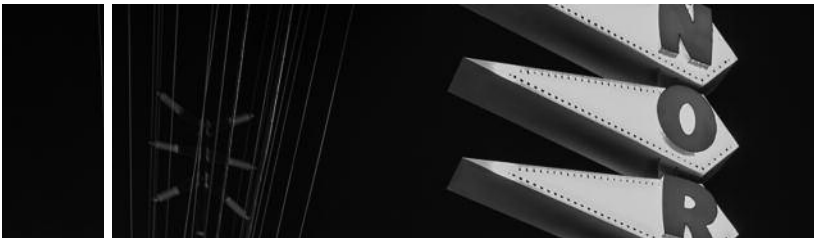

SECURITY
CAMERAS
IN USE



JOSÉ LUIS DOMÍNGUEZ ÁLVAREZ

Interoperabilidad administrativa y protección de datos personales:

claves para garantizar el derecho a una buena Administración

Administrative interoperability and personal data protection:

keys to guarantee the right to good Administration

José Luis Domínguez Álvarez[1]
jldoal@usal.es
Universidad de Salamanca

Citación: Domínguez Álvarez, José Luis (2019). "Interoperabilidad administrativa y protección de datos personales: claves para garantizar el derecho a una buena administración". *Tábula,* n. 22, pp. 95-112

Recibido: 23-9-2019. Aceptado: 13-11-2019

Resumen analítico / Analitic summary

El estudio sistemático de la implementación de la administración electrónica lleva aparejado de forma inherente el análisis exhaustivo de una serie de elementos imprescindibles para conseguir potenciar, de forma efectiva, la digitalización de las estructuras y procedimientos administrativos. En este sentido, la interoperabilidad administrativa se plantea como uno de los principales retos de la gestión administrativa del siglo XXI, en tanto en cuanto constituye el motor de la administración electrónica y una herramienta esencial para reducir el flujo de datos personales de la ciudadanía en manos de las Administraciones públicas, presupuesto indispensable no sólo para el cumplimiento escrupuloso de la nueva regulación en materia de datos personales, sino también para el despliegue de la administración automatizada, presidida por el empoderamiento de los algoritmos y el crecimiento exponencial del tratamiento de datos de carácter personal.

INTEROPERABILIDAD ADMINISTRATIVA | PROTECCIÓN DE DATOS PERSONALES | BUENA ADMINISTRACIÓN | SEGURIDAD | DIGITALIZACIÓN

The systematic study of the implementation of electronic administration inherently entails the exhaustive analysis of a series of essential elements to effectively enhance the digitalization of administrative structures and procedures. In this sense, administrative interoperability is considered as one of the main challenges of the administrative management of the 21st century, insofar as it constitutes the engine of electronic administration and an essential tool to reduce the flow of personal data of citizenship in the hands of the Public Administrations, indispensable budget not only for scrupulous compliance with the new regulation on personal data, but also for the deployment of automated administration, chaired by the empowerment of algorithms and the exponential growth of the treatment of Personal data.

ADMINISTRATIVE INTEROPERABILITY | PERSONAL DATA PROTECTION | GOOD ADMINISTRATION | SECURITY | DIGITALIZATION

La proclamación de la Carta de los Derechos Fundamentales de la Unión Europea, y con ello del derecho a la buena administración, pretendía traer consigo una transformación sin precedentes tanto de las categorías tradicionales del Derecho administrativo como de la propia concepción de las Administraciones públicas. La novedosa regulación en materia de protección de datos de carácter personal, fruto de la preocupación del legislador europeo por limitar los efectos perniciosos que el proceso de digitalización y datificación de la sociedad puede representar para la dignidad y libertad de la ciudadanía, exige hoy realizar una nueva lectura de ese derecho a la buena administración a la luz de estos profundos cambios normativos.

En este sentido, se hace necesario que las Administraciones públicas redoblen los esfuerzos destinados a maximizar los estándares de seguridad de la información que obra en su poder, y especialmente en aquellos casos en los que dicha información pública contenga datos personales, ya que la protección de datos de carácter personal debe constituir, sin lugar a dudas, uno de los presupuestos indispensables para alcanzar el derecho a la buena administración.

Sin embargo, esta tarea de maximización de los estándares de protección de los datos personales, lejos de presentarse como un quehacer sencillo, puede convertirse en un auténtico quebradero de cabeza para buena parte de las Administraciones públicas españolas. En las siguientes líneas, se pretende hacer una pequeña incursión en las estribaciones de esta difícil problemática, planteando algunas respuestas que pueden contribuir a mejorar la seguridad de la información, el correcto tratamiento de los datos personales y la eficacia administrativa, soluciones entre las que destaca por su extraordinaria importancia, el impulso decidido de la interoperabilidad administrativa.

Una revisión del derecho a la buena administración a la luz de la nueva regulación en materia de protección de datos de carácter personal

El 7 de diciembre del año 2000 tiene lugar la proclamación de la Carta de los Derechos Fundamentales de la Unión Europea, Carta que está llamada a ser la positivación de los principios generales del derecho comunitario (RODRÍGUEZ DÍAZ, 2001).

