permite que, una vez transcurrido el plazo más largo establecido, el documento pueda considerarse prescrito desde el punto de vista legal.

El ejemplo se centra en un contrato de adjudicación de una obra pública, cuyos plazos de conservación serían los siguientes:

- Vigencia: 2 años desde la formalización del contrato (o el plazo específico fijado en el mismo).
- Anulabilidad o revocabilidad: 4 años desde la resolución de adjudicación.
- Fiscalización:
    - 7 años desde la resolución de adjudicación.
    - 7 años desde la aprobación de la última certificación de obras.
- Responsabilidad derivada:
    - Los años de garantía ofertados por el contratista en el proceso de selección.
    - 10 años por la dirección de obra desde la formalización del contrato.
    - 15 años por la construcción desde la formalización del acta de recepción de la obra.

En este caso, el plazo más largo sería de 15 años, contado desde la formalización del acta de recepción de la obra, y este prevalecería como el periodo final de retención.

El Ayuntamiento de Girona establece estos periodos de retención basándose en criterios de legalidad, evitando recurrir a decisiones subjetivas basadas en la prudencia. Asimismo, señala la importancia de considerar no solo los plazos de prescripción administrativa, sino también los plazos de prescripción penal, especialmente en áreas sensibles como la contratación pública o la concesión de subvenciones, que generan una elevada atención pública.

No obstante, el Ayuntamiento advierte que, aplicar plazos penales en casos menos relevantes, podría conducir a una conservación excesiva de documentos, lo que resultaría poco eficiente y contrario a los principios de gestión documental.

3.2. Condicionantes en la normativa aplicable a las Administraciones Públicas relativas a la conservación y eliminación de la documentación.

En el apartado 3.1 se ha examinado la normativa general que regula los plazos de supresión aplicables a cualquier tipo de organización. No obstante, resulta imprescindible tener en cuenta una serie de condicionantes específicos del sector público que afectan de manera significativa las decisiones relacionadas con la conservación o eliminación de datos. Estas

particularidades requieren un análisis detallado, ya que pueden alterar de forma considerable los criterios y procedimientos utilizados, diferenciándose significativamente de los aplicados en el sector privado.

3.2.1. El documento administrativo.

En primer lugar, es fundamental definir el concepto de documento administrativo. El portal de internet "Punto de Acceso General electrónico" (PAGe) de la Administración General del Estado recoge que los documentos administrativos son el resultado de la actividad administrativa de los órganos de la Administración en el ejercicio de sus funciones y competencias». Estos tienen dos funciones principales:

- «Constancia: Garantizan la conservación de los actos de la Administración, acreditando sus efectos y permitiendo el derecho de acceso y consulta. Estas características conforman lo que se conoce como "traza documental".
- Comunicación: Actúan como medio de comunicación de los actos administrativos hacia los ciudadanos y otros organismos públicos.»

Por su parte, el artículo 49, apartado 1, de la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español, define el documento, a efectos de dicha norma, «toda expresión en lenguaje natural o convencional y cualquier otra expresión gráfica, sonora o en imagen, recogidas en cualquier tipo de soporte material, incluso los soportes informáticos».

Los documentos administrativos pueden presentarse en formato papel o electrónico. La gestión documental tradicional, basada en la impresión en papel, fue eficaz hasta principios del siglo XXI, cuando el volumen generado era manejable. Sin embargo, el papel en la Administración Pública ha crecido de manera desproporcionada, generando problemas de gestión y elevados costes de almacenamiento.

El coste asociado al mantenimiento de estos documentos representa una carga significativa para los presupuestos públicos. Por ello, es imprescindible adoptar sistemas de gestión documental digital que no solo reduzcan estos costes, sino que también optimicen la eficiencia en la administración y permitan una mejor gestión del derecho de supresión y la conservación de datos. La digitalización, como ya se ha dicho, facilita la aplicación de medidas técnicas para garantizar la protección de datos personales, como el bloqueo de datos y el acceso restringido.

No todos los documentos administrativos contienen datos personales, ya que esto depende de su naturaleza y finalidad. Sin embargo, lo más habitual es que sí incluyan algún tipo de dato personal, como una firma. En este sentido, el artículo 26 de la Ley 39/2015 exige que, para ser considerados válidos, los documentos administrativos electrónicos incorporen las firmas electrónicas correspondientes, salvo aquellos de carácter meramente informativo o que no formen parte de un expediente administrativo.

Por lo tanto, existirán documentos administrativos informativos que no contengan datos de carácter personal y que, por lo tanto, no les serán de aplicación los requisitos específicos de la normativa de protección de datos, lo que no excluye que deban protegerse por otras normas.

3.2.2. Fines de archivo en interés público, investigación científica o histórica y estadísticos.

El artículo 5 del RGPD, ya analizado previamente, establece que los datos podrán conservarse durante periodos más largos cuando se trate de fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos. Estos fines son habituales en el sector público y deben llevarse a cabo conforme lo dispuesto en el artículo 89.1 del RGPD, garantizando siempre que se adopten medidas técnicas y organizativas adecuadas para proteger los derechos y libertades de los interesados.

En este sentido, la LOPDGDD en su artículo 25 recoge el tratamiento de datos en el ámbito de la función estadística pública, que se llevará a cabo por los organismos que tengan atribuidas las competencias en la materia, se someterá a su legislación específica y al RGPD, y solo podrá basarse en el ejercicio de una competencia pública como causa de legitimación cuando, la estadística para la que se requiera la información, venga exigida por una norma de Derecho de la Unión Europea o se encuentre incluida en los instrumentos de programación estadística legalmente previstos.

Por otra parte, el artículo 26 de la LOPDGDD recoge el tratamiento de datos con fines de archivo en interés público por parte de las Administraciones Públicas. Este artículo establece que el tratamiento de datos con fines de interés público por parte de las Administraciones Públicas será lícito y se someterá a lo dispuesto en el RGPD y LOPDGDD con las especialidades que se derivan de lo dispuesto en:

- La Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español, que regula la conservación del patrimonio documental en el contexto de su valor histórico y cultural.
- El Real Decreto 1708/2011, de 18 de noviembre, que establece el Sistema Español de Archivos y regula el acceso a los archivos de la Administración General del Estado y sus organismos públicos.
- La legislación autonómica aplicable, que complementa el marco normativo con disposiciones específicas adaptadas a las particularidades de cada territorio.

Estas normativas son fundamentales para determinar los criterios de conservación y eliminación de la documentación administrativa, ya que establecen los límites y condiciones en los que debe preservarse la información con valor histórico, cultural o administrativo. Su análisis detallado se abordará en los apartados siguientes, dada su relevancia en el contexto de la gestión equilibrada entre la protección de datos y las obligaciones legales de conservación en las Administraciones Públicas.

3.2.3. El documento administrativo y el Patrimonio Documental.

El artículo 49.2 de la LPH define el concepto de Patrimonio Documental:

«Los documentos de cualquier época generados, conservados o reunidos en el ejercicio de su función por cualquier organismo o entidad de carácter público, por las personas jurídicas en cuyo capital participe mayoritariamente el Estado u otras entidades públicas y por las personas privadas, físicas o jurídicas, gestoras de servicios públicos en lo relacionado con la gestión de dichos servicios».

