El derecho a la protección de datos personales como límite a la transparencia administrativa en España*

The right to the protection of personal data as a limit to administrative transparency in Spain

Diana Paola González Mendoza[a]

Resumen / *Abstract*

La transparencia en las Administraciones Públicas resulta crucial para la participación de la ciudadanía en los asuntos públicos e igualmente para la toma de decisiones. Su vertiente negativa, esto es, el acceso a la información pública tiene bien definidos sus límites en la Ley de Transparencia, Acceso a la Información Pública y Buen Gobierno, entre los que se encuentra el derecho a la protección de datos personales. Este artículo está dedicado al análisis normativo, jurisprudencial y doctrinal de ambos derechos, tanto de manera separada como de forma conjunta, evidenciando el equilibrio necesario entre ellos.

Palabras clave: Transparencia, acceso a la información pública, datos personales, RGPD.

Transparency in Public Administrations is crucial for the participation of citizens in public affairs and also for decision making. Its negative aspect, that is, access to public information, has well

* Actividad financiada por la Unión Europea-NextGenerationEU, Ministerio de Universidades y Plan de Recuperación, Transformación y Resiliencia, mediante convocatoria de la Universidad de Oviedo MU-21-UP2021-030 70087867. Proyecto de investigación MCIU-22-PID2021-126784NB-I00 «Reorganización administrativa y de los servicios públicos a los ciudadanos en la post-pandemia» financiado por MCIN/AEI/10.13039/501100011033/ y por FEDER Una manera de hacer Europa

a. Institución: Universidad de Oviedo y Universidad de Cantabria. Contacto: gonzalezdiana@uniovi.es y dianapaola.gonzalez@unican.es

defined limits in the Law on Transparency, Access to Public Information and Good Governance, among which is the right to the protection of personal data. This article is dedicated to the normative, jurisprudential and doctrinal analysis of both rights, both separately and jointly, showing the necessary balance between them.

Keywords: *Transparency, accessit public information, personal data, GDPR.*

1. INTRODUCCIÓN

En todas las democracias avanzadas la transparencia resulta fundamental ya que permite conocer a los ciudadanos sobre los asuntos públicos, controlar la toma de decisiones de las autoridades públicas e incentiva y permite la participación ciudadana. Como en otras constituciones en la española no hay una referencia directa a la transparencia. No obstante, es innegable que es «*una dimensión irrenunciable de la legitimación democrática*» (Villaverde Menéndez, 2019). En palabras del Consejo de Transparencia y Buen Gobierno, esto es, el organismo público encargado de promover la transparencia a nivel estatal, la transparencia «*posibilita el escrutinio público y la fiscalización de la actividad pública, debe constituirse en eje fundamental de la acción política para garantizar la regeneración democrática, la eficacia y eficiencia del Estado y el crecimiento económico»* (CTBG, 2019) [1].

La creación y perfeccionamiento de las nuevas tecnologías han supuesto un verdadero reto para el derecho. Hasta enero de 2023 el número de usuarios de internet superaba los cinco mil millones, de acuerdo con el informe «Digital» realizado por la empresa «We are

1 CTBG, Criterio interpretativo 2/2019, de 20 de diciembre, p.7. El Consejo de Transparencia y Buen Gobierno es un organismo público con personalidad propia e independencia de actuación cuya finalidad es «promover la transparencia de la actividad pública, velar por el cumplimiento de las obligaciones de publicidad, salvaguardar el ejercicio de derecho de acceso a la información pública y garantizar la observancia de las disposiciones de buen gobierno», vid. Arts. 33 y 34 de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno (en adelante LTAIBG).

Social» (We are social, 2023). Y es que, en la actualidad la utilización de la web para el desarrollo de la personalidad o para el acceso a servicios acrecienta los riesgos derivados por la mala utilización de datos personales, que, en caso de materializarse, sus efectos desplegarían una onda expansiva debido a su alcance global. Es por ello que, cobra cada vez mayor relevancia el derecho de las personas a controlar quiénes tienen datos que los identifican o haga identificables, para qué los usan y por cuento tiempo[2].

Así pues, estos dos derechos cobran cada vez mayor importancia debido al avance tecnológico. Las Administraciones públicas españolas no son ajenas a la digitalización, la cual se ha venido implementando desde hace algunos años, sin embargo, esta se intensificó a causa de la pandemia de la Covid-19. Lo anterior se refleja en el Índice de Economía y Sociedad Digitales (DESI) realizado por la Unión Europea, en el cual España en materia de servicios digitales ocupa el quinto puesto de los veintisiete países miembros de la Unión Europea[3].

Este trabajo está dedicado al análisis del equilibro de ambos derechos, sin embargo, primeramente, se analizarán de forma separada para conocer su encaje en el ordenamiento jurídico español, de forma que, se hará un recorrido cronológico de las normas jurídicas que los regulan acompañado de un análisis doctrinal y jurisprudencial. Posteriormente, se profundizará en la relación que mantienen entre ellos, con es Finalmente, se dedicará un epígrafe al equilibrio necesario entre ellos.

2. LA TRANSPARENCIA ADMINISTRATIVA

La transparencia mantiene una estrecha relación con el acceso a archivos en poder de las Administraciones públicas, pues bien, la obtención de esa información pública

2 En relación con el contenido del derecho a la protección de datos personales he de decir que, a lo largo de las últimas décadas se han realizado diferentes denominaciones alrededor de este tales como «habeas data», libertad informática, y autodeterminación informativa. En relación con esta última, como bien señala Murillo de la Cueva este se acuña en 1983 por el Tribunal Constitucional Federal de Alemania «*para identificar ese bien jurídico, el constituido por el dominio del afectado sobre los datos relativos a su persona y su uso ajeno*» (Murillo de la Cueva, 2021).

3 Para posicionar a los diferentes miembros de la Unión Europea se valoran cinco indicadores: usuarios de la administración electrónica, formularios precumplimentados, servicios públicos digitales para los ciudadanos, servicios públicos digitales para empresas y datos abiertos (Comisión Europea, 2022).

o más bien el acceso a ésta, se regula de forma dispar en los ámbitos internacional, europeo y nacional. El acceso a la información ha tenido un desarrollo más antiguo y profundo en el plano internacional. El artículo 19 tanto de la Declaración Universal de Derechos Humanos como del Pacto Internacional de Derechos Civiles y Políticos regulan el derecho de las personas a buscar o investigar y a difundir informaciones[4]. El Comité de Derechos Humanos en su «Observación general Nº34» sobre el art. 19 Libertad de opinión y libertad de expresión determina que «*El párrafo 2 del artículo 19 enuncia un derecho de acceso a la información en poder de los organismos públicos. Esta información comprende los registros de que disponga el organismo público, independientemente de la forma en que esté almacenada la información, su fuente y la fecha de producción» (Comité de Derechos Humanos, 2011)*[5], el cual les ha sido reconocido especialmente a los medios de comunicación.

