Departamento de Derecho Público y Filosofía Jurídica

Transparencia administrativa, acceso a la información y protección de datos personales:

Criterios para una conciliación de derechos desde la jurisprudencia del Tribunal de Justicia de la Unión Europea y la Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno

Tesis Doctoral

Doctorando: Daniel Federico Quesada Monge

Director: Antonio Rovira Viñas

Directora: Blanca Rodríguez-Chaves Mimbrero

Madrid, 2017

Transparencia administrativa, acceso a la información y protección de datos personales: criterios para una conciliación de derechos desde la jurisprudencia del Tribunal de Justicia de la Unión Europea y la Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno

Segunda parte

Transparencia, acceso a los documentos y protección de datos en el ámbito comunitario

Cuarta parte

El necesario equilibrio entre transparencia, acceso a la información y protección de datos y su regulación en la Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno

Abreviaturas

AEPD	Agencia Española de Protección de Datos
AN	Audiencia Nacional
BOE	Boletín Oficial del Estado
CADH	Convención Americana de Derechos Humanos
CE	Comisión Europea
CEADP	Convenio del Consejo de Europa sobre el Acceso a los Documentos Públicos.
CEDEFOP	European Centre for the Development of Vocational Training
CEDH	Convenio Europeo de Derechos Humanos
CNMV	Comisión Nacional del Mercado de Valores
Convenio 108	Convenio 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal
Corte IDH	Corte Interamericana de Derechos Humanos
CRTVE	Corporación de Radio y Televisión Española
CTBG	Consejo de Transparencia y Buen Gobierno
Directiva 95/46	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
DUDH	Declaración Universal de Derechos Humanos
EFSA	European Food Safety Authority / Agencia Europea de Seguridad Alimentaria
INECO	Ingeniería y Economía del Transporte
LOPD	Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal
LORTAD	Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal
LTAIBG	Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno
MAEC	Ministerio de Asuntos Exteriores y Cooperación
MECD	Ministerio de Educación, Cultura y Deporte
MINHAP	Ministerio de Hacienda y Administraciones Públicas
PDCP	Pacto de Derechos Civiles y Políticos
PE	Parlamento Europeo
POA	Planes Operativos Anuales
Reglamento 1049/2001	Reglamento (CE) 1049/2001 del Parlamento Europeo y del Consejo, de 30 de mayo de 2011, relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión.
Reglamento 45/2001	Reglamento (CE) 45/2001 del Parlamento Europeo y el 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
RGPD	Reglamento (UE) 2016/670 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)
RTP	Relación de puestos de trabajo

SAN	Sentencia Audiencia Nacional
SEC	Secretaría de Estado de Cultura
SENASA	Servicios y Estudios para la Navegación Aérea y la Seguridad Aeronáutica
SEPD o EDPS	Supervisor Europeo de Protección de Datos o European Data Protection Supervisor
STEDH	Sentencia Tribunal Europeo de Derechos Humanos
STGUE	Sentencia del Tribunal General de la Unión Europea
STJUE	Sentencia del Tribunal de Justicia de la Unión Europea
STPI	Sentencia del Tribunal de Primera Instancia
STS	Sentencia Tribunal Supremo
TC	Tribunal Constitucional
TEDH	Tribunal Europeo de Derechos Humanos
TFPUE	Tribunal de la Función Pública de la Unión Europea
TGUE	Tribunal General de la Unión Europea
TJCE	Tribunal de Justicia de la Comunidad Europea
TPI	Tribunal de Primera Instancia
TS	Tribunal Supremo
UE	Unión Europea
WP29 o Grupo 29	Working Party Article 29 (Grupo de Trabajo del Artículo 29)

Introducción

No existe prácticamente ningún ámbito de la vida moderna que escape al tratamiento de datos personales. Se trata de un tema de "gente real", como bien refería el Supervisor Europeo de Protección de Datos en su discurso "*The state of privacy 2017: mid-mandate report*" para resaltar esa dimensión social y humana de la protección de datos personales, más allá del típico encasillamiento como una cuestión técnica o legal.