El artículo 52.1 de esta misma norma impone la obligación de proteger y conservar estos bienes de Patrimonio Documental, exigiendo que se mantengan en lugares adecuados. Asimismo, el artículo 55.1 señala que la eliminación o exclusión de estos documentos debe ser autorizada previamente por la Administración competente.

En consecuencia, los documentos generados por las Administraciones Públicas en el ejercicio de sus competencias forman parte del Patrimonio Documental y están sujetos a estrictas obligaciones de conservación. Este marco legal condiciona directamente las decisiones sobre la eliminación de datos en las Administraciones Públicas. Estas disposiciones reflejan la necesidad de equilibrar las obligaciones de conservación impuestas por la LPH con los

principios de protección de datos establecidos en el RGPD, especialmente el derecho de supresión, evidenciando la complejidad de gestionar estos intereses en el sector público.

3.2.4. Transparencia y conservación de datos.

Cuando se aborda la destrucción y conservación de documentos, es inevitable considerar las obligaciones en materia de transparencia que recaen sobre las Administraciones Públicas. Estas obligaciones, reguladas principalmente por la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, exigen que los documentos que sustentan la actividad pública sean conservados de manera adecuada. La falta de conservación o la destrucción indebida podría causar daños irreparables al derecho de acceso a la información pública, derecho nuclear del sistema de transparencia a que está sometida la actividad pública.

La Ley de Transparencia articula estas obligaciones mediante la imposición de deberes de publicidad activa a todas las Administraciones y entidades públicas, garantizando que la información relevante esté disponible para la ciudadanía. En este contexto, la conservación de determinados documentos no solo es una exigencia normativa, sino también una herramienta para promover la rendición de cuentas y la confianza en la gestión pública.

Por lo tanto, la conservación de determinados documentos se convierte en una exigencia para todos los que desarrollan actividades de relevancia pública.

La importancia de estas obligaciones ha sido objeto de análisis en diversos informes de la Comisión de Garantía de Acceso a la Información Pública (GAIP) de Cataluña, que destacan la importancia de criterios claros en la conservación documental para garantizar el acceso público a la información. En un caso presentado en noviembre de 2015, una reclamación contra el Ayuntamiento de L'Hospitalet de Llobregat por el acceso a un expediente de selección de empleados públicos (2010-2011) llevó a la emisión de un informe sobre el Proyecto de orden CLT/2018. Dicho informe subraya la necesidad de aplicar criterios de conservación documental basados en el interés público, desde la perspectiva del control y la transparencia en la gestión administrativa. Se concluyó que el derecho de acceso a la información pública quedaría gravemente comprometido si la documentación relevante fuera destruida sin un marco normativo claro.

Asimismo, en un informe posterior emitido en 2016, la GAIP reafirmó que ningún documento público puede ser eliminado sin cumplir estrictamente con los procedimientos reglamentarios. Este análisis amplía la interpretación del derecho de acceso a la información, considerando que cualquier información con relevancia pública o jurídica, capaz de motivar su ejercicio por parte de la ciudadanía, debe ser conservada conforme a la normativa aplicable.

Aunque el artículo 15 de la Ley de Transparencia hace referencia a la protección de datos, su alcance está limitado al derecho de acceso cuando éste involucra datos personales. Por tanto, no guarda relación directa con el derecho de supresión que se analiza en este trabajo. Su enfoque está centrado en garantizar que el acceso a la información pública respete la privacidad de los datos personales, pero no regula la eliminación o conservación de los mismos, lo que reduce su relevancia en el contexto de este estudio.

Eliminar documentos conforme a una regulación legal clara no solo es imprescindible para cumplir con las exigencias de transparencia, sino que también asegura la calidad y fiabilidad de la información publicada en los portales de transparencia. Este marco regulador debe complementarse con medidas que permitan integrar las obligaciones de transparencia con los principios del RGPD, como el derecho de supresión. De este modo, las Administraciones Públicas pueden garantizar la protección de los datos personales sin comprometer el derecho de los ciudadanos al acceso a la información pública.

3.2.5. La supresión y eliminación de documentos en la Administración Pública relacionada con la normativa de archivos y registros.

Como se ha visto hasta ahora, el hecho de que las Administraciones Públicas estén sujetas a estrictas obligaciones de conservación no implica que la eliminación de documentos sea imposible o que no vayan a suprimirse en ningún caso. La eliminación regulada de documentación administrativa desempeña un papel fundamental en la gestión de riesgos, minimizando las posibles incidencias relacionadas con la vulneración de la privacidad de las personas. No obstante, en el ámbito del sector público, este proceso no se rige por la normativa de protección de datos, sino por disposiciones específicas relativas a archivos y registros. Es decir, la supresión se hará siguiendo los cauces legales establecidos, al margen de la protección de datos personales.

Además, este contexto se ve agravado por los importantes problemas de espacio que enfrentan las Administraciones Públicas y sus archivos. La acumulación física de expedientes, especialmente en soporte papel, genera desafíos logísticos y financieros que afectan la eficiencia administrativa. La eliminación de documentación conforme a una regulación legal clara no solo contribuye a liberar espacio, sino que también asegura la calidad y fiabilidad de los datos disponibles, especialmente en portales de transparencia, donde la información debe ser accesible y relevante.

En este sentido, la digitalización, a la que ya se ha hecho referencia, se presenta como una solución clave para abordar los problemas asociados a la custodia física de expedientes. Al transformar los documentos en formatos digitales, no solo se optimiza el uso del espacio, sino que también se facilita una gestión más eficiente, integrando medidas técnicas para garantizar la protección de los datos personales y cumplir con los principios del RGPD.

Como ya se ha señalado, la supresión de documentos en el sector público no se realiza en virtud de la normativa de protección de datos, aunque esta ayuda a proteger los derechos y libertades de los ciudadanos. En su lugar, la eliminación está condicionada por normativas de archivos y registros, que establecen los criterios para decidir qué documentos deben conservarse y cuáles pueden destruirse.

Aunque no es objeto de este trabajo profundizar en la normativa específica sobre archivos, a continuación, se ofrece un breve resumen de las disposiciones aplicables en la Administración General del Estado (AGE), las Comunidades Autónomas y las Entidades Locales, que proporcionan el marco para la gestión y eliminación de documentos en el sector público.

3.2.5.1. Normas aplicables a cualquier Administración Pública.

Además de la Ley del Patrimonio Histórico Español y la Ley de Transparencia, aplicables de manera general a toda la Administración Pública y ya analizadas en apartados anteriores, existen normativas específicas que regulan la conservación y eliminación de información y documentación en el sector público. Estas disposiciones complementan el marco normativo general al proporcionar criterios y procedimientos claros que guían la gestión documental en las distintas entidades públicas.

Entre estas normativas destaca la Ley 39/2015, cuyo artículo 17.2 establece la obligación de conservar los documentos de forma que se garantice su autenticidad, integridad, conservación y consulta. Asimismo, determina que la eliminación de los documentos debe ser autorizada conforme a la normativa aplicable.

El Esquema Nacional de Seguridad (ENS), aprobado por Real Decreto 311/2022, también aplicable a todo el sector público, incluye obligaciones relacionadas con la conservación y destrucción de equipos y soportes susceptibles de almacenar información, tanto en formato electrónico como físico. Estas disposiciones aseguran un tratamiento adecuado de la información sensible durante su ciclo de vida.