Por su parte, el Tribunal Europeo de Derechos Humanos (en adelante TEDH) interpretando el contenido del art. 10 del Convenio Europeo de Derechos Humanos (en adelante CEDH) ha determinado que no puede leerse como un derecho general de acceso a la información, ni correlativamente como una obligación de los Gobiernos a facilitarla[6]. Aun así, el acceso a la información está vinculado al derecho a la libertad de expresión contenido en el art. 10 del CEDH cuando periodistas, defensores de derechos humanos e incluso asociaciones traten de acceder a información de interés público, siempre que la información para su entrega no suponga su reelaboración. Pues estos sujetos hacen de "perros guardianes" de la democracia frente abusos del poder[7]. La previsión en estos tratados internacionales de este derecho a buscar o a investigar y difundir el resultado de esas actividades obliga, a la luz del art. 10.2

4 En la DUDH literalmente señala que se tiene derecho a «investigar y difundir informaciones», en el PIDCP se señala que se tiene la libertad de «*buscar, recibir y difundir informaciones de toda índole*».

5 Apartado 18 de la Observación general Nº34, Ginebra 11 a 29 de julio de 2011. Disponible en: http://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2FPPRiCAqhKb7yhsrdB0H1l5979OVGGB%2BWPAXiks7ivEzdmLQdosDnCG8FaqoW3y%2FrwBqQ1hhVz2z2lpRr6MpU%2B%2FxEikw9fDbYE4QPFdIFW1VlMIVkoM%2B312r7R.

6 Apartado 36 de la STEDH de 17 de febrero de 2015, caso Guseva contra Bulgaria (TEDH 2015\52590) y apartado 74 de la STEDH de 26 de marzo de 1987, caso Leander contra Suecia (TEDH 1987\4).

7 *Vid.* Apartados 37 y 38 de la STEDH de 17 de febrero de 2015, caso Guseva contra Bulgaria (TEDH 2015\52590) y del apartado 160 al 164 de la STEDH de 8 de noviembre de 2016, caso Magyar Helsinki Bizottság contra Hungría (JUR\2016\260055).

de la CE, a aplicarlos en ese sentido de manera indirecta en nuestro ordenamiento jurídico[8]. Las sentencias que interpreten su contenido se constituyen como «*criterios interpretativos que determinan el contenido constitucional y perfil exacto» (*Cotino Hueso, 2017).

En el marco del derecho de la Unión Europea, el art. 42 de la CDFUE establece el derecho a todo ciudadano de la Unión y a toda persona física o jurídica que resida en el territorio de la UE a «*acceder a los documentos de las instituciones, órganos y organismos de la Unión, cualquiera que sea su soporte». Este derecho de acceso ha sido reconocido como un derecho autónomo por el TJUE*[9] y, es aplicable a las instituciones de la UE. Aunque de conformidad con el contenido del art. art. 51 de la propia CDFUE su observancia sería extensiva a los Estados miembros siempre que apliquen el Derecho de la Unión[10].

Una vez que se ha repasado brevemente la configuración del acceso a la información en textos supranacionales es pertinente esclarecer su encaje jurídico a nivel nacional. El art. 105.b) de la Constitución Española (en adelante CE) establece que: «*La ley regulará: […]*

8 El art. 10.2 de la Constitución Española señala que: «*Las normas relativas a los derechos fundamentales y a las libertades que la Constitución reconoce se interpretarán de conformidad con la Declaración Universal de Derechos Humanos y los tratados y acuerdos internacionales sobre las mismas materias ratificados por España*».

9 Apartado 52 de la STJUE de 18 de julio de 2017 (JUR\2017\199987; ECLI:EU:C:2017:563).

10 El apartado 1 del art. 51 establece que: «*Las disposiciones de la presente Carta están dirigidas a las instituciones, órganos y organismos de la Unión, dentro del respeto del principio de subsidiariedad, así como a los Estados miembros únicamente cuando apliquen el Derecho de la Unión. Por consiguiente, éstos respetarán los derechos, observarán los principios y promoverán su aplicación, con arreglo a sus respectivas competencias y dentro de los límites de las competencias que los Tratados atribuyen a la Unión*». En la actualidad el art.42 de la CDFUE está desarrollado por el Reglamento (CE) n° 1049/2001 del Parlamento Europeo y del Consejo, de 30 de mayo de 2001, relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión, por el cual se regulan las situaciones excepcionales por las que se deniega el acceso, el procedimiento de acceso a los documentos, medidas de aplicación, el acceso por medios electrónicos, etc. Medio año antes, el 12 de enero del año 2001, se publicó en el DOCE (Diario Europeo de las Comunidades Europeas) un reglamento que vendría a compatibilizar a nivel comunitario al derecho de acceso a la información con el derecho a la protección de datos personales. El Reglamento 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos, instrumento de aplicabilidad directa, preveía la convergencia entre estos derechos y concretaba qué información debía proporcionarse a los interesados cuando la información hubiera sido o no recabada de los mismos, así como sus limitaciones: la investigación de delitos, seguridad nacional de los Estados miembros, la salvaguardia del interés económico (Cfr. Arts. 11, 12, 13 y 20 del Reglamento 45/2001). El Reglamento 45/2001 estuvo vigente durante casi dieciocho años, hasta que fue desplazado por el contenido del Reglamento 2018/1725 del Parlamento Europeo y del Consejo de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) 45/2001 y la Decisión 1247/2002/CE. Este reglamento es aplicable cuando se traten datos por instituciones y organismos de la UE, es decir, excluye de aplicación al RGPD. El mismos no afectaba los derechos y obligaciones de los Estados miembros contenidos en la entonces vigente Directiva 95/46/CE.

b) El acceso a los ciudadanos a los archivos y registros administrativos, salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas». Su ubicación dentro de la Constitución hace que se le niegue de forma sistemática su carácter de fundamental, por no estar incluido en la Sección 1ª del Capítulo II del Título I de la CE, de manera que, no goza de las garantías previstas en el art. 53.2 CE y puede desarrollarse a través de una ley ordinaria[11]. Sin perjuicio de su vinculación a los derechos fundamentales de participación en los asuntos públicos (art. 23 CE) y a recibir información (art. 20.1.d CE). Por tanto, la transparencia puede considerarse un medio de vigilancia que permite a los ciudadanos conocer si las administraciones públicas realizan su función tal y como ordena el art. 103.1 de la CE[12], de manera que, se configura también como principio rector de la actuación de estas. Como bien se*ñala la profesora* Rams Ramos *«si bien el art. 105 b CE establece un derecho subjetivo que podría calificarse de derecho de configuración legal y, por tanto, con eficacia diferida hasta que tenga desarrollo legislativo propio, el precepto jurídico sí es de aplicación directa e inmediata porque establece unos principios de actuación de las Administraciones Públicas que, como tales, no necesitan de desarrollo para ser inmediatamente aplicables»* (Rams Ramos, 2008)[13]. El Tribunal

11 En este sentido la Sentencia del TS de 30 de marzo de 1999 establece que: «Este precepto constitucional remite expresamente a la configuración legal el ejercicio del derecho de acceso a los archivos y registros administrativos, como derecho no fundamental, aunque relacionado con el derecho de participación política, con el de libertad de información y con el de tutela judicial efectiva. Refleja una concepción de la información que obra en manos del poder público acorde con los principios inherentes al Estado democrático (en cuanto el acceso a los archivos y registros públicos implica una potestad de participación del ciudadano y facilita el ejercicio de la crítica del poder) y al Estado de derecho (en cuanto dicho acceso constituye un procedimiento indirecto de fiscalizar la sumisión de la Administración a la ley y de permitir con más eficacia el control de su actuación por la jurisdicción contencioso-administrativa)», F.D. 3º de la STS de 30 de marzo de 1999 (RJ\1999\3246; ECLI:ES:TS: 1999:2206). Por tanto, como bien señala Mestre Delgado «*sirve para la consecución de otras finalidades constitucionales […] entre aquéllas se cuentan la existencia del sistema democrático, el derecho fundamental a la participación en asuntos públicos (art. 23.2 de la Constitución) el derecho de comunicar y recibir libremente información veraz (art. 20 CE) o, en fin, el principio de participación al que alude genéricamente el art. 9.2 CE*» (Mestre Delgado, 1993).