Proclamada en el Consejo Europeo de Niza, la Carta es un texto atípico (MARTÍN-RETORTILLO BAQUER, 2008) al que el Tratado de Lisboa otorga el mismo valor jurídico que los Tratados. Dicho texto consta de un Preámbulo y 54 artículos comprendidos en siete Capítulos estructurados en siete grandes rúbricas: Dignidad, Capítulo I –artículos 1 a 5–; Libertades, Capítulo II –artículos 6 a 19–; Igualdad, Capítulo III –artículos 20 a 26–; Solidaridad, Capítulo IV –artículos 27 a 38–; Ciudadanía, Capítulo V –artículos 39 a 46–; Justicia, Capítulo VI –artículos 47 a 50–; y Disposiciones generales, Capítulo VII –artículos 51a 54–, referidas al ámbito de aplicación de la Carta, el alcance de los derechos reconocidos, el nivel de protección y la prohibición del abuso de derecho (CARRILLO SALCEDO, 2001).

Aproximándonos al objeto de nuestro estudio, la Carta de Niza supuso la positivización de un novedoso derecho, el derecho a la buena administración –artículo 41–, cuya importancia estriba en que supone de facto un replanteamiento del derecho administrativo en su conjunto. En este sentido, algunos teóricos señalan que el derecho a la buena administración viene a exigir una nueva formulación del Derecho administrativo y sus principales categorías, al objeto de convertir a la ciudadanía –y la participación activa de ésta– en el centro gravitacional de la nueva concepción del sistema del Derecho administrativo (RODRÍGUEZ-ARANA, 2013).

En efecto, tal y como señala el profesor RODRIGUEZ-ARANA, la buena administración –también conocido como el buen gobierno–, aspira a colocar en el centro del sistema a la persona y sus derechos fundamentales (RODRÍGUEZ-ARANA, 2006). Otros teóricos señalan en cambio que el principio de buena administración responde a las concepciones más recientes del Derecho administrativo, caracterizadas por el intento de superar la visión estrictamente formal que legitima la Administración para el mero cumplimiento neutral y objetivo de la norma que le otorga las potestades de actuación y, por otro lado, por la voluntad de situar al ciudadano en el centro de la preocupación de las normas que ordenan la actividad administrativa (SANZ LARRUGA, 2009).

A grandes rasgos, cuando nos referimos a la buena administración, estamos haciendo alusión a aquella que cumple con las funciones que le son otorgadas en

democracia. Es decir, una Administración pública que sirve objetivamente a la ciudadanía, que realiza su trabajo con racionalidad, justificando sus actuaciones y que se orienta continuamente al interés general. Un interés general que en el Estado social y democrático de Derecho no puede concebirse de otra forma que no sea la mejora permanente e integral de las condiciones de vida de las personas (RODRÍGUEZ-ARANA, 2013).

Pero más allá del espíritu inherente de este artículo 41 de la Carta de Niza, el cual estaba concebido con la finalidad de provocar una verdadera catarsis en el seno del Derecho administrativo europeo, el mismo posee una serie de implicaciones en la cuestión que nos ocupa, la mejora de la protección de datos de carácter personal, con la finalidad de mejorar la seguridad de la información en poder de las Administraciones públicas. Y es que, de conformidad con lo establecido en el artículo 21 del Código Europeo de Buena Conducta Administrativa de la Unión Europea –redactado por el Defensor del Pueblo Europeo y aprobado por Resolución del Parlamento Europeo de 6 de septiembre de 2001– se establece el principio del respeto a la vida privada y a la integridad de las personas, es decir a la protección de los datos personales, como corolario del derecho a la buena administración. De esta forma, se establece lo siguiente: «el funcionario que maneje datos personales referentes a un ciudadano respetará la vida privada y la integridad de la persona, de conformidad con las disposiciones del Reglamento (CE) n° 45/2001 del Parlamento Europeo y del Consejo de 18 de diciembre de 2000 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos».

Todo ello nos conduce a señalar la relación de causalidad y proximidad existente entre el derecho a una buena administración y el derecho a la protección de datos de carácter personal. Ciertamente, en nuestra opinión ambos derechos forman parte de un todo indisoluble –que no es otro que satisfacer los intereses generales y mejorar las condiciones de vida de la ciudadanía–, pues parece lógico que para que se cumpla la premisa de disponer de una buena administración es necesario que esta respete escrupulosamente las exigencias establecidas por la nueva regulación en materia de protección de datos, ya que en caso contrario no sólo se estará entrando en contradicción con el contenido del artículo 41 de la Carta de Niza, sino también vulnerando el derecho al honor y la intimidad personal de la ciudadanía.

Nueva regulación en materia de protección de datos de carácter personal: ¿una respuesta a la digitalización de la sociedad?

El derecho a la protección de datos personales constituye una de las grandes aportaciones de la Unión Europea a la esfera internacional en las últimas décadas y una prueba palpable del liderazgo que ha demostrado nuestro continente en la promoción de los valores de paz y tolerancia en defensa de las libertades y derechos fundamentales del individuo (TERRÓN SANTOS & DOMÍNGUEZ ÁLVAREZ, 2019).

En efecto, la protección de la vida privada ha visto transcurrir un periodo de casi tres cuartos de siglo desde su primera formulación teórica por WARREN y BRANDEIS hasta su reconocimiento jurisdiccional en Estados Unidos o su aparición en nuestro ordenamiento jurídico con la promulgación de la Constitución española de 1978. Pese a todo ello, el derecho a la protección de datos se ha asentado en nuestro ordenamiento con una rapidez inusitada teniendo en cuenta sus especiales características morfológicas y la técnica jurisprudencial que ha determinado su nacimiento (MARTÍNEZ MARTÍNEZ, 2007).

