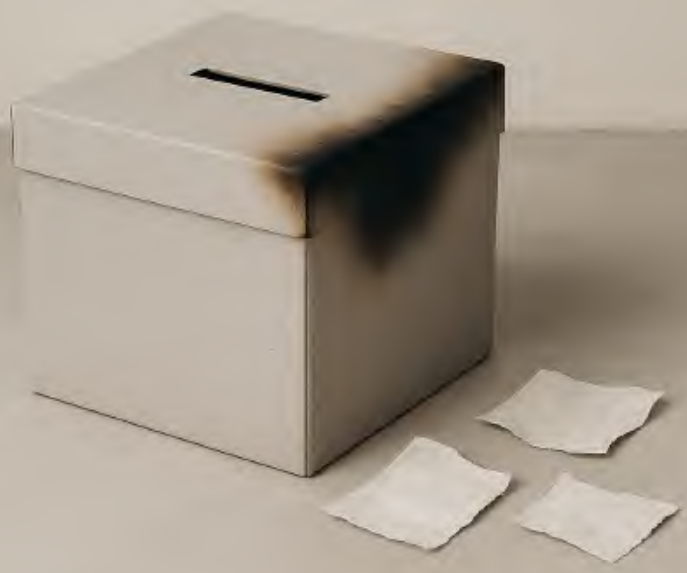
DEMOCRACIA, POLÍTICA Y ADMINISTRACIÓN INTELIGENTES EN TIEMPOS CRÍTICOS

Coordinadores

Gema Sánchez Medero
Oliver Soto Sainz
María José García Solana
Segundo Valmorisco Pizarro
Gema Pastor Albaladejo



COLEX READER
COLEX AUDIO
COLEX

¡Gracias por confiar en nosotros!

La obra que acaba de adquirir incluye de forma gratuita la versión electrónica. Acceda a nuestra página web para aprovechar todas las funcionalidades de las que dispone en nuestro lector.

Funcionalidades eBook

Acceso desde cualquier dispositivo con conexión a internet

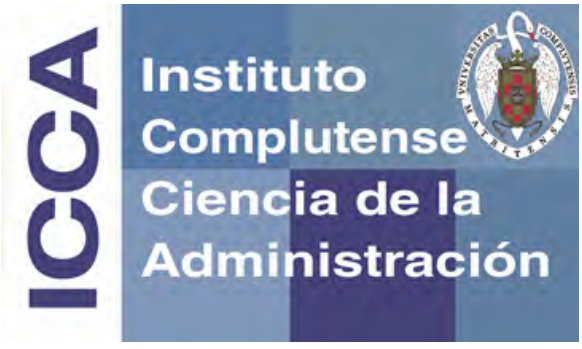
Idéntica visualización a la edición de papel

Navegación intuitiva

Tamaño del texto adaptable

Síguenos en:

DEMOCRACIA, POLÍTICA Y ADMINISTRACIÓN INTELIGENTES EN TIEMPOS CRÍTICOS



DEMOCRACIA, POLÍTICA Y ADMINISTRACIÓN INTELIGENTES EN TIEMPOS CRÍTICOS

Coordinadores

Gema Sánchez Medero
Oliver Soto Sainz
María José García Solana
Segundo Valmorisco Pizarro
Gema Pastor Albaladejo

COLEX 2025

© Editorial Colex, S.L.
Calle Costa Rica, número 5, 3.º B (local comercial)
A Coruña, 15004, A Coruña (Galicia)
info@colex.es
www.colex.es

SUMARIO

LAS MULTAS AL SECTOR PÚBLICO EN PROTECCIÓN DE DATOS: UN ESTUDIO GENERAL[1]

Alejandro Corral Sastre
Universidad Complutense de Madrid

Regina Linden Ruaro
PUCRS/Brasil

1. Introducción

En el año 2016 se aprueba 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). Esta norma de Derecho europeo supone un giro copernicano en la forma de enfrentar la protección del derecho fundamental a la protección de datos en el territorio europeo, es decir, los veintisiete Estados miembros más Noruega, Islandia y Liechtenstein. Y no solo en el territorio de Espacio Económico Europeo (EEE), sino que ha trascendido sus fronteras, convirtiéndose en un modelo de protección de datos para muchos Estados.

El RGPD supone, como se ha apuntado en el párrafo anterior, un cambio en la manera de entender la protección de datos. Se incluyen determinados principios y obligaciones que cambian la concepción y el rol que deben jugar los responsables y encargados de tratamiento entre los que se encuentran, lógicamente, las Administraciones públicas. Así, por poner un ejemplo, el principio de responsabilidad proactiva recogido en el artículo 24.1 de la norma y por el que se exige a aquellos que, bajo su responsabilidad, adopten las medidas técnicas y organizativas necesarias para garantizar y poder demostrar que se cumplen las obligaciones del RGPD.

Pero hay cosas que no han cambiado respecto al modelo anterior regulado en la Directiva 95/46/CE y la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Me refiero, en concreto, a la imposibilidad de imponer multas o sanciones económicas por las Autoridades de Control a todo un elenco de personas jurídico-públicas entre las que se encuentran las Administraciones y otros organismos públicos vinculados o independientes recogidos en el artículo 77.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

1 El presente trabajo ha sido elaborado en el marco del Proyecto de Investigación PID2020-120373RB-I00. Financiado por el Ministerio de Ciencia e Innovación, sobre «Identidad digital, derechos fundamentales y neuroderechos»

Como intentaremos desarrollar en el presente trabajo, entendemos que esta es una anomalía jurídica que se debe revisar mediante un cambio normativo que permita imponer sanciones económicas a todas aquellas entidades del sector público que realicen tratamientos de datos personales, por cuenta propia o de terceros. Y todo ello por las razones que más adelante se expondrán. No es de recibo en este caso, e insisto en la idea, que haya un tratamiento jurídico diferente para según que responsables y encargados de tratamiento. Sobre todo, cuando lo que se pretende proteger es el mismo bien jurídico, el mismo derecho fundamental.

Así, en la medida en que la potestad sancionadora en la materia tiene unos objetivos claros y las sanciones económicas tienden a alcanzar esas metas, no tiene sentido excluir a unos sujetos responsables o encargados cuyo tratamiento de datos puede resultar potencialmente arriesgado para los derechos de los ciudadanos, sobre todo por la atribución legal de potestades públicas y poderes exorbitantes. No debemos olvidar que el tratamiento que se hace desde el sector público, en concreto las Administraciones públicas, puede ser especialmente lesivo para el derecho fundamental a la protección de datos y que, como se verá, el propio RGPD impone especiales requisitos y condiciones a las Administraciones públicas.

Esta premisa resulta imprescindible para concluir, como intentaremos en este trabajo, que las Autoridades de control competentes deben tener la potestad de imponer sanciones económicas a las Administraciones públicas que cometan infracciones en materia de protección de datos en los mismos términos, al menos, que los responsables y encargados del sector privado. Aplicando, si se justifica adecuadamente, determinados criterios de modulación.

Importante aún, es destacar que varios países de Latinoamérica tienen sus Leyes de Protección de Datos Personales inspiradas en el RGPD, por eso nos parece importante verificar en qué medida se aplican sanciones pecuniarias a las Administraciones públicas. El estudio ha elegido Brasil una vez que es el país que forma parte del Grupo de Investigación de Protección de Datos Personales de España y tiene aportado muchas experiencias en la materia. Hay que poner de relieve, que no se trata de un estudio de derecho comparado, pero, aportar la experiencia brasileña en lo que concierne a las sanciones aplicada por la Autoridad Nacional en Protección da Datos Personales (adelante ANPD).

2. Modelo anterior al reglamento general de protección de datos

2.1. Visión general sobre la aplicación de la Directiva 95/46/CE en el territorio de la UE: divergencia entre ordenamientos

El régimen jurídico anterior al RGPD estaba recogido en la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, antes mencionada, que fue transpuesta a nuestro ordenamiento por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Este tipo de normas europeas, como es conocido, han de ser adaptadas a los ordenamientos internos por medio de la legislación nacional. Esto ocasionó una divergencia de ordenamientos jurídicos y una heterogeneidad en el grado de protección del derecho fundamental a la protección de datos personales que debilitaba, en gran medida, su eficacia. Además, era una norma que de la «era pre-Internet»[2] (Piñar Mañas, 2016: 16), lo que generaba algún problema con su aplicación a las tecnologías más avanzadas.

2 Que sea una norma de la era pre-Internet no justifica, en mi opinión, su reforma o derogación pues existen mecanismos jurídicos y fuentes del Derecho que han de ser capaces, aplicados debidamente, de colmar las lagunas y adaptar los ordenamientos a los tiempos actuales.

En lo que se refiere al régimen sancionador, en concreto, se debe señalar que esa divergencia entre ordenamientos se pronunciaba aún más. La Directiva 95/46 no desarrollaba un régimen de infracciones o sanciones uniforme, sino que dejaba una amplia libertad a los Estados miembros para su configuración, lo que generaba distintos regímenes muy diferentes. Así, el artículo 24 de la meritada Directiva 95/46, señalaba expresamente que:

> «Los Estados miembros adoptarán las medidas adecuadas para garantizar la plena aplicación de las disposiciones de la presente Directiva y determinarán, en particular, las sanciones que deben aplicarse en caso de incumplimiento de las disposiciones adoptadas en ejecución de la presente Directiva».

Es decir, los Estados podían establecer diversos regímenes sancionadores, llegando incluso, como en el caso de Irlanda, a no reconocer potestad sancionadora a su Autoridad de Control, lo que generaba una importante diferencia, por ejemplo, con el caso de España. Esto ya se puso de manifiesto en su momento por los representantes de las grandes empresas que se quejaron ante la Comisión «de que las disparidades actuales impiden a las organizaciones multinacionales desarrollar políticas paneuropeas sobre protección de datos. Los operadores económicos requieren de una mayor seguridad jurídica que permita las transferencias de datos personales a través de las fronteras interiores de la UE, algo incompatible con la actual fragmentación de las legislaciones nacionales (Troncoso Reigada, 2012: 70). Así se puso de manifiesto en el Primer informe sobre la aplicación de la Directiva sobre protección de datos (95/46 CE) (COM/2003/0265 final).

2.2. Sanciones a las Administraciones públicas: el caso español

Dentro de ese margen de libertad que otorgaba la Directiva 95/46, se incluía, también, la posibilidad de imponer sanciones económicas a las Administraciones públicas. Estas, sin ninguna duda, quedaban dentro del ámbito de aplicación de la Directiva y, por tanto, de las correspondientes normas de transposición. En el caso español, como es conocido, la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

La aplicación del régimen de protección de datos a las Administraciones públicas y, en general, al sector público, no ha planteado serias dudas en la doctrina. Al contrario, parece que ha habido unanimidad, desde el principio, a la hora de proclamar que los entes públicos deben quedar sometidos a la legislación sobre protección de datos. Algo que resulta completamente lógico y acorde a los principios de protección del derecho fundamental a la protección de datos, sobre todo si se tiene en cuenta la cada vez mayor intervención administrativa en la esfera privada de los ciudadanos y en el mercado. Es más, dado que la Administración ejerce un poder público intenso sobre personas físicas y jurídicas los tratamientos de datos que estas realicen deben ser objeto de especial supervisión por parte de las Autoridades de control competentes.