En las relaciones entre los ciudadanos y la Administración Pública, el flujo cada vez más constante de datos es de dos vías. Por una parte, el tratamiento de los datos personales forma parte de las tareas habituales de las Administraciones Públicas, que han encontrado en las nuevas tecnologías una forma de modernizar la gestión pública y quienes para poder realizar un tratamiento leal y legal de los datos, han de tener en consideración la normativa relativa a la protección de datos de carácter personal. Muchos de estos tratamientos, acuñados hoy en día bajo el concepto de ciudades inteligentes, que pretenden la maximización de la eficiencia y calidad en la prestación de los servicios y la gestión pública, a través del análisis y tratamiento de datos, que en muchas ocasiones son facilitados por los mismos ciudadanos.

Por otra parte las personas exigen con más frecuencia, un mayor flujo de información desde la Administración hacia la sociedad civil, con el fin de poder analizar la gestión de los recursos públicos y exigir rendición de cuentas, aspecto que debe tener en consideración tanto la normativa de acceso a la información como la propia normativa propia de la protección de datos de carácter personal. La transparencia de la gestión pública permite que la ciudadanía esté más cercana a los procesos de toma de decisiones por parte de los agentes públicos y a su vez hace que la Administración tenga mayor legitimación. Cuenta de ello, por ejemplo, es la cantidad de reclamaciones y gestiones que ha resuelto el Consejo de Transparencia y Buen Gobierno (CTBG) en los escasos años de puesta en vigencia la Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno (LTAIBG).

La promoción y consecución del objetivo de la transparencia, en el tanto exige un intercambio constante de información, termina incidiendo de forma directa en la protección de los datos personales de los ciudadanos, ya sea porque forman parte de la Administración o porque han cedido sus datos para poder acceder a los servicios que se prestan. Hasta ahora las exigencias de la normativa en Protección de Datos cristalizaban

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 (Directiva 95/46), como las normas nacionales que la trasponen y en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), que venían siendo redefinidas por la jurisprudencia del Tribunal de Justicia de la Unión Europea (TJUE) que en reiteradas ocasiones se había pronunciado sobre este derecho, adaptándolo a los retos y amenazas que derivan de las nuevas tecnologías.

Por su parte, la transparencia resulta en uno de los componentes vitales y esenciales de la democracia, que permite, como ya se indicó, que los ciudadanos participen de manera más cercana en el proceso de toma decisiones y que cada vez se exija con mayor frecuencia e intensidad, que las personas que se encargan de la gestión pública rindan cuentas. Asimismo, como lo ha señalado la Comisión Europea (CE) en el *"Green Paper European Transparency Initiative"* de 2006, entre mayores sean los estándares de transparencia, mayor legitimación adquiere cualquier Administración Pública moderna. O como bien podría afirmarse en las ya famosas palabras del juez de la Suprema Corte de los Estados Unidos de Norteamérica, BRANDEIS en su obra "*Other people's money and how the bankers use it*", la luz solar es el mejor de los desinfectantes.

En una sociedad democrática, como lo define COLOMBO[1], debe necesariamente partirse de una base de igualdad y dignidad de la persona, que no tolera que exista opacidad por parte de la Administración, que está obligada a ser transparente y le resulta imposible vivir con información inexistente, facciosa o incompleta. Conforme se ha acrecentado y fortalecido el Estado democrático de Derecho, el sistema de secretismo y control de la información propio de gobiernos burocráticos[2], ha ido desapareciendo y a su vez se ha fortalecido el marco jurídico institucional que facilita a los ciudadanos el acceso a la información en aras de garantizar la transparencia en la gestión de las Administraciones Públicas. La transparencia, en tanto publicidad y apertura de los procesos en la toma de decisiones, actores y argumentos, resulta hoy día un barómetro de los Estados democráticos de Derecho, en contraposición a aquellos en los que existe una

[1] Colombo, G. (2008). Sulle regole. Milano: Feltrinelli. p. 41-55
[2] Sánchez Morón, M. (2011). Derecho administrativo: parte general. Madrid: Technos. p. 460.

resistencia al intercambio de información y facilitar el acceso a la misma por parte de los ciudadanos, que son concebidos como sistemas con problemas graves de legitimación.[3]