Ciertamente, el derecho a la protección de datos personales tiene un largo e intenso recorrido durante la segunda mitad del siglo XIX y la primera década del siglo XXI (ÁLVAREZ HERNANDO, 2018). Si se efectúa una primera aproximación a su evolución histórica, encontramos una serie de antecedentes que destacan con extraordinaria claridad. El primero de esos antecedentes lo encontramos en el artículo 12 de la Declaración Universal de los Derechos Humanos, adoptada y proclamada por la Asamblea General en su resolución 217 A (III), de 10 de diciembre de 1948:

> *«Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques».*

Inmediatamente después, el 4 de noviembre de 1950, tuvo lugar la aprobación del Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales[2], más conocido como la Convención Europea de Derechos Humanos (CEDH), instrumento que tenía como finalidad prioritaria reafirmar la profunda adhesión del Consejo de Europa «a las libertades fundamentales que constituyen las bases mismas de la justicia y de la paz en el mundo, y cuyo mantenimiento reposa esencialmente, de una parte, en un régimen político verdaderamente democrático, y, de otra, en una concepción y un respeto comunes de los derechos humanos de los cuales dependen», también hizo mención

expresa en su artículo octavo al Derecho al respeto a la vida privada y familiar, en los términos que a continuación se expresan:

> *«Artículo 8. Derecho al respeto a la vida privada y familiar»*
>
> *1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.*
>
> *2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria.*

Esta inquietud de las organizaciones supranacionales por el respeto a los derechos de la personalidad, así como por las disfunciones sociales que los nuevos medios tecnológicos pueden producir, tuvo su plasmación por vez primera en el Convenio nº 108 del Consejo de Europa (REBOLLO DELGADO, 2018). Dicha norma constituye no sólo el primer instrumento internacional jurídicamente vinculante en materia de protección de datos, sino también, el punto de partida para afrontar los retos de la automatización desde el reconocimiento de un derecho a la protección de datos, derecho que vino a ser reforzado con posterioridad por la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre en 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Sin embargo, la vertiginosa evolución tecnológica y la globalización han planteado la necesidad de acometer importantes cambios normativos, una modernización sin precedentes en aras de ofrecer un enfoque global que garantice el pleno respeto no solo del derecho fundamental a la protección de datos personales sino, también, de la dignidad humana ante los riesgos y amenazas de la realidad digital (PÉREZ LUÑO, 2012).

En este sentido, el Diario Oficial de la Unión Europea, publicaba el 4 de mayo de 2016 el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en adelante RGPD). En esencia, la reforma pretende devolver a los ciudadanos el control de sus datos personales y garantizar en todo el territorio de la Unión Europea unos elevados estándares de protección, adaptados al entorno digital (DAVARA RODRÍGUEZ, 2016). Esta idea-fuerza, presente en todo el texto del RGPD, se establece con meridiana claridad desde sus primeros considerandos –especialmente en el considerando cuarto–:

> *«El tratamiento de datos personales debe estar concebido para servir a la humanidad. El derecho a la protección de los datos personales no es un derecho absoluto, sino que debe considerarse en relación con su función en la sociedad y*

mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad. El presente Reglamento respeta todos los derechos fundamentales y observa las libertades y los principios reconocidos en la Carta conforme se consagran en los Tratados, en particular el respeto de la vida privada y familiar, del domicilio y de las comunicaciones, la protección de los datos de carácter personal, la libertad de pensamiento, de conciencia y de religión, la libertad de expresión y de información, la libertad de empresa, el derecho a la tutela judicial efectiva y a un juicio justo, y la diversidad cultural, religiosa y lingüística».

En líneas generales, podemos decir, que el RGPD nace con vocación de erigirse como el instrumento normativo encargado de dar respuesta y solución al tsunami tecnológico en el que se sumerge la sociedad actual (RALLO LOMBARTE & GARCÍA MAHAMUT, 2015). En este sentido, su finalidad no es otra que la de garantizar un nivel uniforme y elevado de protección de las personas físicas, al tiempo que pretende eliminar los obstáculos a la libre circulación de datos personales dentro de la Unión Europea, apostando de forma decidida por el establecimiento de elevados y equivalentes niveles de protección de los derechos y libertades de las personas físicas –en lo que se refiere al tratamiento de dichos datos– en todos los Estados miembros.

En otras palabras, la nueva regulación trata de dar respuesta a la profunda evolución que el derecho a la libertad informática ha experimentado en el continente europeo, lo que ha propiciado el paso de considerar el *habeas data* como un instituto de protección de otros derechos, principalmente la intimidad, a entenderlo como un derecho autónomo e independiente con su propia configuración y lógica interna (FERNÁNDEZ VILLAZÓN, 2016).

Algo similar ocurre con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (en adelante, LOPDGDD), la cual, sin lugar a dudas, constituye un ejemplo palmario de la transformación provocada por la tecnología en la sociedad contemporánea (RALLO LOMBARTE, 2019). Si el derecho a la protección de datos personales sirvió durante las últimas décadas para preservar los derechos individuales frente a buena parte de los efectos generados por las tecnologías de la información y del conocimiento, la sociedad digital en la que nos hallamos completamente inmersos demanda un haz de derechos que se extienda a la práctica totalidad de los ámbitos en que el individuo se desarrolla en sociedad (RALLO LOMBARTE, 2017).