Esto ya quedaba patente en el modelo anterior. Y la propia Directiva, así como la Ley 15/1999, preveían el sometimiento de las autoridades públicas al régimen de protección de datos. Así en las definiciones que el artículo 2 de la Directiva realizaba sobre responsable y encargado de tratamiento, así como tercero. O en las bases que legitimaba el tratamiento al que se refiere el artículo 7.e):

> «es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos»[3]

3 En este sentido, el Considerando 32 de la Directiva señalaba que: «[...] que corresponde a las legislacio-

Por su parte, la Ley orgánica 15/1999, también reconocía que los ficheros públicos, titularidad de una Administración pública, estaban sometidos al régimen jurídico entonces vigente. Tampoco planteaba duda alguna que las Administraciones pudieran incurrir en la comisión de infracciones administrativas derivadas de este régimen. Sin embargo, el artículo 46 no preveía la posibilidad de imponer sanciones de tipo económico (lo cierto es que tampoco lo prohibía), y se refería a que la AEPD dictaría una: «resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción».

En conclusión, el distinto régimen jurídico sancionador entre el sector público y el sector privado ya venía recogido en el modelo anterior como una opción del propio legislador estatal. Nada impedía en la Directiva a los Estados miembros optar por un régimen igualitario entre el sector público y el sector privado, en que se pudiera imponer sanciones a ambos tipos de entidades. Pero España optó por establecer un régimen más laxo para las Administraciones públicas. Estas quedaban sujetas a las obligaciones en materia de protección de datos, incluso sus actuaciones podían ser, no ya contrarias a Derecho y por tanto nulas o anulables, sino que se reconocía, sin tapujos, la posibilidad de cometer infracciones. Lo que no se podía, sin embargo, es imponer sanciones económicas, a diferencia de lo que ocurre con las entidades del sector privado.

Como se pondrá de manifiesto en los siguientes epígrafes, el mismo régimen se mantiene en el RGPD y en la LOPDyGDD, pese a que aquel daba libertad a los Estados miembros para imponer multas económicas a las Administraciones, si lo estimaban oportuno. España no cambió de opción e intentaremos ver los motivos.

3. Marco jurídico actual de la protección de datos dentro del EEE

3.1. La necesidad de aprobar una nueva norma jurídica

Tal y como ya se ha indicado más arriba, la Directiva 95/46 presentaba algunas carencias que requerían ser atendidas por el legislador comunitario, bien mediante una modificación de la propia Directiva, bien mediante la aprobación de una nueva norma jurídica. Se optó finalmente, como es sabido, por esta última opción.

Las razones que motivaron el cambio de normativa se pueden sintetizar en las siguientes (Jiménez Asensio, 2019: 322): por un lado, la necesidad de poner remedio a la posición dominante, de cuasi monopolio, de las grandes compañías tecnológicas en relación a los datos personales de los ciudadanos; en segundo lugar, la necesidad de adaptar la normativa a tecnologías que no se habían tenido en cuenta en la elaboración de la Directiva anterior como, por ejemplo, la generalización del uso de internet por parte de los ciudadanos[4].

nes nacionales determinar si el responsable del tratamiento que tiene conferida una misión de interés público o inherente al ejercicio del poder público, debe ser una administración pública u otra persona de derecho público o privado, como por ejemplo una asociación profesional».

4 En palabras de Jiménez Asensio, R., (2019) «El nuevo marco normativo de la protección de datos personales: su aplicación a las entidades locales, *Anuario Argonés del Gobierno Local 2018*, p. 322: «Las razones de ese tránsito en la concepción del problema tienen que ver con dos factores sustantivos:
a) La posición dominante de las grandes compañías tecnológicas que tienen una posición de cuasi monopolio en todo lo que afecta a los datos personales con un volumen de información cada vez más abrumador, lo que puede tener serias consecuencias sobre los derechos de la persona y la propia subsistencia del Estado democrático tal como lo hemos concebido tradicionalmente;
b) El acelerado e incierto desarrollo tecnológico que, basado en el dato personal y en los algoritmos, está inaugurando una nueva revolución tecnológica de resultados altamente inciertos, un contexto que exige incidir especialmente en la prevención o en el denominado «enfoque de riesgos».

El profesor José Luis Piñar Mañas (2016: 16) indicaba que «La ya vieja Directiva 95/46, que, junto con el Convenio 108 del Consejo de Europa y las Directrices de la OCDE de 1980, ha revolucionado la protección de datos a nivel mundial, tiene los meses contados. Desde múltiples foros se había advertido la necesidad de reformarla y se había advertido reiteradamente que era una norma de la era pre-Internet».

Parecía, por tanto, necesaria la modificación del escenario normativo y su adaptación a los nuevos tiempos. Lo que no era tan claro ni, por tanto, había unanimidad, era sobre el tipo de norma que habría de utilizarse para establecer el nuevo régimen jurídico. Por algunos Estados miembros se defendió la idea de que lo mejor sería seguir con una Directiva. Otros en cambio, propugnaron el Reglamento como norma más apropiada. Finalmente fue a través de un Reglamento, como se sobradamente conocido, lo que tiene unas implicaciones enormes sobre el régimen jurídico.

3.2. Un Reglamento con aires de Directiva

La norma que finalmente se aprobó, como ya se ha indicado, fue un Reglamento, esto es, se trata de una norma directamente aplicable, de alcance general y obligatorio en todos sus elementos, tal y como establece el artículo 288 del Tratado de Funcionamiento de la Unión Europea. Es decir, no necesita de transposición por parte de los Estados miembros, sino que es obligatorio en todos sus términos.

No obstante, es necesario poner de manifiesto que, pese a su alcance general y su aplicabilidad directa, se trata de una norma jurídica que deja amplios márgenes de apreciación a los Estados miembros[5] para su desarrollo (García Mexia, 2016: 26). Es decir, que el RGPD no agota toda la regulación en sí mismo, sino que permite a los Estados miembros concretar y detallar en su propio ordenamiento interno determinadas cuestiones. Por poner algunos ejemplos, el artículo 8 del RGPD señala que el consentimiento del niño en relación con los servicios de la sociedad de la información será válido cuando este tenga como mínimo 16 años, no obstante, otorga un margen de apreciación a los Estados para que, si lo estiman oportuno, se reduzca a los 13 años.

De la misma manera, y en lo que aquí ahora interesa, el artículo 83.7 del RGPD permite que sean los Estados miembros los que decidan si procede imponer multas administrativas a las autoridades y organismos públicos. España, siguiendo la línea anterior, decide no imponer sanciones económicas a las Administraciones públicas y otros entes integrantes del sector público, como luego señalaremos más detenidamente. Y así, como indicaba, el RGPD está repleto de «guiños», si se me permite la expresión, al acervo de los Estados miembros.

3.3. Cambio de paradigma en el régimen jurídico de la protección de datos

Como se ha indicado más arriba, el régimen jurídico en materia de protección de datos da un giro copernicano pues se avanza hacia un nuevo modelo europeo de privacidad que ha pasado a ser, además, el estándar internacional en la materia (Cervera Navas, 2023: 67). Este cambio puede resumirse en una afortunada frase del profesor José Luis Piñar Mañas: «un nuevo modelo que podemos decir que pasa de la gestión de los datos al uso responsable de la información» (Piñar Mañas, 2016: 16).

5 Se llega a hablar de «efecto Gruyère» por la cantidad de ocasiones en las que el propio RGPD deja «vacíos regulatorios cortésmente cedido al Derecho de los Estados.

Uno de los principios que, quizás, condense esta idea es el de «responsabilidad proactiva» que viene recogido en el artículo 24 del RGPD y que, literalmente, viene a indicar que:

> «1. Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario».

De este precepto llama la atención, en primer lugar, que son los responsables y encargados de tratamiento los que deben conocer a fondo su organización y su actividad y, en base a esto, adoptar las medidas que estimen oportunas. Ya no hay una regulación preestablecida en torno a la cual justificar el cumplimiento. Si se permite la licencia, no vale con cumplir y «echarse a dormir». La vigilancia, después del RGPD, debe ser constante. El cumplimiento debe ser constante y duradero, atentos en todo momento a un posible cambio de las circunstancias.

En segundo lugar, llama poderosamente la atención, a quien suscribe al menos, que sean los responsables y encargados de tratamientos quienes deban no solo garantizar sino también estar en condiciones de demostrar que el tratamiento es conforme al RGPD. Es decir, se produce una suerte de inversión de la carga de la prueba, de forma que, ante una posible inspección o denuncia, es el responsable o encargado el obligado a demostrar que se han adoptado todas las medidas necesarias para cumplir el RGPD. Pero a esta cuestión, si se me permite, me referiré un poco más adelante, pues presenta una problemática muy específica.

Otras novedades que implementó del RGPD, ya conocidas y sin ánimo de ser exhaustivo: el nuevo régimen de transparencia e información[6], los derechos ARCOPOL[7], la necesidad de llevar un Registro de Actividades de Tratamiento[8], la obligación de realizar, en ciertos casos, Evaluaciones de Impacto sobre la privacidad[9], la figura del Delegado de Pro-

6 Artículos 12, 13 y 14 del RGPD

7 Este acrónimo hace referencia a los derechos de acceso, rectificación, supresión (derecho al olvido), limitación, obligación de notificación sobre rectificación, supresión o limitación, portabilidad, oposición y el derecho a no tomar decisiones individuales automatizadas, incluida la elaboración de perfiles, reconocidos en el artículo 15 a 22 del RGPD, y con un régimen especial en cuando a su ejercicio y el incumplimiento por parte de los responsables y encargados de tratamiento. Me gustaría recalcar la importancia del derecho a que no se tomen decisiones individualizadas automatizadas, incluida la elaboración de perfiles, ante el auge de la inteligencia artificial pues resulta que muchos de los derechos que los ciudadanos pueden esgrimir frente al uso indebido de esta tecnología nacen del propio RGPD, pese a la reciente normativa aprobada en julio de este año: Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial).

8 Artículo 30 del RGPD que señala que será obligatorio para todas aquellas empresas u organizaciones que empleen, al menos, a 250 personas, o cuando el tratamiento que realice pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos personales indicadas en el artículo 9, apartado 1, o datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10.

9 Reguladas en el artículo 35 del RGPD.

tección de Datos[10] o el principio de privacidad en el diseño y privacidad por defecto[11], entre otras circunstancias, obligaciones todas ellas que afectan de lleno a las Administraciones públicas.

3.4. Especial atención a las Administraciones públicas

Las Administraciones públicas se convierten en responsables y encargados de tratamiento cualificados, pues el riesgo que genera el ejercicio de potestades públicas y el poder reconocido por la Ley en sus relaciones con los ciudadanos y empresas hace que se deba tener un especial cuidado cuando son este tipo de entidades públicas las que tratan datos personales, pues la posibilidad de que se vean negativamente afectado el derecho fundamental se incrementa exponencialmente.

La historia reciente, además, se ha empeñado en mostrarnos lo terrible que puede ser el uso de este tipo de tecnologías de la información por parte de poderes públicos. La elaboración de perfiles étnicos o religioso, de afiliación a partidos políticos o sindicatos puede tener consecuencias muy perniciosas (Black, 2001)

De ello fue consciente el legislador europeo e incluyó en el RGPD múltiples referencias a las Administraciones y organismos públicos para concretar, de alguna manera, el régimen jurídico del tratamiento de datos personales. Así, en lo que se refiere a la responsabilidad proactiva, se exige a las Administraciones (Romeo Ruiz, 2020: 143) una mayor cautela en su cumplimiento derivada, sin duda, de su especial naturaleza pública.