12 El contenido del art. 103.1 de la CE configura los pilares básicos de la actuación administrativa, este determina que «*La Administración Pública sirve con objetividad los intereses generales y actúa de acuerdo con los principios de eficacia, jerarquía, descentralización, desconcentración y coordinación, con sometimiento pleno a la ley y al Derecho*».

13 Así pues, para justificar la aplicabilidad directa de este principio constitucional determina que: «*entre los principios constitucionales, aquéllos que determinan una forma de ser concreta de los poderes públicos, deben de ser de aplicabilidad directa por conformar la necesaria forma de actuación de la Administración y, por tanto, formar parte esencial de la denominada "parte orgánica de la Constitución" que es, sin duda, de aplicación directa*» (Rams Ramos, 2008, p. 2016).

Supremo ya ha tenido ocasión de vincular el contenido de este derecho de configuración legal con otros derechos de corte fundamental, por ejemplo, en el caso que se pretenda comprobar la veracidad de informaciones en manos de la Administración: «*es un derecho derivado del artículo 20.1.d), pero que es imprescindible conectar en el caso examinado con el derecho establecido por el artículo 105.b), que concierne al acceso a los ciudadanos a los archivos y registros administrativos*»[14].

El derecho de acceso a archivos y registros fue desarrollado por el art. 37 de la hoy derogada Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (LRJPAC), de forma bastante limitada, ya que genéricamente las personas interesadas solo podían tener acceso a los registros y documentos en procedimientos ya concluidos a fecha de la solicitud. Si se pretendía acceder a documentos que tuvieran solo datos de carácter nominativo, con exclusión de aquellos de carácter sancionador o disciplinario, solo podían acceder a ellos los interesados y aquellas personas que acreditaran un interés legítimo y directo. El artículo antes referido limitaba el acceso cuando la autoridad competente alegara razones de interés público, intereses de terceros más dignos de protección o por disposición legal. Además, excluía el acceso si los documentos contenían: información sobre las actuaciones del Gobierno del Estado de las CCAA no sujetas al Derecho administrativo, informaciones relacionadas con la defensa o seguridad nacional, informaciones sobre la investigación de delitos siempre que supusieran peligro a la protección de derechos y libertades de terceros, informaciones protegidas por el secreto comercial o industrial, las relacionadas con la política monetaria y, todas aquellas informaciones que afectasen la eficacia del funcionamiento de los servicios públicos. Igualmente, en este artículo tampoco se establecía un procedimiento para la tramitación de dichas solicitudes, lo que ocasionó fácticamente problemas en la forma de acceder a la misma.

Después de poco más de veinte años de vigencia de la LRJPAC, la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno (LTAIBG), vio la luz, la cual «*alcanza tanto a la transparencia "activa" o publicidad, como al derecho de acceso de los ciudadanos a la información pública o transparencia "pasiva"*» (Razquin

14 F.D. 4º de la STS de 19 de mayo de 2003 (RJ 2003\3834; ECLI: ES:TS: 2003:3359).

Lizarraga, 2019)y, establece una diferenciación entre una y otra, tanto de su contenido como de sus límites. En este sentido, la Audiencia Nacional ha señalado que «*la principal diferencia entre el acceso a la información y la publicidad activa radica en que la primera se realiza mediante solicitud individualizada (artículo 17 de la Ley 19/2013) mientras que la segunda permite el acceso generalizado a la información (artículo 5 de la misma Ley)*[15]. La LTAIBG tiene carácter básico de acuerdo con su disposición final octava[16]. De manera que, a las Comunidades Autónomas les corresponde «*una competencia de desarrollo legislativo que va más allá de la mera adaptación de la ordenación estatal a las especialidades de su organización propia […]. En tal sentido, la legislación autonómica está perfectamente habilitada no sólo para complementar o desarrollar la legislación básica estatal, sino también para mejorar dichas garantías en su ámbito propio de aplicación*» (Fernández Ramos y Pérez Monguió, 2020)[17].

15 F.D. 5º de la SAN de 26 de marzo 2019 (JUR\2019\201813; ECLI:ES:AN:2019:2386).

16 Salvo lo relativo a la Administración General del Estado y al Consejo de Transparencia y Buen Gobierno. Además, de acuerdo con la disposición adicional primera se aplicará de manera supletoria siempre y cuando la normativa sectorial regule de manera específica el acceso a la información, por lo que «*la supletoriedad juega tanto en el caso de las normas sectoriales que únicamente prevén un régimen de reserva o confidencialidad de la información, como en el de las normas que diseñan un auténtico régimen especial, sustantivo y procedimental de acceso a la información en determinadas materias (por ejemplo, medio ambiente), para determinadas finalidades (por ejemplo, reutilización) o por determinados sujetos (por ejemplo, representantes políticos)*» (Guichot Reina, 2022).

17 En buena parte de las Comunidades Autónomas se han realizado un desarrollo legislativo en la materia. Salvo el País Vasco, todas las CCAA cuentan con una ley en la materia: Ley 10/2019, de 10 de abril, de Transparencia y de Participación de la Comunidad de Madrid; Ley 8/2018, de 14 de septiembre, de Transparencia, Buen Gobierno y Grupos de Interés. Comunidad Autónoma del Principado de Asturias; Ley 1/2018, de 21 de marzo, de Transparencia de la Actividad Pública. Comunidad Autónoma de Cantabria; Ley Foral 5/2018, de 17 de mayo, de Transparencia, acceso a la información pública y buen gobierno; Ley 4/2016, de 15 de diciembre, de Transparencia y Buen Gobierno de Castilla-La Mancha; Ley 1/2016, de 18 de enero, de transparencia y buen gobierno. Comunidad Autónoma de Galicia; Ley 3/2015, de 4 de marzo, de Transparencia y Participación Ciudadana de Castilla y León; Ley 8/2015, de 25 de marzo, de Transparencia de la Actividad Pública y Participación Ciudadana de Aragón; Ley 2/2015, de 2 de abril, de Transparencia, Buen Gobierno y Participación Ciudadana de la Comunitat Valenciana; Ley 1/2014, de 24 de junio, de Transparencia Pública de Andalucía; Ley 3/2014, de 11 de septiembre, de Transparencia y Buen Gobierno de La Rioja; Ley 12/2014, de 16 de diciembre, de Transparencia y Participación Ciudadana de la Comunidad Autónoma de la Región de Murcia; Ley 12/2014, de 26 de diciembre, de transparencia y de acceso a la información pública. Comunidad Autónoma de Canarias; Ley 19/2014, de 29 de diciembre, de transparencia, acceso a la información pública y buen gobierno. Comunidad Autónoma de Cataluña; Ley 4/2013, de 21 de mayo, de Gobierno Abierto de Extremadura; Ley 4/2011, de 31 de marzo, de la buena administración y del buen gobierno de las Illes Balears. Desde 2015 se está gestando Ley de Transparencia, Participación ciudadana y Buen Gobierno del Sector público vasco, sin que aún vea la luz. Sin embargo, esta Comunidad Autónoma cuenta con un órgano específico que se encarga de realizar el control de transparencia al amparo de la D.A. 4º de la Ley 19/2013 (art. 1 del Decreto 128/2016, de 13 de septiembre, de la Comisión Vasca de Acceso a la Información Pública).