Y es que, de conformidad con lo establecido en el artículo primero de la norma objeto de estudio, observamos que el legislador español confiere un doble objetivo a la LOPDGDD: en primer lugar, adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta

al tratamiento de sus datos personales y a la libre circulación de estos datos, y completar sus disposiciones, y en segundo lugar garantizar los derechos digitales de la ciudadanía conforme al mandato establecido en el artículo 18.4 de la Constitución.

En definitiva, cuando hablamos del RGPD y la LOPDGDD, nos referimos a nuevos instrumentos normativos diseñados con la finalidad de hacer frente a nuevas y vertiginosas realidades, entre las que destacan especialmente la digitalización y la datificación de la sociedad en su conjunto, lo que exige articular nuevas respuestas jurídicas para salvaguardar la integridad y el ejercicio efectivo de los derechos fundamentales de la ciudadanía. El derecho a la protección de datos de carácter personal se presenta, por tanto, como el presupuesto indispensable para garantizar la dignidad humana ante los riesgos y amenazas de la realidad digital, lo que requiere no sólo el compromiso y el cumplimiento de las exigencias normativas en materia de protección de datos por parte de todos los actores –públicos y privados–, sino también la adopción de las medidas pertinentes y necesarias para garantizar en todo momento la minimización de los riesgos en la seguridad de la información, proceso que deberían abanderar de forma diligente las diferentes Administraciones públicas, y para lo cual urge, de una vez por todas, desplegar todo un haz de actuaciones y de herramientas que contribuyan de forma efectiva a lograr la tan ansiada interoperabilidad administrativa, mecanismo idóneo para reducir la proliferación excesiva de datos personales, datos que se presentan como principal activo para las diferentes unidades administrativas en los albores del nuevo paradigma de la Administración pública: la administración automatizada.

Interoperabilidad administrativa como mecanismo idóneo para reducir la proliferación de datos personales

Cuando nos referimos a los principales frenos o resistencias que presentan las Administraciones públicas a la hora de afrontar el proceso de digitalización de la acción administrativa, necesariamente debemos hacer alusión a la falta de confianza imperante entre las diferentes Administraciones públicas, algo extremadamente preocupante en un contexto de patente evolución y ampliación de los procedimientos administrativos desarrollados por medios electrónicos.

1. El impulso del principio «once only»

La cooperación entre las Administraciones públicas es esencial para proporcionar los servicios a los ciudadanos y garantizarles su derecho a relacionarse con ellas por medios electrónicos. Dicha cooperación requiere unas condiciones tales

que permitan que la misma se pueda llevar a cabo con fluidez para lo cual es necesario que haya interoperabilidad (TERRÓN SANTOS & DOMÍNGUEZ ÁLVAREZ, 2019).

La interoperabilidad[3] se presenta, por tanto, como el desafío más importante que se plantea a la gestión administrativa en la primera mitad del siglo XXI. Hace posible que los datos situados en un punto de un sistema (por ejemplo, los que contenga un expediente administrativo electrónico confiado a un concreto órgano administrativo) puedan ser utilizados de manera electrónica por el conjunto de dicho sistema (es decir, por todos los órganos de una misma Administración) y cruzarse asimismo por medios electrónicos para su uso por los interesados y por otras entidades públicas y privadas (GAMERO CASADO, 2009).

En efecto, una vez superada la fase inicial de concienciación acerca de la necesidad de implantar la administración electrónica y sus beneficios, el problema principal para hacer realidad la gestión electrónica es la interoperabilidad; de ahí que sostenga CERRILLO MARTÍNEZ que la interoperabilidad es el motor de la administración electrónica (CERRILLO MARTÍNEZ, 2008).

La interoperabilidad se convierte así en la piedra angular para el impulso de la administración electrónica integral, fruto de esta importancia, el Real Decreto 4/2010, de 8 de enero, establece el Esquema Nacional de Interoperabilidad (en adelante ENI), entendido éste como el conjunto de criterios y recomendaciones en materia de seguridad, normalización y conservación de la información, que deberán ser tenidos en cuenta por las Administraciones públicas para la toma de decisiones tecnológicas que garanticen la interoperabilidad[4].

Ahora bien, conviene señalar que el ENI se puso en marcha a la luz del estado del arte y tomando como principal referencia las actuaciones puestas en marcha previamente en los países de nuestro entorno más próximo[5]. De esta forma, el ENI se encuentra alineado con la Estrategia Europea de Interoperabilidad[6] y el Marco Europeo de Interoperabilidad, lo que permite que tanto el ENI, como sus normas técnicas de interoperabilidad, contemplan de manera sistemática el enlace con instrumentos equivalentes del ámbito europeo.

Entre los principales objetivos perseguidos por el Esquema Nacional de Interoperabilidad podemos destacar los siguientes:

- Comprender los criterios y recomendaciones que deberán ser tenidos en cuenta por las Administraciones públicas para la toma de decisiones tecnológicas que garanticen la interoperabilidad que permita el ejercicio de derechos y el cumplimiento de deberes a través del acceso electrónico a los servicios públicos, a la vez que redunda en beneficio de la eficacia y la eficiencia, evitando la discriminación a los ciudadanos por razón de su elección tecnológica.