Toda una serie de medias que ahora no se pueden detallar, aunque me quiero referir a una en concreto pues pone de manifiesto, sin duda alguna, la gran preocupación del RGPD por la relación entre las Administraciones públicas y los ciudadanos en este ámbito: el consentimiento expreso que los ciudadanos otorgan para el tratamiento de sus datos personales (Cerrillo i Martínez, 2019: 105). Y es que, consciente del desequilibrio existente entre Administraciones públicas y los ciudadanos, el considerando 43 del RGPD presume que el consentimiento que el interesado pueda dar al tratamiento de datos personales efectuado por una Administración no es libre. Así lo pone de manifiesto expresamente el citado Considerando:

> «Para garantizar que el consentimiento se haya dado libremente, este no debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal en un caso concreto en el que exista un desequilibro claro entre el interesado y el responsable del tratamiento, en particular cuando dicho responsable sea una autoridad pública y sea por lo tanto improbable que el consentimiento se haya dado libremente en todas las circunstancias de dicha situación particular».

Se debe aclarar que cuando la Administración realiza tratamientos de datos por las Fuerzas y Cuerpos de Seguridad del Estado con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, no se aplica el régimen jurídico previsto en el RGPD sino uno mucho más laxo establecido en la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, que ha sido incorporada a nuestro ordenamiento jurídico por la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones

10 Artículos 37 y 38, será necesario cuando el responsable o encargado sea una Administración pública.

11 Artículos 24 y 25 del RGPD. Se trata, en mi opinión, de dos preceptos esenciales para evitar que el RDPD incurra en obsolescencia como consecuencia del avance de las tecnologías.

penales. No puede detenerme a valorar estas normas porque excede, estimo, del objeto de este trabajo, pero plantea cuestiones interesantes el ejercicio de potestades para la salvaguarda de la seguridad pública y la protección del derecho a la protección de datos de aquellas personas sobre las que no existen indicios fundados de que vayan a cometer un delito, es decir, la mayoría de la población (Corral Sastre, 2024: 97).

4. Régimen sancionador en materia de protección de datos y la aplicación especial a las Administraciones públicas en España y en brasil

Volvemos al objeto del trabajo, es decir, la aplicación excepcional del régimen sancionador en materia de protección de datos a determinados entes del sector público, incluidas las Administraciones públicas. Para ello, haremos una breve aproximación sobre el régimen general en la materia para referirnos, posteriormente, a las especiales particularidades en su aplicación a las Administraciones públicas.

Como ya se hemos señalado más arriba, el régimen sancionador previsto en el RGPD y en la LOPDyGDD a ejemplo de Brasil en la LGPD, se aplica también a las Administraciones públicas de manera que estas, como personas jurídico-públicas, pueden cometer infracciones administrativas de las tipificadas en las normas señaladas. La diferencia con respecto a las entidades del sector privado es, como veremos más adelante, que no se pueden imponer sanciones económicas a estas Administraciones. Pero esta no es la única especialidad, como veremos a continuación, del régimen sancionador. Vamos a hacer referencia a las más importantes.

4.1. Aproximación general al régimen sancionador sobre protección de datos en el RGPD. Principales puntos de fricción con el ordenamiento sancionador interno

Una de las principales novedades que se incorporaron al RGPD fue su régimen sancionador. Quizás, lo que más llamó la atención fue el sensible incremento de las sanciones. De acuerdo con lo previsto en el artículo 83, estas podían llegar a 20 millones de euros o el 4 % del volumen global anual de negocio de una empresa. Lo que se ha demostrado que, en el caso de grandes empresas, puede llegar a ser una cifra considerable[12]. Como a continuación veremos, esta no es una preocupación que deban tener las Administraciones públicas.

Pero más allá del considerable incremento de las sanciones, lo que puede implicar una vulneración del principio de proporcionalidad en los términos establecidos por nuestro ordenamiento interno (Tornos Más, 2008: 40), lo cierto es que existen determinadas cuestiones sobre el régimen sancionador que debe ser abordadas con cierto detenimiento. No se pueden agotar todas las cuestiones en este trabajo, pues no es objeto del mismo, pero sí queremos mencionar las que, en nuestra opinión, pueden ser más problemáticas.

12 El 22 de mayo de 2023, *Meta Platforms Ireland Limited* (Meta IE), recibió la multa más alta impuesta en aplicación del RGPD: 1.200 millones de euros. Esta multa se impuso por las transferencias de datos personales de Meta a los EE. UU. sobre la base de cláusulas contractuales estándar (SCC) desde el 16 de julio de 2020. Además, se ha ordenado a Meta que cumpla con sus transferencias de datos. con el RGPD. Véase la nota de prensa en https://www.edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_es, [consultado el 23 de octubre de 2024]

Así, la primera cuestión que llama la atención viene recogida en artículo 24.1 del RGPD que se refiere al ya citado principio de responsabilidad proactiva y que reza lo siguiente:

> «1. Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario».

Según se puede entender, entra esta regulación en conflicto directo con el derecho fundamental a la presunción de inocencia tal y como se reconoce en el artículo 24.1 de la Constitución Española (CE), que supone, y cito textualmente la sentencia 66/2007, de 27 de marzo Tribunal Constitucional que «''no pueda imponerse sanción alguna que no tenga fundamento en una previa actividad probatoria lícita», e implica también el reconocimiento del derecho a un procedimiento administrativo sancionador debido o con todas las garantías, que respete el principio de contradicción y en que el presunto responsable tenga la oportunidad de defender sus propias posiciones, vedando la incoación de expedientes sancionadores cuando resulte apreciable de forma inequívoca o manifiesta la inexistencia de indicios racionales de que se ha cometido una conducta infractora, o en los que esté ausente la antijuridicidad o la culpabilidad». En esta misma línea se ha pronunciado nuestro Tribunal Supremo entre otras en la sentencia de 27 de noviembre de 2011, (RC 2515/2009): «la carga de probar los hechos constitutivos de cada infracción corresponde ineludiblemente a la Administración pública actuante, sin que sea exigible al inculpado una *probatio diabólica* de los hechos negativos».

Se produce aquí una colisión entre dos derechos fundamentales: derecho fundamental a la protección de datos, reconocido en la Carta de Derechos Fundamentales de la Unión Europea (artículo 8) y sobre el que esta tiene competencia para desarrollar normativamente (artículo 16 del Tratado de Funcionamiento de la Unión Europea, en adelante, TFUE) y el derecho fundamental nacional reconocido en el artículo 24 de la CE y que ha sido ampliamente desarrollado por nuestro más alto interprete de la Constitución y el Tribunal Supremo. Derecho este último, por cierto, que también se reconoce en la CDFU, en concreto, en su artículo 48[13], y en el artículo 6.2 del Convenio Europeo de Derechos Humanos.

No obstante lo anterior, y para el ámbito concreto del Derecho de la competencia, se ha de indicar que hay cierta flexibilización de este derecho en la medida que es difícil, en determinados ámbitos, obtener pruebas suficientes para desvirtuar la mencionada presunción[14]. Igualmente, este principio de presunción de inocencia no es absoluto, pues rige el principio de disponibilidad de la prueba, es decir, que «si la persona o entidad contra la que se dirige el procedimiento sancionador alega un hecho con el que pretende justificar

13 Algunas sentencias que se refieren a este derecho en el ámbito sancionador del Derecho de la competencia: (sentencias del Tribunal de Justicia de 17 de diciembre de 1998, Baustahlgewebe/Comisión, C 185/95 P, Rec. p. I 8417, apartado 58, y de 8 de julio de 1999, Comisión/Anic Partecipazioni, C 49/92 P, Rec. p. I 4125, apartado 86; sentencia del Tribunal General de 25 de octubre de 2011, Aragonesas Industrias y Energía/Comisión, T 348/08, Rec. p. II 0000, apartado 90)

14 En este sentido se pronuncia la Audiencia Nacional (Sala de lo Contencioso-Administrativo, Sección 6.ª) en su sentencia de 14 diciembre 2020 (JUR 2021\69866) «por lo que respecta a la llamada prueba indiciaria (...), quien sanciona parte de un hecho conocido y cierto del que a través de un razonado proceso de análisis deductivo se concluye la existencia de otro desconocido, hasta ese momento, pero también cierto y veraz, donde se culmina y manifiesta la conducta infractora y la culpabilidad de quien la cometió. Este proceso debe estar trabado con la suficiente fuerza persuasiva que lleve, sin dudas, a la convicción de quien sanciona de que los hechos se han producido tal y como se describen, de manera que sea posible establecer una directa relación entre estos y las consecuencias punitivas que se anudan, descartando cualquier otra explicación alternativa».

su actuación o excluir su responsabilidad (por ejemplo, alega haber recabado el consentimiento o haber respondido en forma debida al requerimiento), la prueba de estos extremos corresponderá a quien los alega» (Calvo Rojas, 2003: 222)

Otra fricción entre el Derecho de la Unión y el interno en materia sancionadora de protección de datos se produce con el principio de tipificación de las sanciones administrativas y la falta de seguridad jurídica que plantea el hecho de que la sanción económica que puedan imponer las autoridades de control vaya de los 0 euros a los 20 millones de euros o el 4 % del volumen total global anual de una empresa, según lo previsto en el artículo 86.3 del RGPD. Bien es cierto que el apartado 2 del mismo artículo 83 permite amoldar las sanciones a cada caso concreto en función de las circunstancias[15], pero no deja de ser una enorme discrecionalidad que, en mi opinión, atenta directamente contra el principio de seguridad jurídica.

Es comprensible, como defienden algunos autores, que no debamos quedarnos en estas fricciones de Derecho interno y adoptar una visión general de todo el sistema de protección de datos recogido en el RGPD. Así se puso de manifiesto por el profesor Alessandro MANTELERO en una intervención posterior a la ponencia de quien suscribe realizada en un seminario de Universidad de Murcia el pasado 2 de julio[16]. Pero no dejan de ser problemas complejos, reales y cotidianos a los que los juristas debemos enfrentaros diariamente. Vivir en el mundo de las ideas es muy cómodo, si se me permite la expresión, pero pienso humildemente que la Academia debe descender al barro, a las trincheras, y dedicarse a solucionar los problemas reales de la aplicación del Derecho, sin renunciar, como es lógico, a proponer ideas generales mediante, en su caso, procesos de razonamiento inductivo.

En lo que concierne a Brasil, es importante aclarar que Ley General de Protección de Datos Personales (LGPD — Ley n.º 13.709/2018) define «Poder Público» como las personas jurídicas de derecho público, remitiendo su aplicación a las entidades abarcadas por la Ley de Acceso a la Información (LAI — Ley n.º 12.527/2011)[17].

Al esclarecer su ámbito de aplicación, la Autoridad Nacional de Protección de Datos (ANPD) establece que la LGPD se aplica a organismos y entidades de los entes federativos (Unión, Estados, Distrito Federal y Municipios) y a los tres Poderes (Ejecutivo, Legislativo

15 Estos criterios han sido desarrollados por el Comité Europeo de Protección de Datos que ha aprobado las Directrices 04/2022, sobre el cálculo de las multas administrativas contempladas en el RGPD, pero no dejan de ser criterios interpretativos de «soft law»,

16 La ponencia a la que me refiero se titulaba «La potestad sancionadora de las autoridades de control seis años después de la entrada en vigor del RGPD» en el Seminario «Las competencias de las autoridades de control en materia de protección de datos desde la perspectiva de la regulación europea», celebrado el día 2 de julio de 2024 en la Facultad de Derecho de la Universidad de Murcia y a la que fui amablemente invitado por el profesor Julián Valero Torrijos.