Son varios los sujetos obligados al cumplimiento normativo de la LTAIBG sin embargo, en este caso nos centraremos en los que la propia ley considera como Administraciones públicas en su art. art. 2.1 de la LTAIBG[18]. A efectos de esta ley se consideran como Administraciones públicas a las administraciones territoriales, a las entidades gestoras y servicios comunes de la SS, a los organismos autónomos, Agencias y otras entidades investidas de independencia funcional o autonomía por ley y que tengan atribuidas funciones de supervisión o regulación y, a las entidades con personalidad jurídica propia que estén vinculadas o sean dependientes de cualquier Administración pública, «*incluidas las Universidades», de acuerdo con el contenido del art. 2.2 de la LTAIBG. Existen otros sujetos que la LTAIBG considera como «cooperadores»* y aunque no tienen una obligación directa de publicar información son personas físicas o jurídicas que prestan servicios públicos o ejercen potestades administrativas, incluidos los adjudicatarios de contratos. Estos cooperadores están obligados a proveer información a la Administración, organismo o entidad al que estén vinculadas, para que a su vez puedan cumplir con las obligaciones legales que les impone la LTAIBG, previo requerimiento, de acuerdo con el art. 4 de la referida norma legal.

La transparencia en sus dos formas tanto la activa como la pasiva tiene los mismos límites[19]: la seguridad nacional, la defensa, las relaciones exteriores, la seguridad pública, la prevención, investigación y sanción de los ilícitos penales, administrativos o disciplinarios, la igualdad entre partes en procesos judiciales y de tutela judicial efectiva, funciones administrativas de vigilancia y control, intereses económicos y comerciales, la política económica y monetaria, el secreto profesional, intelectual e industrial, los secretos en la toma de decisiones, la confidencialidad, la protección del medio ambiente y la protección de datos personales casi todos establecidos en el art. 14 de la LTAIBG, a excepción del derecho a la protección de datos personales,

18 Tanto el artículo 2 contempla como sujetos obligados a otras instituciones como la Casa real, el Congreso de los Diputados, el Senado, entre otras. En el art. 3 se contemplan también como sujetos obligados a los partidos políticos, sindicatos y organizaciones empresariales, sujetos que «*tienen constitucionalmente asignado un rol esencial en el funcionamiento de nuestro sistema democrático*» (CTBG, 2019b).

19 Conforme a los artículos 14 y 15 de la LTAIBG, así como en lo establecido en el criterio interpretativo del Consejo de Transparencia y Buen Gobierno y la Agencia Española de Protección de Datos 002/2015, de 24 de junio, aplicación de los límites al derecho de acceso a la información, p. 4.

contemplado en el art. 15. A este hay que sumarle otros derechos constitucionalmente protegidos como la intimidad de las personas, límite previsto en el propio art. 105.b) Constitucional.

3. EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES

En España el derecho a la protección de datos personales ha recorrido un largo periplo hasta ser considerado como un derecho fundamental. Esta consideración también se le reconoció en la Carta de Derechos Fundamentales de la Unión Europea. Sin embargo, el antecedente más remoto del derecho a la protección de datos personales en el derecho europeo lo encontramos en el Convenio Europeo para la protección de los Derechos Humanos y de las Libertades Fundamentales, del 4 de noviembre de 1950, adoptado por el Consejo de Europa (en adelante CEDH), en el cual se reconoce a las personas su derecho a la vida privada y familiar en el apartado 1 de su art. 8. Más tarde también en el marco del Consejo de Europa se aprobó el Convenio 108 de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, cuyo fin inicial era garantizar en los territorios parte, «*el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona ("protección de datos")*»[20].

Pues bien, el fundamento constitucional de este derecho lo encontramos en el apartado 4 del art. 18 de la CE, el cual establece que, «*La ley limitará el uso de la informática*

20 Recientemente, este Convenio se ha visto sustancialmente modificado por la introducción de su último protocolo (Protocolo que modifica el Convenio para la Protección de las Personas en lo que respecta al Tratamiento Automatizado de Datos Personales -CETS N° 223-, de 18 de mayo de 2018) pues se realiza un esfuerzo considerable en actualizar su contenido y reforzar el nivel de protección antes previsto, tanto dentro del continente europeo como fuera de sus fronteras. Pues recordemos que hasta antes de esta modificación algunos países latinoamericanos no pertenecientes al Consejo de Europa habían firmado y ratificado este Convenio: Argentina, Uruguay y México. De acuerdo con el actual contenido de su artículo 1, tiene por objeto, «*proteger a todos los individuos, sin importar su nacionalidad o residencia, con respecto al tratamiento de sus datos personales, de manera de contribuir al respeto de sus derechos humanos y libertades fundamentales y, en particular, al derecho a la privacidad*». Conviene destacar también que, de acuerdo las obligaciones de las partes previstas en el art. 4 de dicho Convenio, los Estados que pretendan adherirse o ratificar deberán haber tomado medidas legislativas que garanticen la aplicación efectiva del Convenio, de manera que, el Comité del Convenio podrá evaluar su efectividad en cada caso.

para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos», como se puede observar, esa «limitación de la informática» de manera aparente tiene una función meramente instrumental de la protección de algunos derechos de la personalidad[21]. De hecho, en el texto original de la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen se establecía en su disposición transitoria que «*En tanto no se promulgue la normativa prevista en el artículo dieciocho, apartado cuatro, de la Constitución, la protección civil del honor y la intimidad personal y familiar frente a las intromisiones ilegítimas derivadas del uso de la informática se regulará por la presente ley*». Esta situación perduró varios años, pues no fue hasta el año de 1992 cuando se aprobó la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (también conocida como la LORTAD). Sin embargo, la exposición de motivos de esta ley es muy clara «*su finalidad es hacer frente a los riesgos que para los derechos de la personalidad puede suponer el acopio y tratamiento de datos por medios informáticos*».

Posteriormente, en el marco de la Unión Europea se aprobó 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 respeta al tratamiento de datos personales y a la libre circulación de estos datos. Esta directiva parte del contenido del Convenio 108, ya que precisa y amplía los principios de protección y las libertades de los individuos contenidos en este[22], como consecuencia de la utilización de nuevas tecnologías para el tratamiento y transmisión de datos personales. El objeto de la directiva era «*la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales*» (art. 1.1). Así pues, por muchos años fue considerada como «*ley básica o general de la UE en la materia, con el cometido de armonizar la protección de los derechos y las libertades*

21 Se consideran como derechos de la personalidad al derecho a la intimidad personal y familiar, al derecho a la propia imagen y al derecho al honor. Estos tienen una cualidad de irrenunciables y se recogen en el apartado 1 del art. 18 de la CE. La Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, la intimidad personal y familiar y a la propia imagen regula tanto la protección de estos derechos y el procedimiento a llevar a cabo por posibles intromisiones.