Por su parte, el Esquema Nacional de Interoperabilidad (ENI), aprobado por Real Decreto 4/2010, regula aspectos clave de la conservación y eliminación de datos. En particular, su artículo 21 establece las condiciones necesarias para garantizar una gestión documental adecuada, incluyendo:

- Conservación de documentos: De acuerdo con los periodos determinados por las comisiones calificadoras, conforme a la normativa aplicable en cada caso.
- Medidas para la conservación electrónica: Garantizando la recuperación de documentos en función de los plazos mínimos legales, preservando su valor probatorio y fiabilidad como evidencia, y asegurando su conservación a largo plazo, así como la transparencia, la memoria y la identificación de los órganos de las Administraciones públicas y de las Entidades de Derecho Público vinculadas o dependientes de aquéllas que ejercen la competencia sobre el documento o expediente
- Eliminación de información y soportes: Debe realizarse conforme a la legislación aplicable, dejando constancia de la eliminación mediante un registro.

El ENI, en su disposición adicional primera, establece la obligación de desarrollar una serie de Normas Técnicas de Interoperabilidad (NTI) de cumplimiento obligatorio para las Administraciones Públicas. Entre estas, destaca la Resolución de 28 de junio de 2012, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Norma Técnica de Interoperabilidad de Política de gestión de documentos electrónicos. Esta norma regula que los procesos de gestión documental incluyan la conservación de los documentos en función

de su valor, basándose en el dictamen de la autoridad calificadora y mediante la definición de calendarios de conservación.

3.2.5.2. Administración General del Estado.

En el ámbito de la Administración General del Estado, el Real Decreto 1708/2011, de 18 de noviembre, establece el Sistema Español de Archivos y regula tanto el sistema de archivos de la Administración General del Estado como el régimen de acceso a los mismos. En lo relativo a la eliminación de documentos, su artículo 15 dispone que esta solo podrá realizarse cumpliendo estrictamente los requisitos y procedimientos establecidos en la normativa vigente.

Adicionalmente, este artículo señala que, en los aspectos no previstos en relación con la valoración y eliminación documental, deberá aplicarse lo dispuesto en el Real Decreto 1164/2002, de 8 de noviembre, que regula la conservación del patrimonio documental con valor histórico, el control de la eliminación de otros documentos de la Administración General del Estado y sus organismos públicos, así como la conservación de documentos administrativos en soportes diferentes al original.

Por otra parte, la Disposición Final Tercera del Real Decreto 1708/2011 establece que los titulares de los departamentos ministeriales deberán adoptar las medidas necesarias para garantizar la plena aplicación de esta norma en sus respectivos sistemas archivísticos. En cumplimiento de esta disposición, distintos ministerios han dictado normativas específicas para regular la gestión de sus archivos, por ejemplo:

- El Real Decreto 2598/1998, de 4 de diciembre, por el que se aprueba el Reglamento de Archivos Militares, aplicable al Ministerio de Defensa.
- La Orden JUS/439/2018, de 26 de abril, por la que se crea y regula el Sistema Archivístico del Ministerio de Justicia y de sus organismos públicos vinculados o dependientes.

3.2.5.3. Comunidades autónomas y entidades locales.

Las Comunidades Autónomas han legislado en el ámbito de sus competencias sobre archivos y gestión documental, estableciendo normativas específicas que regulan la conservación, eliminación y valoración de documentos. Entre otros ejemplos:

- Ley 6/1991, de 19 de abril, de Archivos y del Patrimonio Documental de Castilla y León.
- Ley 10/2001, de 13 de julio, de Archivos y Documentos de Cataluña.
- Ley 6/2023, de 30 de marzo, de Archivos y Documentos de la Comunidad de Madrid.
- Ley 19/2002, de 24 de octubre, de Archivos Públicos de Castilla-La Mancha.
- Ley 5/2022, de 23 de junio, de Gestión Documental Integral y Patrimonio Documental de la Comunidad Autónoma del País Vasco.
- Ley 7/2014, de 26 de septiembre, de archivos y documentos de Galicia.
- Ley 7/2011, de 3 de noviembre, de Documentos, Archivos y Patrimonio Documental de Andalucía.

Estas normativas no solo regulan los sistemas archivísticos autonómicos, sino que también definen las competencias y funciones de los archivos municipales, que se integran dentro de los sistemas archivísticos de cada Comunidad Autónoma.

En cada territorio, estas leyes establecen los plazos específicos para la conservación de los documentos generados por las Administraciones Públicas, incluyendo los producidos por las Administraciones Locales. Los archivos municipales son responsables de implementar procesos internos que garanticen la correcta evaluación y expurgo de los documentos. Sin embargo, cualquier eliminación debe contar con la autorización previa de las comisiones o juntas de valoración y expurgo designadas en cada Comunidad Autónoma, o, en su defecto, de los consejos de archivos autonómicos competentes.

Estas disposiciones refuerzan la importancia de la normativa autonómica en la regulación de los plazos de conservación y eliminación, garantizando que las decisiones relacionadas con el ciclo de vida de los documentos cumplan con criterios legales claros y uniformes en todo el territorio autonómico.

El resumen de este tercer apartado tan extenso es que la gestión de la supresión y conservación de datos en las Administraciones Públicas plantea retos significativos debido a la coexistencia de la normativa de protección de datos con disposiciones específicas sobre archivos, registros, transparencia o patrimonio documental.

A diferencia del sector privado, donde las decisiones de eliminación están generalmente regidas por el principio de limitación del plazo de conservación, en las Administraciones estas decisiones no se rigen prioritariamente por la normativa de protección de datos, sino por normativas específicas que regulan la conservación y eliminación documental. Estas normativas priorizan el interés público, la trazabilidad administrativa y la protección del patrimonio documental, lo que hace que la mayor parte de la documentación en este ámbito no pueda ser eliminada directamente conforme al RGPD, ya que existen obligaciones legales que exigen su conservación por razones de interés público, fines históricos o administrativos. Esto refuerza la idea de que la supresión de datos en el sector público está profundamente condicionada por factores normativos y organizativos ajenos a la normativa de protección de datos.

Además, las Administraciones Públicas operan bajo un marco normativo más complejo y estricto, con disposiciones específicas a nivel estatal, autonómico y local, como el Real Decreto 1708/2011 y el Esquema Nacional de Interoperabilidad (ENI). Estas normativas regulan no solo los plazos de conservación, sino también los procedimientos para la eliminación de documentos, exigiendo autorizaciones previas por parte de comisiones calificadoras. Este enfoque asegura que la eliminación documental sea transparente, controlada y compatible con las obligaciones de transparencia y rendición de cuentas, destacando que no es un proceso vinculado al RGPD, sino a la normativa sectorial aplicable.

En contraste, el sector privado goza de mayor flexibilidad para adaptar sus procesos de conservación y eliminación a sus necesidades operativas, siempre que respete los principios del RGPD. Sin embargo, esta flexibilidad no existe en las Administraciones Públicas, donde el marco legal busca equilibrar la protección de los derechos individuales con las responsabilidades colectivas derivadas de sus funciones públicas. En este sentido, herramientas como las tablas de retención documental son esenciales para establecer criterios objetivos y normativos que garanticen una gestión coherente de la conservación y eliminación de datos en el sector público.