17 Artículo 1.º Esta Ley dispone sobre los procedimientos que deben ser observados por la Unión, los Estados, el Distrito Federal y los Municipios, con el fin de garantizar el acceso a la información previsto en el inciso XXXIII del artículo 5.º, en el inciso II del § 3.º del artículo 37 y en el § 2.º del artículo 216 de la Constitución Federal.
Párrafo único. Se subordinan al régimen de esta Ley:
I — los órganos públicos integrantes de la administración directa de los Poderes Ejecutivo, Legislativo, incluidas las Cortes de Cuentas, y Judicial, así como del Ministerio Público;
II — las autarquías, fundaciones públicas, empresas públicas, sociedades de economía mixta y demás entidades controladas directa o indirectamente por la Unión, los Estados, el Distrito Federal y los Municipios.
Artículo 2.º Se aplican las disposiciones de esta Ley, en lo que corresponda, a las entidades privadas sin fines de lucro que reciban recursos públicos directamente del presupuesto o mediante subvenciones sociales, contrato de gestión, término de asociación, convenios, acuerdos, ajustes u otros instrumentos similares para la realización de acciones de interés público. (traducción libre del autor)

y Judicial), incluyendo Tribunales de Cuentas, la Fiscalia General (Ministerio Público), servicios notariales y de registro, empresas públicas y sociedades de economía mixta que desempeñan funciones de interés público.

La LGPD es una legislación inspirada em el RGPD y basada en principios, con el objetivo de garantizar la protección de los datos personales y los derechos de sus titulares. De esta manera, la actuación de la administración pública debe preservar siempre el interés colectivo y los derechos fundamentales. (Peck Pinheiro. 2020)

Al analizar los derechos fundamentales establecidos por la LGPD, se observa que la protección de datos personales, el libre acceso, la transparencia, la seguridad, la prevención y la no discriminación están relacionados con el derecho a la privacidad, según lo dispuesto en el artículo 5, inciso X, de la Constitución Federal. Aunque derivados de este derecho, han evolucionado hasta alcanzar un estatus autónomo, siendo reconocidos internacionalmente, incluso en el sistema de la ONU y en el ordenamiento jurídico europeo. En Brasil, el derecho a la protección de datos personales fue elevado a derecho fundamental por el artículo 5, inciso LXXIX, de la Constitución Federal, introducido por la Enmienda Constitucional n.º 115/2022. (Sarlet, 2021: 21-59).

En este contexto, el tratamiento de datos personales por parte de de las administraciones púbicas debe estar alineado con los principios de finalidad pública, interés colectivo y legalidad, garantizando transparencia y accountability. Cada ente público posee competencia legal específica para ejercer sus funciones y procesar información personal, siempre que haya previsión legal y justificación para dicha actividad.

Dada la masiva recopilación de datos personales por parte de los organismos públicos, derivada de la obligatoriedad de proporcionar esta información por parte de los ciudadanos para acceder a servicios esenciales como la adquisición de bienes inmuebles, la obtención de documentos oficiales y el acceso a servicios de salud, es fundamental garantizar la transparencia en los procesos de tratamiento de datos. Esto incluye la divulgación clara de la base legal, las finalidades y los procedimientos adoptados, evitando así asimetrías informativas entre el ciudadano y el Estado. (Copetti Cravo, et alii, 2021)

La ANPD, como órgano regulador, tiene la responsabilidad de interpretar y aplicar la LGPD, estableciendo directrices para los responsables y operadores en el sector público. Además, posee competencia para la imposición de sanciones administrativas y la mediación de conflictos relacionados con la protección de datos personales. (Coelho y Sousa, 2022).

Dado el volumen de datos tratados por el sector público, es esencial que la ANPD promueva la estandarización y la fiscalización de las prácticas de tratamiento de datos, garantizando mayor seguridad jurídica y eficiencia en la protección de los derechos de los titulares. Además, es necesario fomentar la concienciación y la capacitación de los gestores y funcionarios públicos, asegurando que la implementación de la LGPD se realice de manera eficaz y alineada con los principios que rigen la actuación estatal.

4.2. Autoridades autonómicas de protección de datos

En ese margen de apreciación al que me refería más arriba, el RGPD, igual que hacía la Directiva 95/46, permitía la creación de autoridades de control autonómicas con las competencias a las que se refiere el artículo 57.1 de la LOPDyGDD (Murillo de la Cueva, E.L., 2021: 2645):

> «a) Tratamientos de los que sean responsables las entidades integrantes del sector público de la correspondiente Comunidad Autónoma o de las Entidades Locales incluidas en su ámbito territorial o quienes presten servicios a través de cualquier forma de gestión directa o indirecta.

b) Tratamientos llevados a cabo por personas físicas o jurídicas para el ejercicio de las funciones públicas en materias que sean competencia de la correspondiente Administración Autonómica o Local.

c) Tratamientos que se encuentren expresamente previstos, en su caso, en los respectivos Estatutos de Autonomía».

Por consiguiente, las presuntas infracciones cometidas por las Administraciones públicas autonómicas y locales, corresponde a estas autoridades autonómicas de control. En la actualidad solo tres comunidades autónomas han asumido competencias en materia tratamiento de datos personales efectuados por entidades del sector público: Cataluña[18], País Vasco[19] y Andalucía[20] y el ejercicio de dichas competencias corresponde, por tanto, a la Autoridad Catalana de Protección de Datos, la Autoridad Vasca de Protección de Datos y el Consejo de Transparencia y Protección de Datos de Andalucía.

4.3. Interpretación extensiva de autoridad y organismo público

El RGPD, deja abierta la posibilidad a los Estados miembros de que se puedan imponer multas económicas a las Administraciones públicas. Así, el apartado 7 del artículo 83 de la norma europea establece lo siguiente:

«7. Sin perjuicio de los poderes correctivos de las autoridades de control en virtud del artículo 58, apartado 2, cada Estado miembro podrá establecer normas sobre si se puede, y en qué medida, imponer multas administrativas a autoridades y organismos públicos establecidos en dicho Estado miembro».

En primer lugar, es necesario referir que entiende la LOPDyGDD por «autoridades y organismos públicos». Así, en una interpretación que puede considerarse extensa señala los siguientes (artículo 77.1):

«a) Los órganos constitucionales o con relevancia constitucional y las instituciones de las comunidades autónomas análogas a los mismos.

b) Los órganos jurisdiccionales.

c) La Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local.

d) Los organismos públicos y entidades de Derecho público vinculadas o dependientes de las Administraciones Públicas.

e) Las autoridades administrativas independientes.

f) El Banco de España.

g) Las corporaciones de Derecho público cuando las finalidades del tratamiento se relacionen con el ejercicio de potestades de derecho público.

h) Las fundaciones del sector público.

i) Las Universidades Públicas.

j) Los consorcios.

k) Los grupos parlamentarios de las Cortes Generales y las Asambleas Legislativas autonómicas, así como los grupos políticos de las Corporaciones Locales».

18 Artículo 156 de la Ley Orgánica 6/2006, de 19 de julio, de reforma del Estatuto de Autonomía de Cataluña y Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos.

19 Ley 16/2023, de 21 de diciembre, de la Autoridad Vasca de Protección de Datos

20 Artículo 82 de la Ley Orgánica 2/2007, de 19 de marzo, de reforma del Estatuto de Autonomía para Andalucía y Ley 1/2014, de 24 de junio, de Transparencia Pública de Andalucía.

Sin perjuicio de otras cuestiones que puedan resultar problemáticas desde el punto de vista doctrinal, me quiero detener, si quiera brevemente, en el punto d) de este precepto. Se refiere a organismos públicos y entidades de Derecho público dependientes o vinculadas a las Administraciones públicas. Según lo previsto en el artículo 84.1 de la Ley 40/2015, de 1 de otubre, de Régimen Jurídico del Sector Público, dentro de estos organismos públicos y entidades de Derecho público se encuentran un heterogéneo elenco de entes. Transcribo el precepto para una mejor comprensión:

> «a) Los organismos públicos vinculados o dependientes de la Administración General del Estado, los cuales se clasifican en:
> 1. Organismos autónomos.
> 2. Entidades públicas empresariales.
> 3. Agencias estatales.
> b) Las autoridades administrativas independientes.
> c) Las sociedades mercantiles estatales.
> d) Los consorcios.
> e) Las fundaciones del sector público.
> f) Los fondos sin personalidad jurídica.
> g) Las universidades públicas no transferidas».

Es cierto que el artículo 77.1 de la LOPDyGDD no se refiere expresamente al sector público institucional de manera que puedan entenderse incluidas las sociedades mercantiles públicas. Pero tampoco las excluye expresamente, con lo que no queda claro que este tipo de empresas o sociedades integrantes del sector público estén dentro del régimen «blando» previsto en la LOPDyGDD. Alguna doctrina niega que la exención de las multas económicas se pueda aplicar a las mencionadas empresas o sociedades públicas (Jiménez Asensio, R., 2019: 358), pero lo cierto es que ha habido resoluciones sancionadoras de la AEPD contra empresas públicas a las que se ha considerado incluidas en el artículo 77.1 tantas veces mencionado. Así, por ejemplo, la resolución ps-00189-2022, contra la Empresa Municipal Transportes Urbanos, S.A. De Gijón, por la que se impone una sanción de apercibimiento por la comisión de una infracción del Artículo 58.2 del RGPD, tipificada en el Artículo 83.6 del RGPD, y se hace referencia expresa al artículo 77.1 de la LOPDyGDD[21].

Como es fácilmente comprensible, los argumentos que puedan utilizarse para justificar la no imposición de sanciones económicas, por ejemplo, al Ayuntamiento del El Hornillo, pequeño municipio del sur de Ávila, de 266 habitantes, no sirven para defender la no imposición de sanciones económicas a Paradores de Turismo S.M.E. S.A., una sociedad mercantil estatal, totalmente participada por la Administración General del Estado y que ofrece servicios turístico en el mercado, en competencia con otras empresas del sector. En el primer caso, podría estar justificado una modulación de la sanción en función de las especiales circunstancias, en el segundo, quizás, lo que estuviera justificado sería una agravación de la sanción económica dado que, además, se está falseando el mercado.

No es lo mismo. En el ejemplo del párrafo anterior, sin duda, ambos son entes del sector público, pero su naturaleza es muy diferente. Y, en mi opinión, ahí radica uno de los principales problemas que plantea el régimen de exención de sanciones económicas. Pudiera estar justificado un tratamiento diferente a ciertas Administraciones públicas de ámbito territorial (pequeños municipios) y organismos que cumplen misiones de interés público o presentan servicios públicos, pero no, desde luego, a todas las entidades que se han incluido en el artículo 77 de la LOPDyGDD, algunas de las cuales, incido en la idea, compiten en el mercado con otras empresas y particulares que sí pueden ser sancionados económicamente.

---

21 Resolución disponible en la página web: https://www.aepd.es/documento/ps-00189-2022.pdf, [última vez consultada el 31 de octubre de 2024)

4.4. Imposibilidad de imponer multas económicas a las Administraciones públicas en materia de protección de datos en el ordenamiento jurídico español

Quizás la cuestión que más polémica genera en relación con las Administraciones públicas tiene que ver con lo que constituye el objeto de este trabajo, es decir, con la imposibilidad de que las autoridades de control competentes puedan sancionar económicamente a estas entidades.

Nuestro país, siguiendo la senda marcada por la LOPD 1999, prevé que no se impongan sanciones económicas a las Administraciones públicas. Así, la LOPDyGDD señala en su artículo 77.2[22], de una forma un tanto rebuscada, si se me permite indicarlo:

> «2. Cuando los responsables o encargados enumerados en el apartado 1 cometiesen alguna de las infracciones a las que se refieren los artículos 72 a 74 de esta ley orgánica, la autoridad de protección de datos que resulte competente dictará 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 que se hubiese cometido, con excepción de la prevista en el artículo 58.2.i del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016».