22 Lo anterior, de conformidad con el contenido del considerando 11 de la propia Directiva 95/46/CE.

fundamentales de las personas físicas en relación con las actividades de tratamiento de datos de carácter personal y garantizar la libre circulación de estos datos entre los Estados miembros» (Tomás Mallén, 2019). Esta directiva necesitaba una norma que transpusiera su contenido al ordenamiento jurídico español, es por ello que se aprueba en España la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante LOPD)[23], la cual consagraba «*en nuestro Ordenamiento los dos pilares básicos del tratamiento de datos de carácter personal, de una parte, el del consentimiento del afectado y, de otra parte, el derecho a la información del mismo*» (Piñar Mañas, 2006). Esta LOPD también contenía otros principios relativos a la calidad de los datos y los denominados derechos ARCO (acceso, rectificación, cancelación y oposición). Establecía al igual que la LORTAD que la Agencia Española de Protección de Datos se configuraba como la autoridad de control en la materia a nivel estatal; preveía un régimen aplicable a las transferencias internacionales de datos personales y contemplaba también un régimen de infracciones y sanciones.

Un año más tarde, se llevaron a cabo dos sucesos que sin duda cambiarían la configuración del derecho a la protección de datos personales, pues hasta ahora, por lo menos a nivel nacional lo que se trataba de proteger era la intimidad de las personas[24]. El primero de ellos fue su reconocimiento como derecho fundamental por el Tribunal Constitucional en los

23 *Este tipo de normas pertenecientes al derecho derivado de la Unión Europea obligan «al Estado miembro en cuanto al resultado que deba conseguirse, dejando, sin embargo, a las autoridades nacionales la elección de la forma y de los medios (art. 288, ap. 3º, TFUE), fuerza a la reserva de espacios de decisión a favor de los Estados Miembros e impide considerarla una fuente apta para desplazar a la Ley nacional. La necesaria recepción de la misma en el nivel interno trae consigo, en definitiva, la no relativización, como punto de partida, de las exigencias impuestas por el principio constitucional de la reserva de ley» (Díaz González, 2016). En este caso, de acuerdo con el contenido del art. 81.1 de la CE era necesario realizar la transposición a través de una ley orgánica.*

24 Como hemos visto antes a nivel europeo el Consejo de Europa habla de la protección a la privacidad de las personas. Sin embargo, los términos de privacidad e intimidad no son equiparables. Encontramos en varios textos legales el término «privacidad»: art. 12 de la Declaración Universal de Derechos Humanos, art. 17 del Pacto Internacional de Derechos Civiles y Políticos e incluso, así se recoge también en el art 7 de la Carta de Derechos Fundamentales de la Unión Europea. El Tribunal Europeo de Derechos Humanos por sentencia de 7 de febrero de 2012 determina qué debe entenderse por «vida privada»: «*comprende elementos que hacen referencia a la identidad de la persona tales como el nombre, sus fotos, su integridad física y moral; la garantía que ofrece el artículo 8 del Convenio está destinada principalmente a asegurar el desarrollo, sin emergencias externas de la personalidad de cada individuo en relación con sus semejantes*». Por su parte el art. 18.1 de la Constitución Española reconoce el derecho a la intimidad, el profesor Villaverde Menéndez señala que, «*la privacidad es el género, la intimidad una de sus especies*» (Villaverde Menéndez, 2013). Al hilo de esto el profesor Carrillo al referirse a la intimidad señala que esta consiste en «*aquel ámbito de la vida privada que resulta inaccesible a los demás salvo que medie su propio consentimiento, es un concepto más restringido del que materialmente sirve para definir el ámbito de lo privado*» (Carrillo, 2016).

siguientes términos: «*Este derecho fundamental a la protección de datos (...) atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos cuya concreta regulación debe establecer la Ley, aquella que conforme al art. 18.4 CE debe limitar el uso de la informática, bien desarrollando el derecho fundamental a la protección de datos (art. 81.1 CE), bien regulando su ejercicio (art. 53.1 CE)(...) el objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal. Por consiguiente, también alcanza a aquellos datos personales públicos, que por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos. También por ello, el que los datos sean de carácter personal no significa que sólo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona*» (STC 292/2000, de 30 de noviembre)[25]. El segundo suceso ocurrió el 7 de diciembre del año 2000 con la proclamación de la Carta de Derechos Fundamentales de la Unión Europea (en adelante CDFUE) en Niza[26]. La CDFUE reconoce al derecho a la protección de datos personales. Sin embargo, no es hasta la entrada en vigor del Tratado de Lisboa en 2009 que la carta adquiere el mismo valor que «los Tratados», esto es, Tratado de la Unión Europea (TUE) y el Tratado de Funcionamiento de la Unión Europea (TFUE)[27].

25 Como es bien sabido, para que un derecho sea considerado como fundamental, primeramente, debe situarse en dentro de la Sección 1ª del Capítulo II del Título I de la CE. Ahora bien, como bien señala la profesora Ruiz Palazuelos para que un derecho fundamental sea considerado como tal, también es necesario otras dos cuestiones, la noción jurídica de su objeto y la existencia de un régimen jurídico particular (Ruiz Palazuelos, 2021).

26 De acuerdo con el profesor Martinico, la CDFUE en su momento dio «*energía al debate sobre la redacción de una constitución europea porque ha representado el momento de la codificación de los derechos fundamentales a nivel supranacional y supera la lógica del ius pretorio del TJUE en este campo. Aunque este documento no fue inmediatamente vinculante desde el punto de vista jurídico, en sentido estricto, su proclamación favoreció un importante debate entre los estudiosos, sobre todo entre los constitucionalistas de la Europa continental*» (Martinico, G., 2015).

27 El art. 16 del TFUE prevé también el respeto al derecho a la protección de datos personales.

Durante el periodo de aplicación de la Directiva 95/46/CE y de la LOPD como es lógico las tecnologías de la información y comunicación (TIC) fueron perfeccionándose, se encontraron nuevas aplicaciones a las ya existentes, y tanto la web como internet se convirtieron en dos herramientas imprescindibles en un mundo globalizado. Aunado a esto, la transposición de la Directiva 95/46/CE en los distintos Estados miembros resultaba dispar y, por tanto, de aplicación fragmentada. Debido a la necesidad de contar con un marco jurídico sólido en la materia, se comienza a tramitar en 2012 la propuesta de un nuevo reglamento de protección de datos personales. No fue hasta el año 2016 que 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 (Reglamento general de protección de datos)[28], este supone un hito para la protección de datos personales, ya que refuerza el sistema de principios y derechos que se contenían en la anterior directiva, regula de manera detallada lo relativo a los flujos internacionales de datos personales, se crea un sistema de ventanilla única que beneficia a los titulares del derecho en cuanto a la forma de presentar una reclamación, igualmente crea un mecanismo de cooperación y coherencia al que están sujetas las diversas autoridades de control de los distintos Estados miembros y quizás lo más importe evita «*las divergencias en la ejecución y aplicación de la Directiva, con poderes equivalentes en los veintisiete Estados para supervisar y garantizar el cumplimiento de las reglas bajo sanciones equivalentes*» (Ballesteros Moffa, 2020).