Bien describe SOMMERMANN que "la realización de la democracia, cuya idea principal es la autodeterminación del pueblo, presupone la transparencia de la organización y de la actuación estatal en su conjunto. La posibilidad de informarse directamente sobre las actuaciones y motivos del poder legislativo, así como de los poderes ejecutivo y judicial, constituye un elemento importante para la formación democrática de la opinión y de la voluntad. Sin el conocimiento de las responsabilidades de los actores y de sus criterios de actuación el control democrático queda incompleto o inoperable. La claridad de la atribución de responsabilidades tanto entre los poderes públicos como entre los órganos de cada uno de ellos, constituye, pues, una condición para hacer visible la responsabilidad política".[4]

No obstante las innegables ventajas y beneficios que se derivan de la transparencia administrativa para la vida en democracia, no resulta factible dentro de un Estado de Derecho que operen primacías automáticas a favor de la transparencia o su concreción a través del derecho de acceso a la información, pues existen límites que derivan de su interacción con otros derechos de igual o mayor rango, como sucede en cualquier plano jurídico. Esta situación de paridad con los demás derechos, hace que la transparencia y el acceso a la información estén en constante colisión y conflictos de derechos, especialmente, como ya lo hemos advertido, con el derecho a la protección de datos personales en tanto que una gran parte de la información pública, contiene datos de personas físicas identificadas e identificables –lo definición por excelencia del concepto de dato de carácter personal-.

El objetivo de este trabajo pretende analizar las posibles soluciones que se pueden dar a este conflicto de derechos desde la jurisprudencia del TJUE así como desde la solución que ha propuesto el legislador español en la LTAIBG.

En el Capítulo I, se abordará la importante labor que ha tenido el TJUE en dotar de contenido y vigencia el derecho a la protección de datos de carácter personal a lo largo

[3] Sommermann, K. (2010). La exigencia de una administración transparente en la perspectiva de los principios de democracia y del Estado de Derecho. En R. García Macho (Ed.), Derecho administrativo de la información y administración transparente. Madrid: Marcial Pons. pp. 11-26.
[4] *Ibíd. op. cit.* pp. 11-26.

de las casi dos décadas que ha tardado el legislador comunitario en actualizar el principal marco normativo de protección de datos.

La labor del TJUE a través de su jurisprudencia no sólo ha permitido que el derecho sea capaz de responder a los nuevos retos y amenazas derivados del avance de la tecnología y el Internet, sino que también ha servido como base para el nuevo marco regulatorio, que ha incorporado mucha de la doctrina del TJUE.

Para efectos de este análisis, se partirá de una referencia al marco normativo comunitario existente, que en cierta medida se basa en los antecedentes que existían a nivel del Consejo de Europa en materia de protección de Datos y la interpretación que había dado ya el Tribunal Europeo de Derechos Humanos (TEDH) a estos instrumentos jurídicos: el Convenio Europeo de Derechos Humanos (CEDH) y el Convenio 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio 108).

Posteriormente, se hará referencia al proceso de consolidación normativa del derecho a la protección de datos personales en la UE, que ha pasado por la aprobación de la Directiva 95/46, la emisión del Reglamento 45/2001, la aprobación de la Carta de Derechos Fundamentales de la Unión Europea (CDFUE) y más recientemente, la aprobación del 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 o RGPD).

Hecho este análisis, se expondrá la jurisprudencia del TJUE en materia de protección y como ha ido interpretando en una variedad de casos el contenido esencial del derecho a la protección de datos personales así como su adaptación a los más diversos escenarios en los que se ha visto inmiscuido este derecho desde la aprobación de la Directiva 95/46 en una época en la que resultaban imprevisibles los alcances que al día de hoy tienen el Internet y las nuevas tecnologías.

Seguidamente, el Capítulo II estará destinado a profundizar en los principales cambios que supone el Reglamento General de Protección de Datos, que recoge mucha de la doctrina del TJUE como ya se anunció pero que además supone un nuevo paradigma en la protección de datos personales en el ámbito comunitario, en el tanto su planteamiento general es pasar de un enfoque reactivo del derecho (Directiva 95/46), a

un enfoque proactivo de la normativa, que exige a los responsables y encargados del tratamiento de los datos personales, garantizar en todo momento, el cumplimiento de los derechos y principios contenidos en el RGPD.

El RGPD, diseñado para que los ciudadanos retomen el control de sus datos personales, alcanza a todos los responsables y encargados del tratamiento de los datos de carácter personal, siendo que las Administraciones Públicas no escapan a ello y han tenido que sumergirse, junto con los demás actores, en la labor de revisión y adaptación de los tratamientos de datos que llevan a cabo a las nuevas directrices en el plazo de dos años con el que se cuenta desde la aprobación del RGPD en 2016 hasta su entrada en aplicación a partir del 25 de mayo de 2018.