Precisamente, la medida prevista en el artículo 58.2.i del RGPD se refiere a:

> «i) imponer una multa administrativa con arreglo al artículo 83, además o en lugar de las medidas mencionadas en el presente apartado, según las circunstancias de cada caso particular»;

Como ya se ha dejado indicado más arriba, hemos de señalar que esto no es una imposición de la Unión Europea a través del RGPD, sino una elección del legislador español. Así el texto del RGPD (artículo 83.7) es bien claro:

> «7. Sin perjuicio de los poderes correctivos de las autoridades de control en virtud del artículo 58, apartado 2, cada Estado miembro podrá establecer normas sobre si se puede, y en qué medida, imponer multas administrativas a autoridades y organismos públicos establecidos en dicho Estado miembro».

Por tanto, el legislador español hace una elección. Excluye a determinados entes públicos de la posibilidad de imponer sanciones económicas. Una elección, además, que se aplica de manera específica al ámbito de la protección de datos y que no se extiende a otras materias como, por ejemplo, medio ambiente, vertidos, legislación hidráulica, carreteras, etc., en las que las Administraciones públicas pueden ser sancionadas económicamente por otras Administraciones competentes.

¿Qué ocurre, por consiguiente, en el ámbito de la protección de datos? ¿Qué argumentos pueden darse para justificar esta decisión legislativa? Vamos a analizarlos con mayor detalle a continuación, sin perjuicio de que indicar, desde este momento, que no comparto la idea de excluir a las Administraciones públicas, al menos todas las que se señalan en el artículo 77.1, de la posibilidad de imponer sanciones económicas, pues genera determinados problemas jurídicos.

22 En la redacción dada por la Ley 11/2023, de 8 de mayo, de trasposición de Directivas de la Unión Europea en materia de accesibilidad de determinados productos y servicios, migración de personas altamente cualificadas, tributaria y digitalización de actuaciones notariales y registrales; y por la que se modifica la Ley 12/2011, de 27 de mayo, sobre responsabilidad civil por daños nucleares o producidos por materiales radiactivos, por el que se modifican, entre otras muchas, la LOPDyGDD.

5. Análisis de las diferentes razones esgrimidas (y ya superadas) para justificar la no imposición de sanciones económicas

5.1. El legislador conocía el incumplimiento sistemático del régimen jurídico por parte de las Administraciones públicas y decide no sancionarlas con multas económicas

Es cierto que, en los últimos años, se ha producido un avance extraordinario por parte de las Administraciones públicas para adaptarse al RGPD. En la mayoría de los casos, sobre todo en las Administraciones más grandes, el esfuerzo ha dado resultado y, por consiguiente, se puede decir sin temor a equivocarse que, en general, las Administraciones públicas cumplen con la legislación de protección de datos.

Pero no es menos cierto que esto no ha sido siempre así. Desde la Ley de Protección de Datos del año 1992, y posteriormente con la Ley Orgánica 15/1999, las Administraciones públicas incumplían sistemáticamente todas las obligaciones impuestas por la Ley en materia de protección de datos, por lo que el legislador llegó a la conclusión, triste conclusión por otro lado, de que lo mejor era excluir la posibilidad de imponer multas económicas a las Administraciones públicas por esta materia (Calvo Rojas, 2003: 228)[23]. Esta misma idea subyace la afirmación de que el proceso de adaptación de las Administraciones públicas al régimen de protección de datos va a ser «lento y gradual» (Jiménez Asensio, R., 2019: 326)[24].

Quizás, en los primeros momentos de implantación de un régimen en materia de protección de datos en nuestro país, donde, en efecto, no había cultura en la materia, podía tener cierto sentido, dudoso, no obstante. Pero que esa situación se haya mantenido inalterable

23 «Cabe mencionar dos circunstancias que, sin duda, favorecen estas carencias que venimos señalando, tanto la falta de efectividad en la protección como la escasa beligerancia en la defensa del propio derecho. De un lado, si antes hemos señalado que la LOPD contiene un elenco de sanciones económicas de considerable cuantía, también hemos indicado que ninguna de éstas puede imponerse cuando el responsable de la infracción es una Administración Pública, pues en tal caso el artículo 46 LOPD (y lo mismo sucedía con el art. 45 de la antigua LORTAD) excluye la sanción económica y limita el alcance de la resolución a que por parte del Director de la Agencia de Protección de Datos se establezcan las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción y, en su caso, se proponga la iniciación de actuaciones disciplinarias contra la autoridad o funcionario responsable. Pues bien, aunque a algunos puede parecer un gesto prudente esta decisión del legislador de excluir las sanciones económicas cuando el infractor es una Administración Pública, debe notarse que este trato privilegiado no deriva de una exigencia constitucional ni es consustancial al juego de las relaciones interadministrativas y, de hecho, no existe esa misma cautela o deferencia en otros ámbitos de la acción administrativa. Todo indica que el legislador ha sido consciente de que el incumplimiento era (y es) masivo en este ámbito, y muy particularmente destacada la falta de cumplimiento por parte de las Administraciones Públicas, y ha preferido seguir respecto de éstas la vía de la persuasión para la paulatina implantación de nuevos modos de actuar en materia de protección de datos.

24 Todos y cada uno de los elementos o ejes de ese Nuevo Modelo de Gestión de Protección de Datos Personales deben ser puestos en marcha, con distinta intensidad como se decía, por todas y cada una de las Administraciones Públicas y por las entidades de su sector público (con las matizaciones que se harán en su momento). Sin duda, el reto es importante. Y no cabe orillar que el proceso de adaptación de las estructuras organizativas de las Administraciones Locales y de sus entidades del sector público será lento y gradual, más aún cuando los incentivos para ese proceso de adaptación son pocos y las sanciones enormemente blandas, lo que puede generar aplicaciones lentas o, incluso, poco efectivas en el sector público. Especialmente complejo será ese proceso de cambio en los municipios o entidades locales que no dispongan de capacidad de gestión o de recursos al efecto. Hay, como se señala luego una suerte de ficción a la hora de considerar que cualquier «organismo o autoridad pública» está en condiciones de llevar a cabo semejante adaptación en los plazos que marca la legislación vigente.

en el tiempo no está justificado. Que se exima a las Administraciones públicas de la posibilidad de que reciban sanciones administrativas en materia de protección de datos por su incumplimiento masivo y sistemático no puede justificarse. No es posible eximir a los entes del sector público de recibir económicas por su masivo incumplimiento. Esto supone un claro atentado contra el principio de legalidad y el Estado de Derecho, es decir, dar carta de naturaleza al incumplimiento de la ley por parte de las Administraciones públicas.

5.2. La multa económica que se imponga a las Administraciones será, en última instancia, soportada por los ciudadanos

Este ha sido, tradicionalmente, otros de los grandes argumentos utilizados para evitar imponer sanciones económicas a las Administraciones públicas, es decir, si la sanción que recae en el ente público posteriormente va a ser transferida a los ciudadanos a través de los ingresos públicos. En definitiva, lo que se quiere manifestar con este argumento es que no tiene sentido imponer una multa económica a una Administración que va a pagar con cargo a los presupuestos generales que se nutren, entre otros ingresos, de los tributos de los ciudadanos.

Sin embargo, como señala alguna autora (Ortega Bernardo, 2017: 189), «el hecho de que la sanción recaiga en la Administración y sea ulteriormente transferida al bolsillo de los contribuyentes, lejos de resultar inconveniente tendría ciertas ventajas». Se refiere aquí la autora citada a la posibilidad de afectar al sentido del voto en relación con el Gobierno que dirige a la Administración. Es decir, que el ciudadano que observa que la Administración incumple y eso tiene efectos en la inversión pública (dado que parte del presupuesto debe ir a pagar la multa), puede cambiar el sentido del voto y, por tanto, ser determinante para las futuras elecciones.

Personalmente pienso que esta posibilidad, es decir, imponer multas económicas a las Administraciones públicas puede ayudar a alcanzar unas mayores cotas de democracia. Se trata, en definitiva, de traer al debate público las consecuencias de la legalidad o ilegalidad de la actividad administrativa y las consecuencias que el incumplimiento de la normativa vigente puede tener en vida de los ciudadanos. Dedicar parte del erario público al pago de multas por incumplimientos normativos no puede estar bien visto por los ciudadanos que, a la postre, exigirán la correspondiente rendición de cuentas.

5.3. No se consigue uno de los objetivos esenciales del Derecho sancionador: la finalidad aflictiva o disuasoria

Otro de los argumentos utilizados para no imponer sanciones económicas a las Administraciones públicas tiene que ver con la imposibilidad de alcanzar el objetivo aflictivo que produce el menoscabo patrimonial. Es decir, no se genera en la Administración una finalidad disuasoria si lo que persigue la actividad administrativa no está motivada por el ánimo de lucro sino por el servicio al interés general. Sin embargo (Ortega Bernardo, 2017: 188), no hay duda de que una pérdida patrimonial a la Administración pública infractora puede acarrear importantes consecuencias para el adecuado funcionamiento de esta.

Por consiguiente, sí se cumple la finalidad disuasoria y aflictiva prevista en el Derecho sancionador cundo se impone una multa económica a las Administraciones públicas. Este argumento que justifica un «régimen sancionador blando» para los entes públicos no resulta ser muy sólido.

Desde otro punto, encontramos a Brasil con el mismo sistema de España en lo que toca a no aplicación de sanciones económicas a la Administración Pública lo que confiere a esa

una situación bastante cómoda ante el ordenamiento jurídico de sanciones aplicadas a las empresas privadas, y nos explicamos:

> El Poder Público ha exigido cada vez más la divulgación constante de información personal por parte de los individuos, a menudo sin una explicación adecuada sobre las bases legales que justifican esta recopilación. Este intercambio excesivo con otras entidades estatales representa un riesgo claro para la autodeterminación informativa, cuya limitación se ha vuelto cada vez más evidente. Es importante destacar que el almacenamiento de datos por parte de instituciones públicas no los convierte en información de acceso público, ya que siguen manteniendo su carácter estrictamente personal (Coelho y Sousa, 2022).

Esta realidad está directamente relacionada con la estrategia de digitalización del gobierno brasileño, iniciada en 2016, que busca ampliar el acceso de la población a los servicios públicos en diversos contextos socioeconómicos y culturales. Esta iniciativa está integrada con la acción de los órganos federales con el objetivo de ofrecer servicios más eficientes, accesibles y a un costo reducido para los ciudadanos a través de la tecnología[25].

Hasta finales de 2019, aproximadamente el 53 % de los servicios del gobierno federal ya estaban disponibles en formato digital, incluyendo más de 500 servicios públicos proporcionados por 28 órganos diferentes. Además, el ahorro anual de R$ 345 millones generado con la digitalización permitió la posibilidad de invertir en la construcción de 156 nuevas Unidades de Atención de Emergencia (UPAs) en el sector salud o en la creación de 182 guarderías para la educación infantil[26].

Por otro lado, el acceso simplificado a los servicios gubernamentales eliminó muchas horas que los ciudadanos antes desperdiciaban en desplazamientos, filas y burocracias anualmente. Esta transformación también generó ganancias significativas en eficiencia en la gestión pública, permitiendo la redistribución de servidores a actividades más complejas y demandadas, ya que los procesos anteriormente burocráticos fueron agilizados mediante el uso de la tecnología.

Estos avances llevaron a Brasil a ocupar la segunda posición en el ranking mundial de servicios públicos digitales, según el Banco Mundial. Sin embargo, a pesar de la meta inicial de digitalizar aproximadamente 5.000 servicios federales hasta finales de 2023 a través de la Plataforma GOV.BR, solo el 89 % de esta meta fue alcanzada[27].