Más adelante, con objeto de completar el contenido del RGPD se aprueba la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Esta ley además de prever cuestiones que no se regulan por el RGPD y que son competencia del legislador español tiene una peculiaridad en relación con las anteriores leyes orgánicas en la materia, y es que, de acuerdo con su disposición final primera, esta ley tiene carácter de ley orgánica, sin embargo, algunos de sus preceptos tienen carácter de ley ordinaria, en este sentido el profesor Tolivar Alas apunta que, «*La reserva de ley orgánica tampoco es incompatible con la complementación por ley ordinaria, que puede ser llamada*

28 Sin embrago, se comenzó a aplicar a partir del 25 de mayo de 2018, conforme a su art. 99.

por aquella a integrar en algunos extremos sus disposiciones a modo "de desarrollo", siempre y cuando no se efectúe "un reenvío en blanco o en condiciones tan laxas que viniesen a defraudar la reserva constitucional en favor de la ley orgánica"» (Tolivar Alas, 2018). De manera que, tienen carácter de ley ordinaria mayormente las disposiciones relativas a los llamados «derechos digitales».

Es importante señalar que durante todos estos años la jurisprudencia ha jugado un papel crucial en delimitar tanto el contenido como el alcance del derecho a la protección de datos personales. En España esta labor no solo la ha realizado el Tribunal Constitucional, también otros tribunales pertenecientes al poder judicial, mayoritariamente el Tribunal Supremo y la Audiencia Nacional[29]. Lo anterior, sin restarle importancia a la destacada labor realizada por el Tribunal de Justicia de la Unión Europea, quien se ha encargado de interpretar el contenido de la Directiva 95/46/CE. Y finalmente pero no por ello menos importante, la labor que realizan las autoridades de control en la materia, y en especial en España la realizada por la Agencia Española de Protección de Datos.

4. EL EQUILIBRIO NECESARIO ENTRE LA TRANSPARENCIA Y EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES

Las administraciones públicas, el sector público institucional y aquellas personas físicas o jurídicas que presten servicios públicos, incluidos los adjudicatarios de contratos del sector público tratan datos personales en cantidades ingentes. Las Administraciones públicas y el sector público, genéricamente encuentran su base de licitud del tratamiento de datos personales en los incisos c) y e) del art. 6.1 del RGPD[30]. En el caso de las personas físicas o jurídicas que presten servicios públicos, además de regirse por su por su normativa específica, encuentran la licitud del tratamiento de datos personales en el cumplimiento de una misión realizada en aras de un interés público, como la prestación de un servicio (finalidad del tratamiento), y, por tanto, sujetos a obligaciones específicas de servicio

29 De conformidad con el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso Administrativa.

30 Tal como se reconoce en el apartado II del informe 175/2018 de la AEPD. Disponible en: https://www.aepd.es/es/documento/2018-0175.pdf

público, convirtiéndose en encargados del tratamiento[31]. Además, de acuerdo con el art. 13.h) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, la protección de datos de carácter personal se considera como un derecho que tienen las personas en sus relaciones con las Administraciones Públicas y, en particular, este inciso del art. 13 hace referencia a «*la seguridad y confidencialidad de los datos que figuren en ficheros, sistemas o aplicaciones de las Administraciones Públicas*», lo que guarda relación con los principios establecidos en el art. 5 del RGPD, especialmente con el principio de «integridad y seguridad» (art. 5.1.f RGPD). En el inciso d) del referido artículo también se establece como derecho de las personas frente a las Administraciones Públicas «al acceso a la información *pública, archivos y registros*» el cual hace referencia directa a la LTAIBG.

Como se ha podido observar, el derecho a la protección de datos personales y el de transparencia entendido en su vertiente pasiva guardan una estrecha relación. Sin embargo, ha de ponderarse en todo caso la preeminencia de uno sobre otro y en qué medida. El preámbulo de la LTAIB nos algunas pistas de cómo se aplican los mecanismos de equilibro previstos en esta: *«Así, por un lado, en la medida en que la información afecte directamente a la organización o actividad pública del órgano prevalecerá el acceso, mientras que, por otro, se protegen –como no puede ser de otra manera– los datos que la normativa califica como especialmente protegidos, para cuyo acceso se requerirá, con carácter general, el consentimiento de su titular»* (LTAIBG).

El artículo 15 de la LTAIBG modula la relación entre el derecho a la protección de datos y la transparencia, siendo el primero límite del segundo. La protección de datos personales dentro de la ley LTAIBG según el profesor Guichot Reina, confiere tres círculos de protección con base en el art. 15 de la misma norma. En el círculo más amplio se encuentran los datos personales que contienen datos meramente identificativos, también llamado «circulo externo». Después encontramos un «círculo medio» dónde encontramos datos personales genéricos, es una especie de círculo residual, en el que se hayan datos

31 Aunque actúa por cuenta de otro y se traten datos para el cumplimiento de un contrato, los datos que se van a tratar no son los del contratista sino de los usuarios del servicio que gestionan, por tanto, la base del tratamiento no puede ser el inciso b) del art. 6.1 del RGPD. A lo que se le debe sumar que los fines del tratamiento cuando se presta un servicio público vienen delimitados por una norma de rango legal, que autoriza este tipo de contratos y que conforme con lo establecido en el 33.2 la posición jurídica del prestador de servicios públicos sería el encargado del tratamiento.

personales que no pertenecen al círculo anterior ni datos del «círculo interno» en el que se contienen los datos especialmente protegidos o también llamados de categorías especiales (Guichot Reina, 2018).

De acuerdo con el RGPD y la LOPDGDD los datos personales son clasificados en «datos personales» (art. 4.1 RGPD) y «datos personales de categorías especiales» (art. 9.1 RGPD). Los datos de categorías especiales (art. 9.1 RGPD) a la luz de la normativa de la LTAIBG pueden a su vez dividirse en dos grupos, en el primero se encuentran aquellos que puedan revelar la ideología, afiliación sindical, religión o creencias religiosas de las personas; en el segundo grupo, estarían los datos personales que hagan referencia al origen racial, a la salud o a la vida sexual, incluidos los datos genéticos o biométricos. El contenido del círculo residual y del círculo externo a los que hace referencia el profesor Guichot Reina, desde la perspectiva de la normativa de protección de datos serían datos personales genéricos (art. 3.1 RGPD), ya que el RGPD no habla de datos meramente identificativos y la LOPDGDD tampoco los regula de manera directa[32]. La modulación de este tipo de datos a la luz de la LTAIBG es distinta y en buena medida depende del contenido de la información, es decir, si los datos son o no meramente identificativos. Con el nuevo marco normativo en protección de datos, estos datos genéricos tienden a minimizarse por defecto incluso antes de comenzar su tratamiento teniendo en cuenta siempre las finalidades y su base de licitud.