4. Consecuencias para las entidades públicas por la vulneración de la normativa en materia de conservación y eliminación de datos.

En este apartado se analizarán las consecuencias sancionadoras y correctivas asociadas a la gestión de la eliminación y conservación de datos en las Administraciones Públicas, poniendo el foco especialmente en las previstas en la normativa de protección de datos. Asimismo, se abordará el régimen sancionador derivado de otras normativas específicas, como las relacionadas con la transparencia, los archivos y el patrimonio documental, que también condicionan estos procesos. Las Administraciones Públicas presentan particularidades significativas en comparación con el sector privado, especialmente porque no están sujetas a las mismas sanciones económicas establecidas en el RGPD para las entidades privadas, lo que genera diferencias sustanciales en la aplicación y el impacto del régimen sancionador.

4.1. Régimen sancionador de la normativa de protección de datos.

El RGPD establece un régimen sancionador general para las infracciones de sus disposiciones, caracterizado por la posibilidad de imponer sanciones económicas de gran magnitud. Estas sanciones son ampliamente conocidas por el público debido a sus elevados importes, que pueden alcanzar hasta 20 millones de euros o el 4 % del volumen de negocio total anual global del ejercicio financiero anterior, eligiéndose siempre la cuantía mayor. En particular, estas sanciones se aplican en casos como:

- Incumplimiento de los principios básicos para el tratamiento del artículo 5, entre los cuales se encuentra el “principio de limitación del plazo de conservación”.
- Infracción los derechos de los interesados a tenor de los artículos 12 a 22 que incluyen el derecho de supresión, mediante el cual los interesados pueden solicitar la eliminación de sus datos personales.

En España, el título IX de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD) regula el régimen sancionador en materia de protección de datos, clasificando las infracciones en muy graves, graves y leves, recogidas en los artículos

72, 73 y 74, respectivamente. Estas infracciones incluyen incumplimientos relacionados con el ejercicio de los derechos de los interesados, encuadrados en las tres categorías:

- ✓ Infracciones muy graves: El impedimento o la obstaculización o la no atención reiterada del ejercicio de los derechos establecidos en los artículos 15 a 22 del RGPD.
- ✓ Infracciones graves: El impedimento o la obstaculización o la no atención reiterada de los derechos de acceso, rectificación, supresión, limitación del tratamiento o a la portabilidad de los datos en tratamientos en los que no se requiere la identificación del afectado, cuando este, para el ejercicio de esos derechos, haya facilitado información adicional que permita su identificación.
- ✓ Infracciones leves: No atender las solicitudes de ejercicio de los derechos establecidos en los artículos 15 a 22 del RGPD, salvo que resultase de aplicación lo dispuesto en el artículo 72.1.k) LOPDGDD.

Asimismo, el artículo 72.1.a) de la LOPDGDD señala que la vulneración de los principios fundamentales recogidos en el artículo 5 del RGPD constituye una infracción muy grave. Entre estos principios se encuentra el "principio de limitación del plazo de conservación", analizado a lo largo de este trabajo. Su incumplimiento representa una de las infracciones más severas reconocidas por la legislación, subrayando la importancia de respetar este principio en la gestión de datos personales.

Pero en el caso de las Administraciones Públicas españolas hay que tener en cuenta, especialmente, el artículo 77 de la LOPDGDD, dedicado al régimen aplicable a determinadas categorías de responsables o encargados del tratamiento. Este artículo establece que, cuando una entidad del sector público de las enumeradas en el 77.1 de la LOPDGDD (AGE, Administraciones autonómicas, Entes locales, órganos constitucionales, autoridades administrativas independientes, Universidades públicas, etc...) cometa alguna infracción en la materia, la autoridad de datos competente dictará una resolución declarando la infracción y estableciendo, en su caso, las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción cometida.

Anteriormente, antes de la reforma de mayo de 2023, la única sanción aplicable a una Administración Pública era el apercibimiento. Sin embargo, con la modificación de la

LOPDGDD, el apercibimiento ha dejado de considerarse una sanción y se configura ahora como una medida de naturaleza correctiva, dentro de los poderes no sancionadores de las autoridades de control. Esta reforma ha sido introducida para ajustar la normativa española a las disposiciones del RGPD y reforzar el enfoque correctivo en lugar de punitivo en el ámbito público.

Igualmente, tras la reforma, las Administraciones Públicas continúan estando exentas de sanciones económicas, lo que sigue diferenciando significativamente al sector público del privado en el régimen sancionador.

Además, conforme al apartado 6 de este mismo artículo, la AEPD publicará en su página web las resoluciones relacionadas con las Administraciones Públicas, indicando la identidad del responsable que hubiera cometido la infracción.

Así, en la página web de la AEPD encontramos un apartado denominado: «Administraciones Públicas sancionadas por no responder a requerimientos y por incumplimiento de medidas». En este apartado se muestran las resoluciones sancionadoras de aquellas Administraciones Públicas que han sido sancionadas a lo largo de ese ejercicio por incumplimiento. Este incumplimiento puede referirse tanto a una orden dada por la Agencia como a la falta de contestación a un requerimiento de petición de información en el marco de unas actuaciones previas de investigación, todo ello de acuerdo con los poderes correctivos regulados en el artículo 58.2 del RGPD.

Cabe destacar que la mayoría de los procedimientos sancionadores iniciados durante 2022 y 2023 por no atender órdenes de cumplimiento de medidas o requerimientos de la Agencia Española de Protección de Datos (AEPD) corresponden a entidades de la Administración Local, especialmente Ayuntamientos. Este hecho refleja una tendencia significativa en la que las Administraciones Locales concentran un mayor número de incumplimientos relacionados con el artículo 58.2 del RGPD, que regula los poderes correctivos de las autoridades de protección de datos.

En el gráfico siguiente, se muestra claramente esta distribución. Las Administraciones Locales encabezan el número de procedimientos sancionadores, mientras que las Administraciones Generales del Estado y las Administraciones Autonómicas presentan cifras considerablemente inferiores. Este comportamiento puede deberse a varios factores, como la mayor proximidad

de las entidades locales al ciudadano y la frecuencia de sus interacciones, así como posibles carencias en recursos técnicos, organizativos o de formación en materia de protección de datos.