El creciente uso de datos por parte del Poder Público se refleja en la interconexión de información de más de 203 millones de brasileños, de los cuales el 84 % tiene acceso frecuente a internet. Aunque el Estado busca optimizar procesos mediante el uso de datos, una investigación de Kaspersky, en asociación con la consultora Corpa, reveló que Brasil lidera el ranking global de desconocimiento de los derechos relacionados con la protección de datos personales. Según el estudio, el 20 % de los encuestados desconocen sus derechos en el contexto de la Ley General de Protección de Datos (LGPD), y solo la mitad de los participantes está consciente de las consecuencias de la legislación para las organizaciones en las que trabajan. Además, el estudio señala que la principal causa de las filtraciones de información personal son los ciberataques, que han aumentado tanto

25 Governo Federal. *Estratégia de governo digital.* 2023. Disponível em: https://www.gov.br/governodigital/pt-br/estrategias-e-governanca-digital/EGD2020. Acesso em: 09 maio 2024.

26 FEDERAL, Governo. Estratégia de governo digital. 2023. Disponível em: https://www.gov.br/governodigital/pt-br/estrategias-e-governanca-digital/EGD2020. Acesso em: 09 maio 2024.

27 FEDERAL, Governo. Estratégia de governo digital. 2023. Disponível em: https://www.gov.br/governodigital/pt-br/estrategias-e-governanca-digital/EGD2020. Acesso em: 09 maio 2024.

en volumen como en sofisticación. Esto refuerza la necesidad de fortalecer la seguridad cibernética para prevenir violaciones de datos (Kaspersky).

En este contexto, es imprescindible que los órganos públicos actúen con transparencia en relación con las bases legales para la recopilación, almacenamiento y uso de los datos personales. La falta de información clara puede llevar a los ciudadanos a proporcionar sus datos sin una comprensión plena de los impactos y las garantías legales asociadas a la compartición de su información.

Un estudio realizado por Tenable, una empresa estadounidense especializada en la gestión de exposición cibernética reveló que, en 2023, aproximadamente 984,7 millones de datos fueron filtrados en Brasil. Este volumen equivale a 112 terabytes de información expuesta en el país, representando el 43 % de los 257 terabytes filtrados a nivel mundial, según el Informe del Escenario de Amenazas de la empresa (Otávio, 2023).

Un ejemplo reciente de este problema ocurrió el 31 de enero de 2024, cuando la Coordinación General de Fiscalización (CGF) de la ANPD emitió cuatro advertencias a la Secretaría de Estado de Educación del Distrito Federal (SEEDF) debido a infracciones a los artículos 37, 38 y 48 de la LGPD y al artículo 5 de la normativa de fiscalización de la ANPD. El caso implicó la exposición indebida de datos de registro y salud de aproximadamente 3.000 personas inscritas en el Programa de Educación Precoz, debido a una falla de seguridad en el formulario de inscripción del programa (Ingizza, 2024).

A pesar de la formalización del incidente, la SEEDF optó por no notificar a los titulares de los datos para evitar una alarma innecesaria, resolviendo el problema internamente. Sin embargo, incluso después de la evaluación de la Coordinación de Tecnología e Investigación de la ANPD, que constató la gravedad del incidente y la insuficiencia de las medidas adoptadas, no se presentaron informes de impacto sobre la protección de datos ni registros de operaciones de tratamiento[28].

Además, el 20 de septiembre de 2023, la Justicia Federal determinó que aproximadamente 4 millones de personas fueran indemnizadas con R$ 15 mil cada una debido a la masiva filtración de datos ocurrida en 2022. Las indemnizaciones serán pagadas por la Caixa Económica Federal, Dataprev (empresas públicas de naturaleza privada) y la ANPD, conforme a una acción civil pública presentada por el Instituto Brasileño de Defensa de la Protección de Datos. [29]

Ante este panorama, la excesiva compartición de datos entre organismos gubernamentales puede comprometer la autodeterminación informativa, la privacidad y la libertad de los ciudadanos, además de fomentar un entorno propicio para el abuso de poder y la violación de derechos fundamentales.

Esta filtración de datos almacenados afectó principalmente a los beneficiarios del programa Auxilio Brasil, quienes, en el período previo a las elecciones presidenciales de 2022, obtuvieron la posibilidad de destinar una parte significativa de sus beneficios para la adquisición de crédito consignado. Como resultado, los datos personales expuestos

28 BRASIL. Autoridade Nacional de Proteção de Dados. Nota Técnica N.º 57/2022/Cgf/Anpd n.º 57/2022. Secretaria de Estado de Educação do Distrito Federal (SEEDF). Brasília, DF, 31 de janeiro de 2024. Processo Sei/Anpd N.º 00261.001472/2021-41: Comunicação de Incidente de Segurança com Dados Pessoais. Brasília: Governo Federal, 31 jan. 2024. Disponível em: https://www.gov.br/anpd/pt-br/composicao-1/coordenacao-geral-de-fiscalizacao/pas-gdf-processo-publico.pdf. Acesso em: 24 março 2025.

29 BRASIL. Justiça Federal da 3.ª Região — 1.º Grau. Indenização Por Dano Moral, Indenização Por Dano Material, Lei Geral de Proteção de Dados (Lgpd), Lei Geral de Proteção de Dados (Lgpd) n.º: 5028572-20.2022.4.03.6100. Decisão Judicial. São Paulo, 11 set. 2023. Disponível em: https://static.poder360.com.br/2023/09/decisaojustica-13set2023.pdf. Acesso em: 27 maio 2024.

fueron adquiridos indebidamente por agentes bancarios externos, que los utilizaron para ofrecer préstamos y otros servicios financieros. [30]

De esta manera, el intercambio excesivo de datos entre entidades gubernamentales puede llevar a la creación de perfiles detallados de los ciudadanos, incrementando la exposición de su información personal a diversos agentes interesados en influir en sus decisiones a través de algoritmos. La consecuencia directa de tales prácticas es la violación de la autodeterminación informativa de los individuos, comprometiendo sus derechos a la libertad y la privacidad. En la sociedad de vigilancia, las tecnologías de recopilación y análisis de datos permiten a las autoridades gubernamentales y otras entidades monitorear y controlar a los ciudadanos a una escala sin precedentes. Esto no solo erosiona la privacidad y la libertad individual, sino que también crea un entorno propicio para abusos de poder y violaciones de derechos fundamentales.

Como señala Rodotà, el derecho al respeto de la vida privada y familiar se concebía predominantemente como un aspecto individualista. No obstante, dentro de esta protección, la salvaguarda de los datos personales constituye una forma dinámica de tutela, acompañando los datos en todos sus movimientos. Esto implica una ampliación del alcance del derecho a la privacidad, que culmina en la especificación del derecho a la autodeterminación informativa. Dicho derecho incluye la capacidad de mantener el control sobre la propia información y la libertad del titular para determinar cómo gestionar su esfera privada (Rodota, 2008).

A ejemplo de lo que ocorre en España, Brasil no há adoptado un sistema de aplicación de multas a las infracciones de la Administración pública a la LGPD**.** Según el artículo 52, de la LGPD, la ANPD puede imponer sanciones administrativas en caso de infracciones a la normativa. Sin embargo, cuando se trata de órganos y entidades de la administración pública, por cuenta del apartado 3, las sanciones aplicables tienen particularidades, ya que no pueden incluir multas pecuniarias. En lugar de sanciones financieras, la ley prevé mecanismos correctivos y sancionatorios específicos lo que demuestra um caracter mas pedagógico que económico. Las principales sanciones que la ANPD puede aplicar a los órganos públicos incluyen:

1. Advertencias, que se emiten cuando la infracción no es grave o cuando se trata de una primera falta. Em estos casos, la administración pública recibe un plazo para adecuarse a la normativa y corregir las irregularidades identificadas.
2. Publicación de la infracción, la ANPD puede exigir que el órgano público infractor haga pública la sanción impuesta. Esto sirve como medida de transparencia y puede afectar la reputación del ente gubernamental, generando presión social y política para su adecuación.
3. Recomendación de medidas correctivas, em este caso la ANPD puede emitir directrices y exigir la implementación de políticas de seguridad y gobernanza de datos y se pueden solicitar auditorías, capacitaciones internas y la mejora de los sistemas de tratamiento de datos personales.
4. Bloqueo o eliminación de datos personales, en casos de uso indebido o tratamiento sin base legal, la ANPD puede determinar el bloqueo o eliminación de los datos personales afectados. Esta sanción busca evitar que la administración pública continúe utilizando información obtenida de forma irregular.

30 FEDERAL, Ministério Público. Justiça determina indenização de R$ 15 mil a cidadãos que tiveram dados pessoais vazados em 2022. 2023. Disponível em: https://www.mpf.mp.br/sp/sala-de-imprensa/noticias-sp/justica-determina-indenizacao-de-r-15-mil-a-cidadaos-que-tiveram-dados-pessoais-vazados-em-2022. Acesso em: 10 maio 202

5. Suspensión parcial del tratamiento de datos, cuando se detectan graves incumplimientos, la ANPD puede suspender temporalmente el uso de ciertos datos personales hasta que se garantice su tratamiento conforme a la ley. Esta medida puede afectar la prestación de servicios públicos, lo que, em tesis, incentivaria a la administración a corregir rápidamente las irregularidades.
6. Responsabilidad y medidas preventivas, los órganos públicos deben implementar mecanismos de compliance y gobernanza de datos para evitar sanciones. Algunas medidas clave incluyen: Designación de un Encargado de Protección de Datos (DPO) para actuar como intermediario entre la administración y la ANPD; Implementación de políticas de privacidad y seguridad de datos; Capacitación de funcionarios y servidores públicos en protección de datos personales; Evaluaciones de impacto y auditorías periódicas para asegurar el cumplimiento de la LGPD.

Sin embargo, al sector privado se incluyen multas significativas. Se puede referir que el articulo 52 de la LGPD, además de las sanciones aplicables a la Administración publica, prevê que la ANPD pueda imponer una multa simple de hasta el dos por ciento (2 %) del volumen de negocios de la persona jurídica privada, grupo o conglomerado en Brasil en su último ejercicio, impuestos excluidos, limitada a un total, a R$50.000.000 (cincuenta millones de reales brasileños) en euros a fecha de hoy, cerca de 8 millones de euros, por infracción.

6. Una revisión necesaria del sistema de sanciones al sector público

Hace poco más de un año, se publicó en el BOE la Ley 11/2023, de 8 de mayo, de trasposición de Directivas de la Unión Europea en materia de accesibilidad de determinados productos y servicios, migración de personas altamente cualificadas, tributaria y digitalización de actuaciones notariales y registrales; y por la que se modifica la Ley 12/2011, de 27 de mayo, sobre responsabilidad civil por daños nucleares o producidos por materiales radiactivos, en cuya Disposición Adicional 9.9, modificaba el apartado 2 del artículo 77 de la LOPDyGDD.

Lo cierto es que la modificación es importante en la medida aumenta las medidas que se pueden adoptar frente a infracciones cometidas por las Administraciones públicas. Así, si en la primera redacción del artículo la única resolución posible frente a una infracción era el apercibimiento, con la modificación del 2023, se indica que la autoridad de control competente «dictará 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 que se hubiese cometido». Eso sí, excluyendo expresamente la posibilidad de imponer sanciones económicas.

Vamos a proponer, a continuación, algunas tesis por las que, entiendo, debe revisarse el régimen actual e incluir la posibilidad de imponer sanciones económicas a aquellas entidades del sector público que cometan infracciones en materia.