- Introducir los elementos comunes que han de guiar la actuación de las Administraciones públicas en materia de interoperabilidad.
- Aportar un lenguaje común para facilitar la interacción de las Administraciones públicas, así como la comunicación de los requisitos de interoperabilidad a la industria.

No debemos olvidar que la interoperabilidad se concibe desde una perspectiva integral, de manera que no caben actuaciones puntuales o tratamientos coyunturales, debido a que la debilidad de un sistema determina su punto más frágil y, a menudo, este punto es la coordinación entre medidas individualmente adecuadas, pero deficientemente ensambladas. Por ello, apostar por la mejora paulatina de la interoperabilidad administrativa es esencial desde el punto de vista de los procesos de impulso y desarrollo de la administración electrónica, ya que no solamente es imprescindible para la correcta extensión del proyecto de digitalización de la acción administrativa, sino también desde la perspectiva de la protección de datos. La interoperabilidad es el motor de la administración electrónica y el vehículo adecuado para reducir la proliferación de datos de carácter personal en un contexto dominado por el tratamiento masivo de datos a través de internet (TERRÓN SANTOS & DOMÍNGUEZ ÁLVAREZ, 2019).

Justamente, la Administración electrónica, en esencia, conlleva de forma intrínseca el impulso de los procesos de simplificación administrativa. Esto significa suprimir trámites redundantes o innecesarios, reducir la documentación que se exige a los ciudadanos –especialmente aquellos documentos que ya tenga la Administración y que se pueden obtener a través de la interconexión de registros administrativos–, implantar bases generales de procedimientos y plazos únicos y la instauración progresiva del silencio positivo como regla general. Todo ello permite una gestión administrativa más rápida y más clara (TRONCOSO REIGADA, 2008).

Esta idea de simplificación administrativa ligada a la supresión de trámites innecesarios y a la reducción de la documentación exigida a la ciudadanía no es novedosa. La propia Ley 30/1992, de 26 de noviembre, del Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (LRJPAC) pretendía de manera ambiciosa modernizar la gestión de la Administración pública, simplificando la necesidad de aportar documentos que se encontraran ya en poder de la Administración. Así, reconoce el derecho de los ciudadanos en sus relaciones con las Administraciones públicas «a no presentar documentos no exigidos por las normas aplicables al procedimiento de que se trate o que ya se encuentren en poder de la Administración actuante» –artículo 35.f)–.

Este mismo precepto –conocido también como principio *once only* (MARTÍN DELGADO, 2017)– se reproduce igualmente en la actual Ley 39/2015, concretamente en el artículo 28.3 LPAC –precepto modificado por la

Disposición final duodécima de la LPDGDD con la finalidad de mejorar la protección de datos de carácter personal en poder de las diferentes Administraciones públicas–, al señalar que *«[…] Las Administraciones no exigirán a los interesados la presentación de documentos originales, salvo que, con carácter excepcional, la normativa reguladora aplicable establezca lo contrario. Asimismo, las Administraciones públicas no requerirán a los interesados datos o documentos no exigidos por la normativa reguladora aplicable o que hayan sido aportados anteriormente por el interesado a cualquier Administración. A estos efectos, el interesado deberá indicar en qué momento y ante qué órgano administrativo presentó los citados documentos, debiendo las Administraciones públicas recabarlos electrónicamente a través de sus redes corporativas o de una consulta a las plataformas de intermediación de datos u otros sistemas electrónicos habilitados al efecto, salvo que conste en el procedimiento la oposición expresa del interesado o la ley especial aplicable requiera su consentimiento expreso. Excepcionalmente, si las Administraciones públicas no pudieran recabar los citados documentos, podrán solicitar nuevamente al interesado su aportación»*.

Esta reciente modificación normativa pone de manifiesto la relevancia que el legislador español confiere a la interoperabilidad administrativa, consciente de que el intercambio de datos entre las diferentes Administraciones públicas constituye un axioma imprescindible, no sólo desde el punto de vista de la prestación de servicios avanzados de administración electrónica a los ciudadanos, sino también como mecanismo idóneo para la reducción de los costes de transacción y la mejora de la eficiencia y la eficacia de las organizaciones.

En este sentido, la Norma Técnica de Interoperabilidad de Protocolos de intermediación de datos, aprobada mediante Resolución de 28 de junio de 2012, de la Secretaría de Estado de Administraciones Públicas, supuso la creación de la *Plataforma de Intermediación de Datos (PID)* del Ministerio de Hacienda y Administraciones Públicas, hoy dependiente del Ministerio de Política Territorial y Función Pública, proyecto concebido en última estancia con la finalidad de facilitar el intercambio de datos entre Administraciones públicas, evitando con ello la solicitud reiterada al ciudadano de aquellos datos que ya obren en poder de la Administración (BARRERA, 2019). La PID permite verificar y consultar los datos de un ciudadano mediante el acceso a los servicios de verificación y consulta de datos (SVD), debiendo en todo momento asegurar la confidencialidad e integridad de la información intercambiada entre las diferentes organizaciones, y no almacenando, en ningún caso, la información personal de ciudadano alguno, derivada de los procesos de transacción de intercambio de datos.