Los datos personales tanto de categorías especiales como genéricos pueden ser recabados directamente del interesado o no, y dependiendo del caso se le tendrá que proporcionar determinada información descrita en los arts. 13 y 14 del RGPD, respectivamente. De cualquier forma, cuando se vaya a realizar algún tratamiento de datos de cualquier tipo, se debe cumplir con el principio de transparencia regulado en el art. 12 del RGPD. Consecuentemente la información que se proporcione al interesado deberá ser: concisa,

32 Por su parte el profesor Razquin Lizarraga habla de «niveles de protección», concretamente tres. Los primeros dos niveles se contienen datos que el RGPD considera de «categorías especiales» (art.9 RGPD), sin embargo, se subclasifican en datos ideológicos y datos relativo a la salud. Otra diferencia entre estos dos niveles radica en que en el segundo caso «*una ley puede amparar el acceso por razones de interés legal*». El tercero de los niveles se refiere a aquellos que no son especialmente protegidos, esto es, cualquier dato personal que identifique o haga identificable a los individuos, lo cual «*provoca la inversión de la regla de la denegación salvo consentimiento, que se transforma aquí en acceso previa ponderación*». Finalmente, se refiere a los datos meramente identificativos en cuyo caso «*rige la regla de acceso general*» (Razquin Lizarraga, 2015).

transparente, inteligible, de fácil acceso, con lenguaje claro y sencillo, por escrito u otros medios (preferentemente electrónicos), y en relación con sus derechos contemplados del art. 15 al 22: acceso, rectificación, supresión, acerca de las limitaciones del tratamiento, portabilidad, oposición, a saber si se toman decisiones individuales automatizadas. Igualmente, se les deberá dar a conocer la identidad y los datos de contacto del responsable, los datos del contacto del DPD, los fines del tratamiento, plazo de conservación. En su caso, si la recogida de datos es una obligación o un requisito legal y las consecuencias de no facilitarlos.

De acuerdo con el Criterio interpretativo del CTBG y la AEPD 004/2015, de 23 de julio de 2015 son considerados datos meramente identificativos: el nombre, apellidos, dirección o teléfono, así como «*otros datos que identifican la posición del afectado dentro de la organización administrativa, como los relacionados con la identificación de rango o puesto de trabajo»* (CTBG y AEPD, 2015b). En este sentido el profesor Razquin Lizarraga dispone que aquellos otros datos «*que excedan de lo anterior ya no son datos meramente identificativos y se incardinan en el tipo anterior de datos personales no sensibles. Así, pues, los datos como el número de DNI de NIF o de pasaporte, el domicilio, el correo electrónico o el número de móvil no son datos meramente identificativos»* (Razquin Lizarraga, 2019).

El límite del art.15 y los parámetros de ponderación no serán aplicables a los datos que son disociados cuando deba ser entregada con motivo de una solicitud[33], esto es que, que no se identifiquen o no se puedan identificar a las personas titulares de la información que se proporciona. De acuerdo con el Diccionario de la lengua española, disociar supone separar algo de otra cosa a la que estaba unida (Diccionario de la lengua Española, 2022). Sin embargo, el hecho de que se incluya o no la información puede deberse a que esta esté anonimizada o seudonimizada, según sea el caso por sí misma en el tratamiento o que se haya «disociado» a efectos de entregar la información sin entrar en la ponderación que determina el art. 15. En el primero de los casos, hablamos de anomimización cuando se rompe la cadena de identificación y su finalidad es «*eliminar o reducir al mínimo los riesgos de reidentificación de los datos anonimizados manteniendo la veracidad de los resultados*

33 Cfr. Arts. 5.3, 15.4 y 24 de la LTAIBG.

del tratamiento de los mismos, es decir, además de evitar la identificación de las personas, los datos anonimizados deben garantizar que cualquier operación o tratamiento que pueda ser realizado con posterioridad a la anonimización no conlleva una distorsión de los datos reales. Un análisis masivo de los datos o macrodatos que puedan derivar de los datos anonimizados no debería diferir del análisis que pudiera obtenerse si hubiera sido realizado con datos no anonimizados» (AEPD, 2016). Si la anonimización pudiera garantizarse al cien por cien, solo en ese caso, implicaría la inaplicación de la normativa en materia de protección de datos, pues no sería posible ya identificar a las personas. No obstante, suele ser habitual que no se rompa esa «cadena de anonimización*», bien por metadatos que permiten la identificación directa o por aquellos que permiten indirectamente de manera cruzada la identificación. En ese caso le seguiría siendo de aplicación la normativa en materia de protección de datos.*

En cambio, estaríamos ante una seudonimización cuando al entregar la información se borren los datos de las personas de manera que no puedan identificarse, pero en el tratamiento de datos personales esta información se encuentre permanentemente separada y, por tanto, se sigue aplicando la normativa de protección de datos vigente[34].

5. CONSIDERACIONES FINALES

Como se ha advertido antes el derecho a la protección de datos personales y la transparencia mantienen una estrecha relación, sin embargo, es imprescindible realizar una ponderación entre estos dos derechos en cada caso concreto. Contrariamente, si de forma generalizada se le diera preferencia a uno de estos derechos sobre el otro se estaría aceptando su carácter absoluto. La importancia de estos dos derechos es innegable en una sociedad globalizada y cada vez más automatizada.

La necesidad de utilizar medios electrónicos y herramientas informáticas se hizo mucho más visible a raíz de la crisis sanitaria provocada por la SARS-CoV-2. De

34 Pues tal y como señala el art. 4.5 del RGPD la seudonimización supone que «*ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable».*

forma que, la digitalización en las Administraciones públicas ha supuesto un cambio sustancial, sobre todo en sus relaciones *ad extra* y especialmente con las personas. Así pues, los ciudadanos cada vez más utilizan los medios electrónicos para relacionarse con las diferentes Administraciones públicas, de manera, que estas están obligadas a implementar medidas técnicas y organizativas que aseguren la integridad de los datos y su seguridad.

La tramitación de las solicitudes de acceso a la información en el marco de la LTAIBG puede realizarse a través de medios electrónicos, lo cual implica una serie de problemas sobre todo en materia de protección de datos personales. Y es que, aunque los datos est*én anonimizados o* seudonimizados hay que poner especial atención en los metadatos que se incorporan en el documento electrónico. Tal y como exige la normativa en materia de protección de datos personales, los responsables del tratamiento deberán asegurar el cumplimiento de los principios rectores de la materia, incluidas las Administraciones públicas. El siguiente paso sería dar repuesta a los problemas derivados de la inclusión de metadatos en los documentos electrónicos partiendo de los principios en materia de protección de datos personales: responsabilidad proactiva, minimización, exactitud, integridad y confidencialidad. Además, sería conveniente que la normativa excluyera los metadatos que puedan identificar o hacer identificables a las personas en la entrega de documentos electrónicos. Ahora bien, de forma inversa, la transparencia se constituye como una herramienta crucial para conocer cómo funcionan estas nuevas tecnologías y qué implicaciones pueden llegar a tener en la esfera jurídica de las personas, puesto que la tecnología basada en algoritmos ya está aquí.

6. BIBLIOGRAFÍA.

Ballesteros Moffa, L.Á. (2020). *Las fronteras de la privacidad. El conflicto entre seguridad pública y datos personales en una sociedad amenazada y tecnológica.* Comares.

Carrillo, M. (2016). Los ámbitos del derecho a la intimidad en la sociedad de la comunicación. En *El derecho a la privacidad en el nuevo entorno tecnológico: XX Jornadas de la Asociación de Letrados del Tribunal Constitucional.* Centro de Estudios Políticos y

Constitucionales.