6.1. Discriminación injustificable entre el sector público y el sector privado

De las razones que, quizás, más llaman la atención en lo que al diferente régimen jurídico se refiere nos encontramos, precisamente, con el de la injustificable discriminación entre el sector público y el privado.

Tal y como se ha señalado más arriba, no existen razones de peso suficiente para mantener respecto del sector público un régimen sancionador que impida imponer sanciones económicas y que con el sector privado se pueda llegar a más de 20 millones de euros. No

está justificado. Como es lógico, el efecto disuasorio en el sector privado será mucho más eficaz que en el sector público, donde no se pueden imponer sanciones económicas.

La cuestión alcanza cotas kafkianas cuando la exención a la imposición de sanciones económicas se aplica a entidades públicas que ofrecen bienes y servicios en el mercado y, por tanto, compiten con otras empresas del sector privado que, por cierto, si pueden ser sancionadas con multas astronómicas. Más arriba se ha señalado el ejemplo de la Empresa Municipal Transportes Urbanos, S.A. De Gijón (resolución ps-00189-2022). Pero existen otros ejemplos como el apercibimiento al Organismo Autónomo Regional Establecimientos Residenciales para Ancianos de Asturias (resolución: ps-00123-2022) o la Fundación Pública Andaluza para la Gestión de la Investigación en Salud de Sevilla (FISEVI) (resolución: ps-00220-2023).

Se incide en la idea, no hay razón alguna para que el sector privado pueda ser sancionado con multas económicas y el público no. Es una discriminación contraria a los artículos 20 y 21 de la Carta de Derechos Fundamentales de la Unión Europea y al artículo 14 de la Constitución Española, por lo que, debería realizarse, en mi opinión, una reforma del sistema sancionador.

6.2. Un régimen sancionador dual que resulta ineficaz

No se puede considerar útil un sistema sancionador cuyo principal objetivo es proteger el derecho fundamental a la protección de datos personales de las personas físicas cuando se prevén, por un lado, rigurosísimas sanciones a personas físicas y jurídicas del sector privado y, sin embargo, por otro lado, no se permiten imponer sanciones, solo de apercibimiento, a entidades y organismos del sector público.

La eficacia del sistema, como es lógico, disminuye exponencialmente. Solo una parte de los responsables y encargados de tratamiento sometidos al régimen europeo de protección de datos viven pendientes de las posibles consecuencias de incumplir sus obligaciones: es decir, las durísimas sanciones económicas. Este peligro no existe en el ámbito de lo público por lo que el miedo al incumplimiento es mucho menor, las consecuencias son mucho más débiles y, por consiguiente, el cuidado y la atención disminuye.

No es eficaz, por tanto, un sistema que prevé un régimen sancionador duro, para el sector privado, y blando, para el sector público. No es eficaz, repito, pero tampoco comprensible, porque las empresas y profesionales observan que sus posibles incumplimientos van a ser tratados de forma mucho más dura que los realizados por entes públicos. Y esto genera, como no puede ser de otra forma, resistencia en el cumplimiento e incomprensión por parte de los ciudadanos y empresas.

Es necesario, por consiguiente, equiparar las sanciones previstas para el sector público y el privado, de manera que se elimine esa sensación de impunidad y trato favorable del primero respecto al segundo.

6.3. Los tratamientos del sector público son especialmente arriesgados

A lo largo de este trabajo se ha venido haciendo referencia a que el legislador europeo ha sido especialmente cauteloso con los tratamientos efectuados por las Administraciones públicas y restantes entes del sector público. Hay un dato esencial, lógico por otra parte, que hace que estos tratamientos sean especialmente arriesgados: el ejercicio de potestades públicas y la relación de sujeción de los ciudadanos al poder público que representan las Administraciones.

No es el momento adecuado de realizar un análisis de las teorías del ejercicio del poder público, pero lo cierto es que en el ejercicio de potestades públicas las Administraciones gozan de potestades, prerrogativas y privilegios frente a las personas físicas y jurídicas privadas. No hay igualdad, así de claro. Tal y como prevé la LPACAP los actos de las Administraciones públicas se presumen válidos y surten efectos desde el momento en que se dictan[31], siendo, además ejecutables[32].

Sin perjuicio de los derechos que se reconocen a los ciudadanos y empresas en las leyes (LPACAP y LRJSP), lo cierto es que la posición de autotutela de las Administraciones es mucho más beneficiosa, desde el punto de vista jurídico, que la de las personas privadas. Por eso, en mi opinión, carece de sentido que, además, se les «premie» con la exención del pago de sanciones económicas.

Los tratamientos de datos efectuados por las Administraciones públicas son especialmente delicados: datos de salud, datos relativos a investigaciones criminales[33] datos sobre infracciones administrativas, datos de seguridad social, tributarios, huellas dactilares, patrimonio, origen racial, étnico, militancia política, afiliación sindical, entre otros muchos ejemplos. La información de la que disponen las Administraciones públicas puede hacer realidad la gran distopía imaginada por George Orwell y convertir a los Estados e verdaderos «Grandes Hermanos»[34].

Por eso no tiene sentido, según estimo, que, además, sus incumplimientos en materia de protección de datos queden impunes, es decir, sin ningún tipo de sanción económica. Es necesario, por tanto, incido en la idea, una revisión de este sistema en el sentido de permitir que se puedan imponer sanciones económicas.

La transformación digital en el sector público de Brasil ha sido una prioridad estratégica para el Gobierno Federal de Brasil en los últimos años. En este contexto, se han desarrollado iniciativas que buscan modernizar la Administración pública, optimizar los servicios ofrecidos a la ciudadanía y garantizar una gestión de datos eficiente y segura. Entre las principales herramientas creadas con este objetivo se encuentran la plataforma Conecta.gov.br y el Cadastro Base del Cidadão (CBC), elementos fundamentales para la interoperabilidad entre los sistemas públicos y la consolidación de una gobernanza digital centrada en el ciudadano.

La plataforma Conecta.gov.br fue desarrollada para facilitar la integración entre los sistemas y servicios digitales de los órganos y entidades de la Administración pública.

---

31 Artículo 39.1 de la Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas: «Los actos de las Administraciones Públicas sujetos al Derecho Administrativo se presumirán válidos y producirán efectos desde la fecha en que se dicten, salvo que en ellos se disponga otra cosa»

32 Artículo 98.1 de la misma Ley 39/2015: Los actos de las Administraciones Públicas sujetos al Derecho Administrativo serán inmediatamente ejecutivos [...]

33 Estos datos, por cierto, tiene un régimen todavía más laxo previsto en la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y en la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

34 En una noticia publicada en la página web de «La Sexta», «El 'Gran Hermano' de China, Rusia y EEUU: así usan la inteligencia artificial para vigilar a sus ciudadanos». Se pone de manifiesto los sistemas de crédito social que utilizan Estados como China, Rusia o Estados Unidos. Existe el riesgo de que la seguridad pública y un pretendido estado de «preguerra», pueda trasladar estos sistemas a la Unión Europea, aunque lo cierto es que el RGPD lo prohíbe. [última vez consultado el 2 de noviembre de 2024]

Su principal función es permitir el intercambio seguro, estructurado y eficiente de información entre diferentes niveles de gobierno (federal, estatal y municipal), promoviendo la interoperabilidad y reduciendo la redundancia de procesos.

Este entorno tecnológico permite que los sistemas públicos se comuniquen mediante APIs padronizadas, preservando la seguridad de los datos y garantizando que las instituciones compartan únicamente la información necesaria para el cumplimiento de sus finalidades legales.

El Cadastro Base del Cidadão (CBC) representa el mayor banco de datos personales del gobierno federal brasileño. Se trata de una base de datos unificada que consolida información personal de millones de brasileños, recopilada a partir de diversas fuentes oficiales, tales como la Receita Federal, el Ministerio de Salud, el INSS y los programas sociales.

Su propósito es integrar y estandarizar la información de los ciudadanos, permitiendo una visión única y confiable que mejore la entrega de servicios públicos y contribuya a la formulación de políticas públicas más efectivas.

Tanto la plataforma Conecta.gov.br como el CBC operan en conformidad con la Ley General de Protección de Datos Personales (LGPD), que regula el tratamiento de datos en el sector público y privado en Brasil. La ley impone principios como la finalidad, necesidad, transparencia y seguridad, los cuales deben guiar todas las actividades de tratamiento de datos personales por parte de los órganos públicos.

La interoperabilidad, en este sentido, debe estar acompañada de una gobernanza responsable, con controles de acceso, trazabilidad de las operaciones y mecanismos de rendición de cuentas, asegurando el respeto a los derechos de los titulares de los datos. Sin embargo, como hemos citado antes, no raras veces se há producido fuga de datos personales.

6.4. En otros sectores las Administraciones públicas pueden ser sancionadas

No se alcanza a comprender que en otros ámbitos o sectores como el de la protección del medio ambiente, vertidos, aguas, competencia, orden social, sin ánimo de ser exhaustivo, se pueden imponer multas económicas entre Administraciones públicas y no en el ámbito de la protección de datos.

Por poner un reciente ejemplo, la Sentencia del Tribunal Supremo 179/2023, de 15 de febrero (recurso de casación 430/2021), confirma la multa de 1 millón de euros impuesta al Ayuntamiento de San Cibrao Das Viñas (Ourense), por el Consejo de Ministros, por la comisión de una infracción muy grave contra dominio público hidráulico, prevista en el artículo 117 del Texto Refundido de la Ley de Aguas, aprobado por Real Decreto Legislativo 1/2001, de 20 de julio (en adelante, TRLA), en relación con los artículos 116-3.° de dicho Texto Legal y 326 y siguientes del Reglamento de Dominio Público, aprobado por Real Decreto 849/1986, de 11 de abril. Ninguno de los argumentos esgrimidos por el citado Ayuntamiento, ni tampoco el Tribunal Supremo lo trae a colación en la resolución, se hace referencia a la imposibilidad de imponer multas económicas a las Administraciones públicas.

Quiere esto decir, a mi entender, que no hay objeciones jurídicas a que una Administración pública pueda ser sancionada económicamente. Se hace habitualmente, sobre todo con los entes locales que, presupuestariamente tienen mayores problemas, por lo que tampoco puede ser un óbice la cuestión presupuestaria o que el dinero salga, al final, de los presupuestos generales de la Administración correspondiente.

6.5. No hay un aumento significativo del gasto público

Al hilo de lo manifestado en el último párrafo del epígrafe anterior, la imposición de multas a entes público no puede suponer un aumento significativo del gasto público salvo, quizás, para los pequeños municipios o entidades locales menores. En estos casos sí puede suponer un problema sobre todo teniendo en cuenta la cuantía de las sanciones.

No obstante, en estos últimos casos, al igual que el RGPD establece criterios de modulación para las sanciones[35] en el paso de personas físicas o pequeñas empresas, se pueden hacer lo mismo con las entidades locales más pequeñas.

Es más, tal y como señala la profesora Ortega Bernardo (Ortega Bernardo, 2017: 189), el hecho de que la multa, en última instancia, deban soportarla los ciudadanos con el pago de tributos, más que un inconveniente debe considerarse una ventaja, dado que puede llegar a ser un motivo para modificar el sentido del voto en relación con el Gobierno que ha cometido la infracción administrativa.

6.6. Principio de legalidad y la Administración pública como modelo de cumplimiento: nulidad más sanción y refuerzo del principio democrático

Otro de los argumentos que se puede utilizar en defensa de la revisión del actual sistema, tiene que ver con reforzar el principio de legalidad en la actuación administrativa y ampliar las consecuencias de la nulidad de la actuación administrativa.