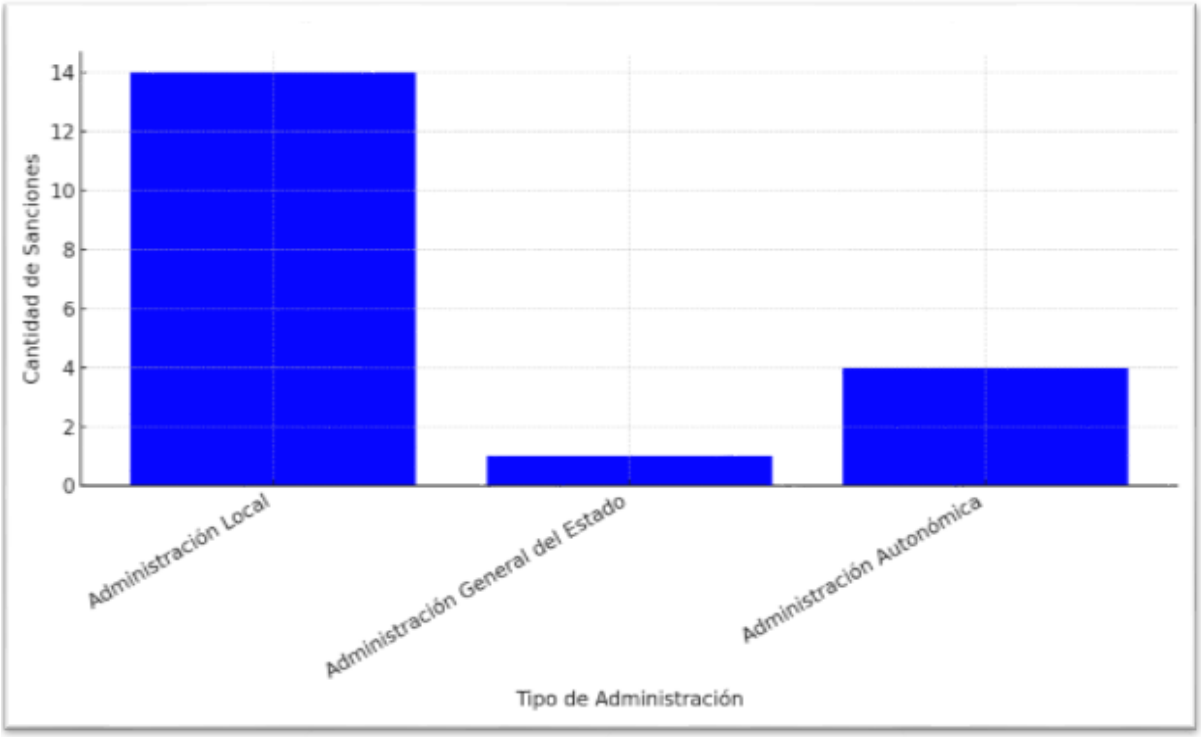

Figura 2: Distribución de procedimientos sancionadores de la AEPD realizados durante 2022 y 2023 como consecuencia de no atender una orden de cumplimiento de medidas o un requerimiento de medidas, clasificados por Administración pública. Fuente: elaboración propia.

La visualización de estos datos pone de manifiesto la importancia de implementar mecanismos adecuados para garantizar el cumplimiento de los requerimientos de la AEPD y las órdenes de adopción de medidas correctivas, especialmente en el ámbito local. Además, subraya la necesidad de reforzar la capacidad de gestión en estas entidades para garantizar que se cumplen plenamente las normativas aplicables y se minimizan los incumplimientos detectados.

En lo que respecta al régimen sancionador del RGPD, puede concluirse que en el ámbito público no existen sanciones pecuniarias dirigidas a las Administraciones Públicas, a diferencia de lo que ocurre con el sector privado, donde las empresas pueden enfrentarse a multas de gran magnitud por el incumplimiento de la normativa de protección de datos. Este contraste

significativo tiene importantes implicaciones: por un lado, la ausencia de multas económicas en el sector público reduce el incentivo real para priorizar el cumplimiento de la normativa, y por otro, puede generar una percepción de impunidad que debilita la confianza de los ciudadanos en la capacidad de las Administraciones Públicas para proteger adecuadamente sus datos personales.

No obstante, como se ha analizado, sí existen medidas correctoras y la posibilidad de publicación de las resoluciones sancionadoras, que buscan principalmente resolver los problemas identificados y fomentar la mejora en la gestión de datos por parte de las entidades públicas. Sin embargo, resulta evidente que estas medidas pueden no ser suficientes para garantizar que las Administraciones prioricen el cumplimiento de la normativa de protección de datos. Por ello, sería necesario explorar soluciones alternativas que refuercen el compromiso del sector público con la normativa de protección de datos, incentivando una mayor responsabilidad en la gestión de los datos personales de los ciudadanos.

4.2. Otras sanciones relacionadas con la normativa aplicable.

El análisis del régimen sancionador no se limita a la normativa de protección de datos. En el sector público, las Administraciones podrían estar sujetas a sanciones derivadas de otras normativas, como las relativas a la transparencia o el patrimonio documental, que también condicionan su gestión de la información.

4.2.1. Ley de Transparencia.

En el ámbito de la Ley de Transparencia, no se prevé un régimen sancionador específico relacionado directamente con la conservación y eliminación de documentos por parte de las Administraciones Públicas. Si bien esta normativa establece obligaciones claras en materia de publicidad activa y acceso a la información pública, no regula sanciones concretas para casos de negligencia en la custodia de documentos o su destrucción indebida. Esta ausencia puede interpretarse como una laguna legislativa que afecta la capacidad de garantizar plenamente la transparencia y el derecho de acceso a la información por parte de los ciudadanos.

En opinión de FERNÁNDEZ RAMOS, S. (2020) una de las carencias más relevantes de la LTAIBG, que tampoco ha sido subsanada por la mayoría de las leyes autonómicas, es la referente a la conservación de la información pública. En muchas ocasiones, el derecho de acceso a la

información no se ve frustrado por la negativa expresa o tácita del acceso, ni por la aplicación de los límites legales establecidos, sino por la imposibilidad material de ejercerlo debido a la destrucción, pérdida o falta de localización de la documentación que contiene la información solicitada. Este problema evidencia la necesidad de que las normativas de transparencia presten mayor atención a la adecuada conservación de la información y a las consecuencias de su pérdida. En este sentido, debería considerarse la tipificación de estas acciones como una infracción, especialmente en los casos en que no estén ya contempladas en la legislación aplicable sobre archivos y documentos, garantizando así una protección más efectiva del derecho de acceso a la información pública.

4.2.2. Ley del Patrimonio Histórico Español.

El artículo 76 de la Ley 16/1985, del Patrimonio Histórico Español, establece un régimen sancionador dirigido a diversas infracciones relacionadas con la conservación del patrimonio documental y bibliográfico. Entre las disposiciones más relevantes para el contexto de este trabajo destacan:

a) El incumplimiento por parte de los propietarios, titulares de derechos reales o poseedores de bienes de las disposiciones contenidas en los artículos 52.1 y 3 (artículo 76.1.a).
b) La exclusión o eliminación de bienes del Patrimonio Documental y Bibliográfico que contravenga lo dispuesto en el artículo 55 (artículo 76.1.j).

Estas infracciones pueden ser sancionadas con multas de hasta 601.012,10 euros, lo que refleja la gravedad de las acciones que pongan en riesgo la preservación del patrimonio documental en el ámbito público. Además, el apartado 2 del artículo 76 señala que, cuando la lesión al Patrimonio Histórico Español ocasionada por estas infracciones sea valorable económicamente, se impondrá una multa que oscile entre el tanto y el cuádruplo del valor del daño causado.

El artículo 76 evidencia que las sanciones no se limitan al ámbito de la protección de datos, sino que también abarcan la gestión de documentos que forman parte del patrimonio cultural. Esta dualidad normativa refuerza la necesidad de una gestión documental integral en las Administraciones Públicas, que garantice el cumplimiento tanto de los principios de

conservación establecidos por la Ley 16/1985 como de los principios de limitación del plazo de conservación recogidos en el RGPD.