De esta forma, mediante el acceso a los servicios de verificación y consulta de datos de la Plataforma de Intermediación de Datos se permite que cualquier organismo de la Administración, pueda consultar o verificar datos previamente aportados por los ciudadanos o administrados, sin necesidad de solicitar la aportación de los correspondientes documentos acreditativos, permitiendo así hacer

efectiva esta supresión y reduciendo de forma significativa la proliferación de datos personales en las relaciones Administración-administrado. Actualmente en SVD se pueden verificar los siguientes tipos de datos:

- Servicios de Verificación y Consulta de Datos de Identidad (SVDI).
- Servicio de Verificación de Datos de Residencia (SVDR).
- Servicio de Verificación de Datos de Prestación de Desempleo (SVDP).
- Servicio de Verificación de Datos de Títulos Oficiales (SVDT).
- Servicio de Verificación de Datos de la Tesorería General de la Seguridad Social (TGSS).
- Servicio de Verificación de Datos de la Agencia Estatal de Administración Tributaria (AEAT).
- Servicio de Verificación de Datos Catastrales.
- Servicio de Consulta de Nivel y Grado de Dependencia (IMSERSO).
- Servicio de Consulta de Prestaciones Públicas (INSS).
- Servicio de Consulta de Datos del Ministerio de Justicia.
- Servicio de Consulta de entidades aseguradoras y reaseguradoras de la Dirección General de Seguros y Fondos de Pensiones (DGSFP).
- Servicio de Impuesto sobre Actividades Económicas (IAE) Gobierno de Navarra.
- Servicio de Impuesto sobre Actividades Económicas (IAE) Gobierno del País Vasco.
- Servicio de Consulta de Firmas para Legalización Diplomática de Documentos Públicos Extranjeros del Ministerio de Justicia.
- Servicios de Poderes Notariales del Consejo General del Notariado.
- Servicios de MUFACE.
- Servicio del Instituto Cervantes.
- Servicio de la Conferencia de Rectores de las Universidades Españolas (CRUE).

Todos estos servicios, unidos al conjunto de previsiones en materia de seguridad, confidencialidad y privacidad de los datos establecidas en la Resolución de 28 de junio de 2012, de la Secretaría de Estado de Administraciones Públicas, convierten a la Plataforma de Intermediación de Datos en la herramienta idónea para maximizar la protección de los datos personales de la ciudadanía en poder de las Administraciones públicas, siempre y cuando se aseguren las máximas

garantías de seguridad y confidencialidad de las consultas, preservando la privacidad de los datos consultados tanto en el propio intercambio como en el tratamiento posterior de la información obtenida. Para ello, la normativa vigente prevé el establecimiento de controles de autorización, acceso y uso por parte de los usuarios en aras de potenciar el correcto funcionamiento de la interoperabilidad administrativa en nuestro país.

Esta herramienta representa a grandes rasgos el posicionamiento mayoritario de la doctrina administrativista, la cual ha señalado desde un primer momento, la necesidad de establecer una base de datos general radicada, por ejemplo, en la Administración General del Estado (o Comunidad Autónoma en su caso), a la que pudiesen acceder los aplicativos del resto de Administraciones gracias a la debida interoperabilidad; hasta su consecución debería garantizarse, al menos, para dar cumplimiento al principio «*once only*», que todos los datos obrantes en una determinada Administración sean retroalimentados al realizar trámites en un procedimiento posterior al primero (MARTÍN DELGADO, 2017). Esta idea, vista con recelo por quienes enarbolan un férreo discurso en favor de la –malentendida– autonomía de las Comunidades Autónomas, ha supuesto de facto el principal escollo para el establecimiento de un sistema interoperable que propiciara el despliegue efectivo de la administración electrónica en nuestro país, lo que se ha traducido en última instancia en numerosos desvelos para quienes se han visto obligados a relacionarse por medios telemáticos con las Administraciones públicas. Ciertamente, la pluralidad de sistemas y productos informáticos implementados por las diferentes instituciones –especialmente las Comunidades Autónomas– al objeto de desplegar la administración electrónica en sus respectivos territorios, unido al desconocimiento de los elementos indispensables –tanto en términos de eficacia como en términos legales– para garantizar la interoperabilidad administrativa por parte de quienes se erigieron como expertos en el diseño de herramientas y plataformas para el avance de la administración digital, dificulta extraordinariamente la adopción de un modelo eficaz de administra electrónica, algo carente de toda lógica.

Por todo ello, y a pesar de los avances alcanzados en el campo de la interoperabilidad administrativa, la efectividad de ese principio que apuntábamos con anterioridad conocido como «*once only*» sigue pareciendo más una quimera que una realidad tangible próxima a nuestros días. Su puesta en marcha decidida contribuiría de manera significativa a la mejora de la seguridad de la información, al tiempo que reduciría el grado de vulnerabilidad de los datos personales de la ciudadanía en poder de las Administraciones públicas. No podemos más que reafirmarnos en esta tesis, pues parece lógico que una reducción de la documentación exigida por parte de las Administraciones públicas –y ya aportada previamente por el administrado–, llevaría aparejada la consiguiente disminución del riesgo y la vulnerabilidad de los datos personales de la ciudadanía, lo que

redundaría en la realización efectiva del contenido establecido en el artículo 18.4 CE, según el cual, la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos. Esta aspiración loable exige un replanteamiento de las herramientas concebidas por la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios públicos con la finalidad de impulsar la administración electrónica: el Esquema Nacional de Interoperabilidad (ENI) y el Esquema Nacional de Seguridad (ENS); renovación necesaria tanto para afrontar la transformación digital que ha experimentado la sociedad española en la última década, como para preparar el próximo salto cualitativo que se está fraguando ya en el seno de la Administración pública, cuando nos encontramos en los albores de la administración automatizada. Con todo ello, ¿será necesario replantear la estrategia de interoperabilidad y seguridad de las Administraciones públicas?