Si mediante una actuación administrativa un ente público vulnera una obligación prevista en el RGPD, no basta con que dicho acto sea declarado nulo o anulable, sino que, en buena lógica, se habrá cometido, además, una infracción administrativa de las tipificadas en el artículo 83 del RGPD, por lo que habría que imponer la correspondiente sanción administrativa.

No basta en estos casos, en mi opinión, con establecer la actuación ilegal y declararla nula (vulnera un derecho fundamental), sino que tiene que haber más consecuencias. Los ciudadanos no entienden que la Administración que comete las mismas infracciones no sea sancionada en similares términos. No se trata solo de una cuestión de discriminación, que también, sino de reforzamiento del principio democrático. Que los ciudadanos vean que, ante los mismos hechos, todos, incluidas las Administraciones públicas, pueden ser sancionadas.

Todo ello, además, teniendo en cuenta que quien regula y sanciona debería ser absolutamente pulcro en el cumplimiento de las obligaciones que supervisa. Es decir, que la Administración debe ser un modelo de cumplimiento normativo, no ya solo porque ejerce poder público y los tribunales controlan la legalidad de su actuación, sino porque los ciudadanos exigen ese cumplimiento. De alguna manera, el hecho de que los entes públicos puedan ser sancionado por la comisión de infracciones en la misma manera que los ciudadanos refuerzan, si se permite la expresión, el principio democrático.

Esto genera una cuestión que no puede ser tratada en este trabajo pero que puede resultar interesante: ¿Quién controla al controlador?, es decir ¿Quién supervisa el cumplimiento de las obligaciones del RGPD por parte de las autoridades de control?

35 Directrices 04/2022, sobre el cálculo de las multas administrativas contempladas en el RGPD

Y no se debe olvidar que, estamos, en definitiva, ante un derecho fundamental cuya defensa debe ser prioridad para las Administraciones, sin perjuicio de otros derechos fundamentales que pueden entrar en conflicto y que habrá que ponderar, como es lógico.

7. Sanciones administrativas a las administraciones sí, pero con necesarios matices

No obstante, lo manifestado en el apartado anterior y la reivindicación que se hace en relación con una necesaria revisión del sistema que permita imponer sanciones económicas a los entes del sector público, lo cierto es que, según estimamos, también es necesario, de alguna manera, atemperar el régimen sancionador a la especial naturaleza de las Administraciones públicas.

Por ello, entendemos que, al igual que el Comité Europeo de Protección de Datos aprobó unas directrices sobre modulación de las sanciones (Directrices 04/2022, sobre el cálculo de las multas administrativas contempladas en el RGPD), sería conveniente, de revisarse el sistema, establecer unos criterios normativos mínimos que tuvieran en cuenta determinadas circunstancias como el tamaño del ente, su naturaleza territorial o institucional, las circunstancias del incumplimiento, etcétera. En definitiva, establecer unos matices necesarios atendiendo a la especial naturaleza de la misión que constitucionalmente tiene encomendada el sector público, es decir, servicio al interés general.

En esta línea, es necesario indicar que no puede ser tratado de la misma manera el incumplimiento que realizan los servicios de salud o de emergencia en una comunidad autónoma para salvaguardar la vida y a integridad física de los ciudadanos, que el que realiza una empresa pública que ofrece bienes y servicios en el mercado.

Todas estas cuestiones deberían tenerse en cuenta en una posible revisión del sistema. Una revisión que debe pasar, necesariamente, por una reforma del artículo 77 de la LOPDyGDD y por el correspondiente desarrollo reglamentario. En este sentido, dado que el legislador europeo ha dado libertad a los Estados para configurar las sanciones a las autoridades y organismos públicos, debe hacerse a través de normas jurídicas internas. No resulta aquí adecuada la aprobación de directrices por el Comité Europeo de Protección de Datos cuya naturaleza jurídica, dicho sea de paso, no queda muy clara. Los instrumentos de *soft law* pueden ser adecuados, quizás, en el sector privado (aunque tengo mis dudas), pero no, desde luego, en el sector público donde rige el principio de legalidad y debe haber un mínimo de densidad normativa para que las Administraciones públicas puedan actuar.

Presentada la cuestión en lo que concierne a UE y más en específico España, como se dijo anteriormente, tomamos la experiencia de Latinoamérica a partir de la Ley brasileña.

8. Conclusiones

El RGPD permite a los Estados miembros configurar libremente el régimen sancionador a las autoridades y organismos públicos. Es decir, imponer sanciones económicas o no, según el legislador nacional considere.

En España, el artículo 77.2 de la LOPDyGDD impide imponer multas económicas a las Administraciones y demás entes establecidos en el apartado primero del mimo artículo. En Brasil, el artículo 52 de la LGPD también lo impide. Pero, según estimamos, es necesario llevar a cabo una revisión de los dos sistemas para se permita imponer multas a estos entes públicos. Las razones son variadas.

No existe ninguna objeción jurídica que impida optar por este régimen. Es, además, según entiendo, discriminatorio que las sanciones económicas afecten solo al sector pri-

vado, amén de ineficaz. Las Administraciones públicas deben, en este sentido, ser modelos de cumplimiento normativo, sobre todo teniendo en cuenta que se trata de un derecho fundamental. No es suficiente con la declaración de nulidad de la actuación administrativa de que se trate o solamente imposiciones de sanciones limitativas del uso de los datos personales. Las consecuencias, en caso de incumplimiento y comisión de infracciones debe ser igual que en el sector privado, es decir, la imposición de sanción económica. Así se hace, sin mayor problema, en otros sectores del ordenamiento jurídico y está unánimemente aceptado por la doctrina.

Tampoco el presupuesto se verá gravemente afectado, y se refuerza, de paso, el principio democrático, es decir, los ciudadanos y empresas comprenderán que las normas son para todos y las consecuencias de su incumplimiento similares. En definitiva, que no hay excepciones ni islas de impunidad para el sector público.

Con ello no se quiere negar la especial naturaleza de las Administraciones y demás entes del sector público. Lógicamente, según entendemos, habrá que modular las correspondientes sanciones en función de la naturaleza específica del ente público. En esta línea, no puede ser igualmente considerado una pequeña Administración local, con problemas presupuestarios y que tiene encomendada por Ley la prestación de servicios públicos, que una gran empresa pública que ofrece bienes y servicios en el mercado.

No es de recibo, además, que dos de los países tradicionalmente más rigurosos, desde el punto de vista sancionador[36], sean especialmente débiles con su sector público, llegando a exonerar las sanciones económicas a los entes públicos.

Estimamos, por tanto, que la revisión es necesaria. Que los tiempos exigen una mayor responsabilidad del sector público, una mayor implicación con la defensa de este esencial derecho fundamental que se ha convertido, con la transformación digital, en una de las claves de bóveda del sistema de defensa de los ciudadanos frente a los avances tecnológicos más desarrollados. Especialmente, cuando el uso de estas tecnologías viene del poder público, es decir, de las Administraciones públicas que pueden imponer jurídicamente sus actos y ejecutar los mismos sin necesidad de acudir al Poder Judicial.

9. Bibliografía

Black, E. (2001). *IBM y el Holocausto: La alianza estratégica entre la Alemania nazi y la más poderosa corporación norteamericana*. Atlántida.

Calvo Rojas, E. (2003). «Algunas consideraciones sobre el procedimiento sancionador en el ámbito de la protección de datos personales», *Cuadernos de Derecho Público*, 19-20: 215-230.

Corral Sastre, A. (2024). «Las obligaciones de registro documental e información sobre hospedaje y alquiler de vehículos a motor en España a la luz de la normativa europea sobre protección de datos», *Revista Española de Derecho Europeo*, 90: 89-114

Comisión Europea, «Informe de la Comisión — Primer informe sobre la aplicación de la Directiva sobre protección de datos (95/46 CE) COM/2003/0265». Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52003DC0265&from=EN [Consulta 19 de octubre de 2024]

36 En la página web: https://www.enforcementtracker.com, se pueden comprobar la actividad sancionadora de las autoridades de control nacionales. Bien es cierto que las sanciones económicas más altas han sido impuestas, hasta ahora, por la autoridad irlandesa, pero lo cierto es que España tiene una actividad muy intensa desde el punto de vista sancionador.

Cerrillo i Martínez, A. (2019). «Las características del consentimiento del interesado y su incidencia en el tratamiento de datos en las Administraciones Públicas», *Consultor de los ayuntamientos y de los juzgados*, 3: 100-109.

Cervera Navas, L. (2023). «La apuesta de la Unión Europea por la protección global de los datos personales», en J. L. Piñar Mañas. (Dir.), *Privacidad en un mundo global*. Valencia: Tirant lo Blanch.

Copetti Cravo, D., Zago Gonçalves da Cunda, D., Ramos, R. (2021). *Lei Geral de Proteção de Dados e o Poder Público*. Porto Alegre: Tribunal de Contas do Estado do RGS. Disponíble en: https://lproweb.procempa.com.br/pmpa/prefpoa/pgm/usu_doc/ebook_lgpd_e_poder_publico_23052021.pdf. Acesso em: 09 maio 2024.

García Mexia, P. (2016) «La singular naturaleza jurídica del Reglamento General de Protección de Datos de la UE. Sus efectos en el acervo nacional sobre protección de datos», en J. L. Piñar Mañas. (Dir.), *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad.* Reus..

Green, M. C., Krosnick, J.A. y **Holbrook, A L.** (2001). *The survey response process in telephone and face-to-face surveys. Differences in respondent satisficing and social desirability response bias*. Disponible en web: http://www.Clas.ufl.edu/users/kenwald(pos6757/spring02/tch62.pdf [Consulta: 21 de septiembre de 2010]

Jiménez Asensio, R. (2019). «El nuevo marco normativo de la protección de datos personales: su aplicación a las entidades locales, *Anuario Aragonés del Gobierno Local:* 321-365.

Murillo de la Cueva, E. L. (2021). «Las autoridades autonómicas de protección de datos (Comentario al artículo 57 LOPDyGDD)», en A. Troncoso Reigada (Dir.) y J.J. González Rivas (Pr.), *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos personales y Garantía de los Derechos Digitales*. Thomson Reuters Aranzadi.

Ortega Bernardo, J. (2017). *¿Se puede sancionar a la Administración por la ilegalidad de su actuación?* II Congreso de la Asociación Española de Profesores de Derecho Administrativo. Madrid: INAP.

Piñar Mañas, J. L. (2016). «Introducción. Hacia un nuevo modelo europeo de protección de datos», en J.L. Piñar Mañas. (Dir.), *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad. Editorial Reus.*

Rodotà, S. (2008). *A vida na sociedade da vigilância — a privacidade hoje*. Organização, seleção e apresentação de Maria C. B. de Moraes. Trad. Danilo Doneda e Luciana C. Doneda. Rio de Janeiro: Renovar.

Romeo Ruiz, A. (2020). «La responsabilidad Proactiva de las Administraciones Públicas en la Protección de datos Personales», *Revista Vasca de Gestión de Personas y Organizaciones Pública*, 18: 138-153.

Tornos Más, J., (2008), «Potestad sancionadora de la Agencia Española de Protección de Datos y principio de proporcionalidad», en *La potestad sancionadora de la Agencia Española de Protección de Datos*. Madrid: Thomson-Aranzadi, pp. 33-50.

Troncoso Reigada, M. J. (2012) «Hacia un nuevo marco jurídico europeo de la protección de datos personales», *Revista Española de Derecho Europeo*, 43: 25-184.