Cotino Hueso, L. (2017). El reconocimiento y contenido internacional del acceso a la información pública como derecho fundamental. *Teoría y realidad constitucional*, 40, pp. 279-316. https://doi.org/10.5944/trc.40.2017.20910

Díaz González, G.M. (2016). *La reserva de ley en la transposición de las directivas europeas*. Iustel.

Fernández Ramos, S. y Pérez Monguió, J. M. (2020). *El derecho de acceso a la información pública en España*, 2ª edición. Thomson Reuters Aranzadi.

Guichot Reina, E. (2018). Transparencia y protección de datos en las Universidades Públicas. *Revista Española de Derecho Administrativo*, 193, pp. 85-126.

Guichot Reina, E. (2022). La supletoriedad de la normativa general sobre transparencia respecto a las regulaciones especiales de acceso a la información. *Revista española de Derecho Administrativo,* 221, pp. 81-108.

Martinico, G. (2015). I. Una introducción terminológica: qué queremos decir con 'constitucionalización', 'derecho constitucional' y 'Constitución de la Unión Europea'. En Gordillo, L. y Martinico, G., *Historias del país de las hadas. La jurisprudencia constitucionalizadora del Tribunal de Justicia* (pp. 13-46). Thomson Reuters- Civitas.

Mestre Delgado, J.F. (1993). *El derecho de acceso a archivos y registros administrativos [Análisis del art. 105.b) de la Constitución]*. Civitas.

Murillo de la Cueva, P.L. (2021). El objeto del Reglamento General de Protección de datos y de la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (comentario al artículo 1 RGPD y al artículo 1 LOPDGDD). En A. Troncoso Reigada (Dir.), *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales*, Tomo I (pp.303-324). Thomson Reuters- Civitas.

Piñar Mañas, J.L. (2006). El derecho fundamental a la protección de datos personales. En J.L. Piñar (Dir.), *Protección de datos de carácter personal en Iberoamérica* (pp. 19-35). AEPD – Tirant lo blanch.

Rams Ramos, L. (2008). *El derecho de acceso a archivos y registros administrativos.* Reus.

Razquin Lizarraga, M.M. (2015). *El derecho de acceso a la información pública*. Instituto

Vasco de Administración Pública.

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

Ruiz Palazuelos, N. (2021). La libertad de creación artística, ¿Un derecho autónomo? ("L'oiseau rebelle" en la Constitución y en la jurisprudencia constitucional). *Revista de Administración Pública,* 215, pp. 111-142. https://doi-org.uniovi.idm.oclc.org/10.18042/cepc/rap.215.04

Tolivar Alas, L. (2018). Leyes Orgánicas. En Pendás, B. (Dir.), *España Constitucional (1978-2018). Trayectorias y perspectivas*. Tomo III (pp. 2033-2050). Centro de Estudios Políticos y Constitucionales.

Tomás Mallen, B. (2019). Las sinergias entre el Reglamento General de Protección de Datos de la Unión Europea y el Convenio 108+ del Consejo de Europa. En García Mahamut, R. y Tomás Mallén, B. (Ed.), *El Reglamento General de Protección de Datos. Un enfoque nacional y comparado. Especial referencia a la LO 3/2018 de Protección de Datos y garantía de los derechos digitales* (pp. 57-91). Tirant lo blanch.

Villaverde Menéndez, I. (2013). La intimidad, "ese terrible derecho" en la era de la confusa publicidad virtual. *Espaço Jurídico: Journal of Law*, 14 (3), 57-72. https://dialnet.unirioja.es/descarga/articulo/4546679.pdf

7. OTRAS FUENTES CONSULTADAS

AEPD (2016). Orientaciones y garantías en los procedimientos de anonimización de datos personales. https://www.aepd.es/documento/guia-orientaciones-procedimientos-anonimizacion.pdf

AEPD (2018). Informe 175/2018. https://www.aepd.es/es/documento/2018-0175.pdf

Comisión Europea (2022). Índice de Economía y Sociedad Digitales (DESI). https://digital-strategy.ec.europa.eu/es/policies/desi

Comité de Derechos Humanos (2011). Observación general Nº34, Ginebra 11 a 29 de

julio de 2011. http://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG-1d%2FPPRiCAqhKb7yhsrdB0H1l5979OVGGB%2BWPAXiks7ivEzdmLQdosD-nCG8FaqoW3y%2FrwBqQ1hhVz2z2lpRr6MpU%2B%2FxEikw9fDbYE4QPF-dIFW1VlMIVkoM%2B312r7R

CTBG (2019). Criterio interpretativo 2/2019, de 20 de diciembre. https://www.consejodetransparencia.es/ct_Home/Actividad/criterios/2-2019.html

CTBG (2019b). Criterio interpretativo 3/2019, de 20 de diciembre. https://www.consejodetransparencia.es/ct_Home/Actividad/criterios/3-2019.html

CTBG y AEPD (2015). Criterio 002/2015, de 24 de junio, de aplicación de los límites al derecho de acceso a la información. https://docs.google.com/viewer?url=https%3A%2F%2Fwww.consejodetransparencia.es%2Fdam%2Fjcr%3A77d11404-2f9a-45e6-be70-d6c96409acd5%2FC2_2015_limites_derecho_de_informacion.pdf

CTBG y AEPD (2015b). Criterio 004/2015, de 23 de julio de 2015, Publicidad activa de los datos del DNI y de la firma manuscrita. https://docs.google.com/viewer?url=https%3A%2F%2Fwww.consejodetransparencia.es%2Fdam%2Fjcr%3A936f611d-e6f4-436f-bc3c-6e56a8e38779%2FC4_2015_firma_manuscrita.pdf

Diccionario de la lengua española (2022). Disociar. https://dle.rae.es/disociar

SAN de 26 de marzo 2019 (JUR\2019\201813; ECLI:ES:AN:2019:2386).

STC 292/2000, de 20 de noviembre. ECLI:ES:TC:2000:292.

STEDH de 26 de marzo de 1987, caso Leander contra Suecia (TEDH 1987\4).

STEDH de 7 de febrero de 2012. Caso Von Hannover v. Alemania (n.º2). https://hudoc.echr.coe.int/eng?i=001-139414

STEDH de 17 de febrero de 2015, caso Guseva contra Bulgaria (TEDH 2015\52590) y apartado 74 de la STEDH de 26 de marzo de 1987, caso Leander contra Suecia (TEDH 1987\4).

STEDH de 8 de noviembre de 2016, caso Magyar Helsinki Bizottság contra Hungría (JUR\2016\260055).

STJUE de 18 de julio de 2017 (JUR\2017\199987; ECLI:EU:C:2017:563).

STS de 30 de marzo de 1999 (RJ\1999\3246; ECLI:ES:TS: 1999:2206).

STS de 19 de mayo de 2003 (RJ 2003\3834; ECLI: ES:TS: 2003:3359).
We are social. (2023). *Digital 2023*. https://wearesocial.com/es/blog/2023/01/digital-2023/

_

DIANA PAOLA GONZÁLEZ MENDOZA. Institución: Universidad de Oviedo y Universidad de Cantabria. Contacto: gonzalezdiana@uniovi.es y dianapaola.gonzalez@unican.es