Conclusiones

El vertiginoso proceso de digitalización y datificación experimentado por la sociedad de su conjunto en los últimos años ha traído consigo la necesidad de acometer importantes y profundas transformaciones del sistema jurídico, todo ello con la finalidad de limitar y minimizar el alcance lesivo que el avance de la tecnología puede suponer para el disfrute efectivo de los derechos fundamentales de la ciudadanía. Consciente de ello, el legislador europeo ha llevado a cabo un ambicioso proceso de modernización y mejora de la regulación en materia de protección de datos de carácter personal, cuyo mayor hito ha sido la adopción del RGPD, o lo que es lo mismo, un auténtico cambio de paradigma en la normativa sobre la materia hasta la fecha. Nuevas obligaciones y exigencias con un horizonte común, crear las condiciones necesarias que garanticen que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. Exigencias y obligaciones a las que, por otro lado, no son ajenas las diferentes Administraciones públicas, las cuales deberían adoptar una posición de liderazgo en la defensa del derecho a la protección de datos de carácter personal, para lo cual resulta indispensable la mejora tanto de las herramientas como de la estrategia de interoperabilidad administrativa –así como la plena eficacia de principios tan manidos como el de «once only»–, cuestión clave para evitar la proliferación innecesaria de datos personales en la relación Administración-ciudadano.

En este sentido, conviene poner en marcha no solo los procedimientos pertinentes de mejora y perfeccionamiento continuado de las herramientas articuladas para promover la interoperabilidad administrativa, sino también implementar la difusión y conocimiento de los mecanismos articulados por la

Administración pública a tal fin, algo para lo que es imprescindible mejorar la formación de los empleados públicos –como principales usuarios de estos instrumentos–, ardua tarea en la que los archiveros están llamados a ser los auténticos protagonistas.

Urge, en definitiva, la puesta en marcha de medidas concretas en el campo de la interoperabilidad que contribuyan de manera significativa a la mejora de la seguridad de la información y a reducir notoriamente el grado de vulnerabilidad de los datos personales de la ciudadanía en poder de las Administraciones públicas, sólo así podrá darse cumplimiento a las previsiones realizadas por la Unión Europea en lo referente al derecho a una buena administración: *el buen gobierno implica necesariamente un tratamiento eficaz de los datos personales de la ciudadanía, principal activo para el correcto funcionamiento de la acción administrativa*.

Bibliografía

Álvarez Hernando, Javier (2018). "Practicum de protección de datos 2018". Pamplona, *Thomson Reuters-Aranzadi,* pág. 48.

Barrera, Jorge (2019). "La plataforma de intermediación de datos". *Consultor de los ayuntamientos y de los juzgados: Revista técnica especializada en administración local y justicia municipal*, núm. 4, págs. 87-104.

Carrillo Salcedo, Juan Antonio (2001). "Notas sobre el significado político y jurídico de la Carta de Derechos Fundamentales de la Unión Europea". *Revista de Derecho Comunitario Europeo*, núm. 9, pág. 12.

Cerrillo Martínez, Agustí (2008). "Cooperación entre Administraciones públicas para el impulso de la administración electrónica", en Gamero Casado y Valero Torrijos (coord.), *La Ley de administración electrónica. Comentario sistemático a la Ley 11/2007, de acceso electrónico de los ciudadanos a los servicios públicos*. Thomson Reuters-Aranzadi, Navarra, pág. 497.

Davara Rodríguez, Miguel Ángel (2016). "Reglamento Europeo sobre protección de datos". *Actualidad administrativa*, núm. 7, pág. 10.

Fernández Villazón, Luis Antonio (2016). "El nuevo Reglamento Europeo de Protección de Datos". *Nueva época,* vol. 19, núm. 1, pp. 395-411.

Gamero Casado, Eduardo (2009) "Interoperabilidad y Administración electrónica: conéctense, por favor". En: *Revista de Administración Pública*, núm. 179, Madrid, págs. 291–332.

Martín Delgado, Isaac (2017). "La reforma de la Administración electrónica: Una oportunidad para la innovación desde el Derecho". Madrid, Instituto Nacional de Administraciones Públicas.

Martínez Martínez, Ricard (2007). "El derecho fundamental a la protección de datos: perspectivas". *IDP: revista de Internet, derecho y política= revista d'Internet, dret i política*, núm. 5, pág. 4.

Martín-Retortillo Baquer, Lorenzo (2008). "Los Derechos Fundamentales en el ámbito de la Unión Europea y su incidencia en España (con especial referencia a la Ley Orgánica 1/2008, de 30 de julio, por la que se autoriza la ratificación del Tratado de Lisboa, de 13 de diciembre de 2007)". *Revista Aragonesa de Administración Pública*, núm. 33, pág. 35.

Pérez Luño, Antonio Enrique (2012). "Los derechos humanos en la sociedad tecnológica". Madrid, Universitas.

Rallo Lombarte, Artemi & García Mahamut, Rosario (2015). *"Hacia un nuevo derecho europeo de protección de datos. Towards a new European Data Protection Regime"*. Valencia, Tirant lo Blanch.