Esta situación pone de manifiesto la importancia de una regulación clara que permita compaginar las normas aplicables mediante criterios objetivos, evitando decisiones subjetivas que puedan comprometer tanto la conservación como la eliminación adecuada de la documentación en el sector público.

Así se complementa el marco sancionador aplicable a las AAPP, reflejando la complejidad normativa en la que se enmarca la gestión de la conservación y eliminación documental en el sector público. La aplicación rigurosa de estas normativas no solo busca garantizar el cumplimiento legal, sino también preservar el patrimonio documental, garantizar la transparencia y proteger los derechos de acceso a la información de los ciudadanos.

5. Conclusiones.

El presente trabajo analiza los desafíos que enfrentan las Administraciones Públicas en la gestión de la supresión y conservación de datos personales, poniendo de manifiesto la complejidad que supone la coexistencia de normativas de protección de datos, transparencia, archivos y patrimonio documental. Esta superposición normativa condiciona significativamente el cumplimiento de obligaciones como el derecho de supresión y el principio de limitación del plazo de conservación, y plantea la necesidad de soluciones que equilibren la protección de los derechos de los ciudadanos con las obligaciones legales de conservación documental.

A continuación, se presentan las principales conclusiones:

Primera.- Este trabajo aborda una problemática clave en el ámbito público: la gestión de la supresión y conservación de datos en las Administraciones Públicas en un marco normativo complejo. La coexistencia de normativas de protección de datos, transparencia, archivos y patrimonio documental limita significativamente el alcance del derecho de supresión, priorizando obligaciones de conservación que reflejan el interés público, la trazabilidad administrativa y la protección del patrimonio documental. Este enfoque integral pone de manifiesto las tensiones normativas que enfrentan las AAPP y resalta la necesidad de armonizar estas disposiciones para garantizar un equilibrio adecuado entre los derechos de privacidad y las responsabilidades legales de conservación.

Segunda.- En el sector público, el derecho de supresión a solicitud del interesado se encuentra sujeto a tantas excepciones que, en la mayoría de los casos, la petición será denegada. Esto se debe a que las Administraciones Públicas actúan bajo competencias públicas y obligaciones legales que justifican la conservación de datos de los datos. Esta situación lleva a cuestionarse si un ciudadano puede, en la práctica, ejercer realmente su derecho de supresión en sus relaciones con la Administración Pública. Este hecho no solo limita el alcance de los derechos individuales reconocidos por el RGPD, sino que también plantea importantes retos sobre cómo garantizar el equilibrio entre las necesidades colectivas del sector público y la privacidad de los ciudadanos.

Tercera.- El cumplimiento del principio de limitación del plazo de conservación en las Administraciones Públicas es complejo debido a la diversidad de normativas aplicables. Mientras que el RGPD establece limitar la conservación de datos personales, las obligaciones específicas impuestas por normativas sectoriales como las de archivos, transparencia y patrimonio documental dificultan su cumplimiento y promueven la no eliminación. Esta variedad normativa no solo genera tensiones en la gestión de datos, sino que también evidencia la necesidad de establecer criterios más claros y homogéneos que permitan a las AAPP equilibrar las obligaciones de conservación con el respeto al principio de limitación del plazo de conservación. Sin este marco armonizado, se corre el riesgo de que las decisiones sobre la conservación y eliminación de datos sigan siendo inconsistentes y arbitrarias.

Cuarta.- Este trabajo destaca las profundas diferencias entre el sector público y el privado en la gestión de la supresión y conservación de datos. En el sector público, las normativas específicas, como las de transparencia, archivos y patrimonio documental, condicionan significativamente las decisiones, mientras que, en el sector privado, el RGPD actúa como la principal normativa aplicable, con menos restricciones externas. Además, las sanciones económicas establecidas en el RGPD, aplicables al sector privado, generan un incentivo real para el cumplimiento normativo, algo que no ocurre en el ámbito público debido a la ausencia de multas económicas. Este contraste plantea una reflexión crítica: mientras que en el sector privado la normativa está orientada principalmente a proteger los derechos individuales de los ciudadanos, en el sector público, las obligaciones legales condicionan el ejercicio de estos derechos. Estas diferencias subrayan la necesidad de enfoques normativos diferenciados para cada sector, pero también la importancia de buscar soluciones que incentiven el cumplimiento en el sector público sin que ello repercuta en los recursos de los ciudadanos.

Quinta.- Aunque las Administraciones Públicas están limitadas en su capacidad para suprimir datos personales debido a las obligaciones legales de conservación impuestas por normativas específicas, sí realizan procesos de eliminación documental. Sin embargo, estos no están motivados por el cumplimiento de la normativa de protección de datos, como el RGPD, sino por disposiciones sectoriales relacionadas con archivos y registros. Estas normas tienen como prioridad la gestión eficiente del patrimonio documental y el cumplimiento de obligaciones administrativas, pero también contribuyen indirectamente a proteger los derechos de los ciudadanos al garantizar una adecuada organización y eliminación de datos obsoletos. Este

enfoque refleja cómo las normativas sectoriales pueden complementar los principios de protección de datos, incluso cuando sus objetivos primarios son distintos.

Sexta.- Aunque las Administraciones Públicas no suprimen, como norma general, datos en virtud de la normativa de protección de datos, pueden adoptar medidas significativas para proteger la privacidad de los ciudadanos, como limitar la accesibilidad de datos personales en páginas web, boletines oficiales y otras plataformas digitales. Estas acciones, vinculadas al derecho al olvido, permiten equilibrar las obligaciones legales de conservación con la protección de los derechos de los interesados, contribuyendo a minimizar riesgos de *hiperaccesibilidad* y reforzando la confianza ciudadana en la gestión de datos públicos. Este enfoque es especialmente relevante porque aporta una solución práctica que no contradice las normativas de conservación específicas, pero que sí contribuye a garantizar que los ciudadanos mantengan cierto control sobre la exposición de sus datos personales en el entorno público.

Séptima.- Las nuevas tecnologías ofrecen oportunidades significativas para mejorar la gestión de datos en las Administraciones Públicas, pero también plantean retos en su integración con las normativas de protección de datos. Entre ellas, el blockchain destaca por su capacidad para garantizar la trazabilidad y la seguridad de la información, aunque su aparente naturaleza de inmutabilidad dificulta la supresión de datos personales. Este trabajo resalta que, mediante la implementación de medidas técnicas y legales adecuadas, el uso del blockchain puede adaptarse para cumplir con los principios del RGPD, incluyendo el derecho de supresión, sin comprometer su funcionalidad principal. Este enfoque refleja cómo la innovación tecnológica, bien regulada, puede contribuir a una gestión documental más eficiente y a la vez proteger los derechos de los ciudadanos.

Octava.- Este trabajo pone de manifiesto la necesidad urgente de que el sector público cuente con un marco normativo más claro y cohesivo en materia de gestión documental, que permita integrar de manera efectiva los principios de protección de datos con las obligaciones de trazabilidad y conservación documental propias de las Administraciones Públicas. Una regulación que armonice estas dimensiones no solo facilitaría la eliminación de documentación obsoleta de forma más objetiva y menos sujeta a interpretaciones subjetivas,

sino que también garantizaría el equilibrio entre la protección de los derechos de los ciudadanos y la preservación del patrimonio documental y la transparencia administrativa.

Este enfoque normativo integral resulta fundamental para asegurar que las decisiones sobre la conservación y eliminación de datos se tomen de manera coherente, evitando arbitrariedades y fortaleciendo la confianza de los ciudadanos en la capacidad de las AAPP para gestionar sus datos de manera responsable. Solo a través de esta armonización normativa será posible afrontar los retos actuales, respetar los derechos individuales y, al mismo tiempo, mantener la traza documental imprescindible para el adecuado funcionamiento del sector público.

Novena.- Finalmente, ante la falta de una respuesta normativa clara sobre la supresión de datos en las Administraciones Públicas, se hace imprescindible valorar si la solución debe ser de alcance europeo, nacional o una combinación de ambos. Una modificación del RGPD podría proporcionar una mayor homogeneidad en el tratamiento de los datos dentro de la UE, garantizando coherencia y seguridad jurídica en todos los Estados miembros. Sin embargo, una regulación específica a nivel nacional también tiene sentido, pues permitiría adaptar la normativa a las particularidades del ordenamiento jurídico español, integrando de manera más efectiva disposiciones sobre transparencia, patrimonio documental y archivos. La opción más adecuada podría ser una combinación de ambos enfoques: un marco armonizado desde la Unión Europea, que establezca principios generales sobre conservación y supresión de datos en el sector público, complementado por una normativa nacional detallada que regule su implementación en España. Este enfoque garantizaría un equilibrio entre la protección de datos y las obligaciones administrativas, asegurando que las Administraciones Públicas gestionen los datos de manera responsable y conforme a los principios de la legalidad, transparencia y eficiencia.

Referencias bibliográficas

Bibliografía básica

APARICIO SALOM, J. «Derechos de los interesados (Arts. 12-19 RPGD. Arts. 11-16 LOPDGDD)», 345-395. En: LÓPEZ CALVO, J. (coord.). *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGD*. 2ª ed. Madrid: Wolters Kluwer España, 2019.

HERNÁNDEZ PEÑA, JC. «Protección de datos personales», 237-247. En: VALPUESTA GASTAMINZA, E y HERNÁNDEZ PEÑA, JC. (coord.). *Tratado de Derecho Digital*. 1ª ed. Madrid: Wolters Kluwer España, 2021.

LÓPEZ CALVO, J. La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGD. 2ª ed. Madrid: Wolters Kluwer España, 2019.

VALPUESTA GASTAMINZA, E y HERNÁNDEZ PEÑA, JC. (coord.). Tratado de Derecho Digital. 1ª ed. Madrid: Wolters Kluwer España, 2021.

Bibliografía complementaria

E. GARCÍA DE ENTERRÍA, E. La lengua de los Derechos. La formación del Derecho Público europeo tras la Revolución Francesa, Alianza Universidad, Madrid, 1994.

Revista electrónica

FERNÁNDEZ RAMOS, S. «Las infracciones relativas al ejercicio del derecho de acceso a la información pública. Revista Española de la Transparencia». Primer semestre 2020, número 10, páginas 19-20. ISSN 2444-2607 [consulta: 7 de febrero de 2024]. Disponible en: file:///C:/Users/bfdelgado/Downloads/Dialnet-LasInfraccionesRelativasAlEjercicioDelDerechoDeAcc-7591721.pdf

Legislación citada

REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). *Diario Oficial de la Unión Europea*, 4 de mayo de 2016. Disponible en: https://www.boe.es/doue/2016/119/L00001-00088.pdf

Constitución Española. Boletín Oficial del Estado, 29 de diciembre de 1978, núm. 311. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1978-31229

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. *Boletín Oficial del Estado*, 6 de diciembre de 2018, núm. 294. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673

Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. *Boletín Oficial del Estado*, 24 de noviembre de 1995, núm. 281. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444

Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español. *Boletín Oficial del Estado*, 29 de junio de 1985, núm. 155. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1985-12534

Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno. *Boletín Oficial del Estado*, 10 de diciembre de 2013, núm. 295. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2013-12887

Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica. *Boletín Oficial del Estado*, 15 de noviembre de 2002, núm. 274. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2002-22188

Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. *Boletín Oficial del Estado*, 2 de octubre de 2015, núm. 236. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2015-10565&p=20241106&tn=1#a17

Ley 21/2000, de 29 de diciembre, sobre los derechos de información concernientes a la salud y la autonomía del paciente, y la documentación clínica. *Boletín Oficial del Estado*, 2 de febrero de 2001, núm. 29. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-2001-2353

Ley 14/2007, de 3 de julio, de Investigación biomédica. *Boletín Oficial del Estado*, 4 de julio de 2007, núm. 159. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2007-12945

Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo. *Boletín Oficial del Estado*, 29 de abril de 2010, núm. 103. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2010-6737&p=20230629&tn=1#a25

Ley 6/1991, de 19 de abril, de Archivos y del Patrimonio Documental de Castilla y León. *Boletín Oficial del Estado*, 5 de junio de 1991, núm. 134. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-1991-14132

Ley 6/2023, de 30 de marzo, de Archivos y Documentos de la Comunidad de Madrid. *Boletín Oficial del Estado*, 4 de julio de 2023, núm. 158. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2023-15468

Ley 10/2001, de 13 de julio, de Archivos y Documentos de Cataluña. *Boletín Oficial del Estado*, 28 de agosto de 2001, núm. 206. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2001-16691

Ley 19/2002, de 24 de octubre, de Archivos Públicos de Castilla-La Mancha. *Boletín Oficial del Estado*, 17 de diciembre de 2002, núm. 301. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-2002-24540

Ley 5/2022, de 23 de junio, de Gestión Documental Integral y Patrimonio Documental de la Comunidad Autónoma del País Vasco. *Boletín Oficial del Estado*, 28 de julio de 2022, núm. 180. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2022-12587

Ley 7/2014, de 26 de septiembre, de archivos y documentos de Galicia. *Boletín Oficial del Estado*, 24 de octubre de 2014, núm. 258. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2014-10825

Ley 7/2011, de 3 de noviembre, de Documentos, Archivos y Patrimonio Documental de Andalucía. *Boletín Oficial del Estado*, 28 de noviembre de 2011, núm. 286. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2011-18654

Real Decreto 1164/2002, de 8 de noviembre, por el que se regula la conservación del patrimonio documental con valor histórico, el control de la eliminación de otros documentos de la Administración General del Estado y sus organismos públicos y la conservación de documentos administrativos en soporte distinto al original. *Boletín Oficial del Estado*, 15 de

noviembre de 2002, núm. 274. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-2002-22192

Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. *Boletín Oficial del Estado*, 4 de mayo de 2022, núm. 106. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2022-7191

Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. *Boletín Oficial del Estado*, 4 de mayo de 2022, núm. 106. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2022-7191

Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica. *Boletín Oficial del Estado*, 29 de enero de 2010, núm. 25. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2010-1331

Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso. *Boletín Oficial del Estado*, 25 de noviembre de 2011, núm. 284. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2011-18541.