Rallo Lombarte, Artemi (2017). "De la «libertad informática» a la constitucionalización de nuevos derechos digitales (1978-2018)". *Revista de Derecho Político*, núm. 100, págs. 637-667.

Rallo Lombarte, Artemi (2019). "Del derecho a la protección de datos a la garantía de nuevos derechos digitales". En: Rallo Lombarte, Artemi et al. *Tratado de Protección de Datos*. Valencia: Tirant lo Blanch, págs. 23-52.

Rebollo Delgado, Lucrecio (2018). "Protección de datos en Europa. Origen, evolución y regulación actual". Madrid, Editorial Dykinson, pág. 83.

Rodríguez-Arana Muñoz, Jaime. (2006). "El buen gobierno y la buena Administración de las Instituciones Públicas (adaptado a la Ley 5/2006, de 10 de abril)". Cizur Menor, Thomson-Aranzadi.

Rodríguez-Arana Muñoz, Jaime. (2014). "La buena Administración como principio y como derecho fundamental en Europa". *Misión Jurídica, Revista de Derecho y Ciencias Sociales*. núm. 6**,** págs. 23-56.

Rodríguez Díaz, Alonso (2001). "Sobre la naturaleza jurídica de la Carta de Derechos Fundamentales de la Unión Europea". *Revista de Derecho Político*, núm. 51.

Samuel D. Warren & Louis D. Brandeis (1890). "The right to privacy". *Harvard Law Review*. Vol. IV, n.° 5.

Sanz Larruga, J. (2009). El ordenamiento europeo, el derecho administrativo español y el derecho a una buena administración. *Anuario da Facultade de Dereito da Universidade da Coruña*, núm. 13, págs. 729-751.

Terrón Santos, Daniel & Domínguez Álvarez, José Luis (2019). "Nueva regulación de la protección de datos y su perspectiva digital". Granada, Editorial Comares.

Troncoso Reigada, Antonio (2008). "La administración electrónica y la protección de datos personales". *Revista jurídica de Castilla y León*, núm. 16, págs. 31-112.

Notas

[1] Personal Investigador en Formación del Área de Derecho Administrativo de la Universidad de Salamanca |FPU 17/01088 Ministerio de Ciencia, Innovación y Universidades.

[2] El texto del Convenio ha sido modificado tras su aprobación por las disposiciones del Protocolo n° 14 (STCE n° 194) a partir de su entrada en vigor el 1 de junio de 2010. El texto del Convenio fue anteriormente modificado por las disposiciones del Protocolo n° 3 (STE n° 45), que entró en vigor el 21 de septiembre de 1970, del Protocolo n° 5 (STE n° 55), que entró en vigor el 20 de diciembre

de 1971 y del Protocolo nº 8 (STE nº 118), que entró en vigor el 1 de enero de 1990. Incluía asimismo el texto del Protocolo nº 2 (STE nº 4) que, de conformidad con su artículo 5 párrafo 3, formaba parte integrante del Convenio desde su entrada en vigor el 21 de septiembre de 1970. Todas las disposiciones modificadas o añadidas por dichos Protocolos fueron sustituidas por el Protocolo nº 11 (STE nº 155), a partir de la fecha de su entrada en vigor el 1 de noviembre de 1998. Desde esa fecha, el Protocolo nº 9 (STE nº 140), que entró en vigor el 1 de octubre de 1994, quedó derogado y el Protocolo nº 10 (STE nº 146) quedó sin objeto.

[3] El enchufe es un ejemplo rudimentario de interoperabilidad en procesos puramente industriales: la clavija de que disponga un aparato debe ser compatible con la clavija de suministro de corriente a la que vamos a conectarlo, porque en caso contrario no podríamos enchufar el equipo, cosa que no es tan fácil de lograr cuando son muchos los fabricantes y la distribución del producto abarca grandes áreas.

[4] El Esquema Nacional de Interoperabilidad se establece en el artículo 156.1 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, que sustituye al apartado 1 del artículo 42 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

[5] Decisión 2004/387/CE de la Comisión, de 28 de abril de 2004; Decisión 2004/387/CE del Parlamento Europeo y del Consejo, de 21 de abril de 2004, relativa a la prestación interoperable de servicios paneuropeos de administración electrónica al sector público, las empresas y los ciudadanos.

[6] Mediante la Decisión (UE) 2015/2240 del Parlamento Europeo y del Consejo de 25 de noviembre de 2015 por la que se establece un programa relativo a las soluciones de interoperabilidad y los marcos comunes para las administraciones públicas, las empresas y los ciudadanos europeos (programa ISA2) como medio de modernización del sector público la Comisión persigue continuar el esfuerzo del Programa ISA (Soluciones de interoperabilidad para las administraciones públicas europeas) extendiendo la proyección a los ciudadanos y las empresas, con el objetivo de desarrollar, mantener y promover un enfoque holístico hacia la interoperabilidad en la Unión para eliminar la fragmentación en el panorama de la interoperabilidad en la Unión; facilitando una interacción electrónica transfronteriza o intersectorial eficiente y eficaz tanto entre las administraciones públicas europeas como entre ellas y las empresas y los ciudadanos, y contribuir al desarrollo de una administración electrónica más eficaz, simplificada y orientada a los usuarios en los niveles nacional, regional y local de la administración pública; y promoviendo la reutilización de las soluciones de interoperabilidad por parte de las administraciones públicas europeas.


PRIVATE
NATURE
RESERVE