Real Decreto 2598/1998, de 4 de diciembre, por el que se aprueba el Reglamento de Archivos Militares. *Boletín Oficial del Estado*, 19 de diciembre de 1998, núm. 303. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1998-29347.

Resolución de 28 de junio de 2012, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Norma Técnica de Interoperabilidad de Política de gestión de documentos electrónicos. *Boletín Oficial del Estado*, 26 de julio de 2012, núm. 178. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2012-10048

Jurisprudencia referenciada

Sentencia Tribunal de Justicia (Gran Sala), de 13 de mayo de 2014, C-131/12, ECLI:EU:C:2014:317.

Otros

Resolución núm. R/00750/2022 de la Agencia Española de Protección de Datos, Expediente núm. EXP202204488, de 8 de agosto de 2022. Disponible en: https://www.aepd.es/documento/pd-00133-2022.pdf

Informe núm. 2018-0175 de la Agencia Española de Protección de Datos de 19 de noviembre de 2018. Disponible en: https://www.aepd.es/documento/2018-0175.pdf

Informe N/REF: 022147/2019 de la Agencia Española de Protección de Datos de 20 de febrero de 2020. Disponible en: https://www.aepd.es/documento/2019-0074.pdf

Informe N/REF: 00148/2019 de la Agencia Española de Protección de Datos, de 9 de diciembre de 2020. Disponible en: https://www.aepd.es/documento/2019-0148.pdf

Prueba de concepto. Blockchain y el derecho de supresión de la Agencia Española de Protección de Datos, de noviembre de 2024. Disponible en: https://www.aepd.es/guias/nota-tecnica-blockchain.pdf

Dictamen 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE, Grupo de trabajo sobre protección de datos del artículo 29, Adoptado el 9 de abril de 2014. Disponible en: https://www.aepd.es/documento/wp217_es_interes_legitimo.pdf

Prueba de concepto Blockchain y el derecho de supresión. Noviembre 2024. Disponible en: https://www.aepd.es/guias/nota-tecnica-blockchain.pdf

Informe 2/2018 de la Comisión de Garantía de Acceso a la Información Pública (GAIP) de Cataluña sobre el Proyecto de orden CLT/ /2018 por la cual se aprueban, se modifican y se derogan las tablas de avaluación y acceso documental, de 19 de octubre de 2018. Disponible en: https://www.gaip.cat/es/detall/normativa/Informe_2018_02

Informe 1/2016 de la Comisión de Garantía de Acceso a la Información Pública (GAIP) de Cataluña sobre el Proyecto de Orden CLT / / 2016 por la que se aprueban, se modifican y se derogan tablas de evaluación y acceso documental, de 28 de enero de 2016. Disponible en: https://www.gaip.cat/es/detall/normativa/Informe_2016_01

Aplicaciones de Blockchain en el Sector Público, del Observatorio Público IECISA, 2018. Disponible en: https://www.ospi.es/export/sites/ospi/documents/informes/IECISA_Informe_Blockchain-version-final-online.pdf

Report of the work undertaken by the ChatGPT Taskforce, del Comité Europeo de Protección de Datos de 23 de mayo de 2024. Disponible en: https://www.edpb.europa.eu/system/files/2024-05/edpb_20240523_report_chatgpt_taskforce_en.pdf

Páginas web consultadas

«Formulario de solicitud de retirada de datos personales». Google. 3 noviembre 2024, 17:00. Disponible en: https://reportcontent.google.com/forms/rtbf

«Legitimate interests». Information Commissioner's Office, ICO. 3 noviembre 2024, 16:30. Disponible en: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/lawful-basis-for-processing/legitimate-interests/

«Registro de actividades de tratamiento de la Secretaría de Estado de Defensa». Sede Electrónica Central del Ministerio de Defensa. Tablón de anuncios. 1 noviembre 2024, 21:00. Disponible en: https://sede.defensa.gob.es/acceda/tablon/descargarfichero?id=604

«Buscador de actividades de tratamiento de datos personales de la Comunidad de Madrid». Comunidad de Madrid. 1 noviembre 2024, 20:30. Disponible en: https://www.comunidad.madrid/info/rgpd?f[0]=consejeria_path:Consejer%C3%ADa%20de%20Digitalizaci%C3%B3n

«Protección de Datos. Actividades de Tratamiento del Servicio de Información y Administración Electrónica». Ayuntamiento de Valladolid. 1 noviembre 2024, 20:30. Disponible en: https://www.valladolid.es/es/temas/hacemos/proteccion-datos-actividades-tratamiento-servicio-informaci

«Inventario de actividades de tratamiento de la AEPD». Agencia Española de Protección de Datos. 1 noviembre 2024, 20:30. Disponible en: https://www.aepd.es/la-agencia/transparencia/informacion-en-materia-de-proteccion-de-datos/inventario-actividades-tratamiento-aepd

«Documentos Administrativos». Punto de Acceso General electrónico: tu punto de acceso a las Administraciones Públicas. 15 diciembre 2024, 10:00. Disponible en: https://administracion.gob.es/pag_Home/espanaAdmon/Publicaciones-oficiales-y-documentos-administrativos/Documentos-Administrativos-basica.html

«Plazos de conservación de los documentos generados por las Administraciones Públicas». El consultor de los Ayuntamientos. 16 diciembre 2024, 19:00. Disponible en: https://elconsultor.laley.es/Content/Documento.aspx?params=H4sIAAAAAAAEAMtMSbENCDIAAVMTCyNDtbLUouLM_DxbIwNDS0MjA2O1vPyU1BAXZ9vSvJTUtMy81BSQksy0Spf85JDKglTbtMSc4lS11KT8_GwUk-LhJpQkJhX7ZBaX2HoACcd0t_yiXFUjE1XzZN_UvFI_IC-x2CmxODM5sRgoDADUtSKPkQAAAA==WKE

«Destrucción de documentos y transparencia: ¿criterios más allá de la retórica?». El consultor de los Ayuntamientos. 16 diciembre 2024, 10:00. Disponible en: https://elconsultor.laley.es/Content/Documento.aspx?params=H4sIAAAAAAAEAFWMsQ7CIBRFv6bMlDbBhUFLjIM6sZtXeBhiC4YHJv176WLiHW5yT25OcE5pw1vEOMj-wD6YKaSoBO8lH8TIYnJo9KRqdOhDRLdfgt90smZ7o_KwEDKcU3r9mR4_Q4GZroGKurQ6Ps8pr50YeSftDWO9twl0AgoWaOfMLghZQ8EJFowOsjK54hdCpA7yqgAAAA==WKE

«Administraciones Públicas sancionadas por no responder a requerimientos y por incumplimiento de medidas». Agencia Española de Protección de Datos. 18 de diciembre de 2024. Disponible en: https://www.aepd.es/areas-de-actuacion/administraciones-publicas/administraciones-publicas-sancionadas

Listado de abreviaturas

AAPP: Administraciones Públicas.

AEPD: Agencia Española de Protección de Datos.

AGE: Administración General del Estado.

ENI: Esquema Nacional de Interoperabilidad.

ENS: Esquema Nacional de Seguridad.

ICO: Information Commissioner's Office.

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

LOPDGDD: Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

LPH: Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español.

RAT: Registro de actividades de tratamiento.

RGPD: REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.