Pese a que en el momento de aprobación del RGPD ya el TJUE había resuelto en numerosas ocasiones el conflicto que suscita la relación entre transparencia, acceso a la información y documentos de carácter personal, el legislador comunitario únicamente incluyó una disposición de carácter general en este sentido, que no termina de dar las luces necesarias para una resolución del conflicto y que conduce necesariamente al análisis de este tema a través de la jurisprudencia del TJUE, que como hemos mencionado, sin lugar a dudas se verá afectada por el nuevo marco regulatorio.

En los Capítulos III y IV, la investigación se enfoca propiamente en la relación entre transparencia, acceso a la información y protección de datos, y especialmente, en la solución que ha entendido el TJUE es la más adecuada. Para esto, se hace necesario hacer un repaso del marco normativo vigente en la UE que regula la materia: por un lado el Reglamento 1049/200, sobre acceso a la información que está en poder de las instituciones comunitarias y el Reglamento 45/2001, relativo a la protección de datos por parte de las instituciones comunitarias.

Analizado el marco normativo, se profundizará en la evidente tensión que surge de dos normas que en principio parecen contrapuestas pero que el TJUE se ha encargado, a través de su jurisprudencia, de conciliar, de forma que no se produzcan sacrificios innecesarios de uno u otro derecho, así como de evitar que se tomen posturas maximalistas o radicalizadas a favor de uno u otro derecho. En ese sentido, se dará cuenta de la jurisprudencia específica del TJUE en esta materia, así como de las claves para la solución del conflicto de derechos que se desprende de la misma.

Finalizado estos dos Capítulos, se estudiará en contraposición la solución que ha preferido dar el legislador español a la solución de la controversia, que si bien no se aleja de la solución principal ofrece la jurisprudencia del TJUE, si ha incorporado una serie de elementos y criterios de conciliación que entiende pueden ayudar a una mejor solución de cualquier controversia que suscite el acceso a información pública que contenga datos de carácter personal.

Siguiendo un esquema similar a los dos anteriores, comenzaremos el análisis desde el marco normativo en el ordenamiento jurídico español que regula la materia. El capítulo V estudiará el tema de la protección de datos personales, desde la óptica de la LOPD, que se verá afectada con la entrada en vigencia del RGPD desde 2016 y su aplicación a partir de 2018, en los términos expuestos en los capítulos precedentes. Se centrará el análisis particularmente en la creación jurisprudencial de este derecho, por la paradoja que puede llegar a constituir frente al no reconocimiento jurisprudencial del carácter iusfundamental de otros derechos como el acceso a la información pública, así como el objeto que persigue la propia LOPD.

En el Capítulo VI, el trabajo se enfoca en el estudio del derecho de acceso a la información pública a través de su regulación más reciente en la LTAIBG que lo concibe como un derecho de configuración legal, sin ningún tipo de vinculación al derecho fundamental a la libertad de expresión y de recibir y difundir informaciones, en un sentido totalmente contrario al reconocimiento que al efecto han practicado no sólo las legislaciones de la mayoría de los países sino que también el TEDH y la Corte Interamericana de Derechos Humanos (Corte IDH).

Expuesta la jurisprudencia del TEDH y la Corte IDH y el carácter de configuración legal que le ha dado el ordenamiento jurídico español, se explicará una de las críticas más fuertes que ha recibido la LTAIBG y que en resumen consiste en la desventaja en que se coloca el derecho de acceso a la información pública como derecho ordinario, frente al derecho a la protección de datos personales que sí tiene reconocido ese carácter iusfundamental, problemática que ha quedado plasmada en los informes que rindieron la Agencia Española de Protección de Datos (AEPD) y el Consejo de Estado en la tramitación de la LTAIBG.

Habiendo explicado las bases jurídicas sobre las que se mueve la relación entre transparencia, acceso a la información y protección de datos en el ordenamiento español,

se entrará en el Capítulo VII a analizar la regulación que ha dado el legislador español a este conflicto en la LTAIBG: la creación de una excepción al acceso a la información en función de la protección de datos de carácter personal, que contempla los supuestos bajo los cuales no se puede tratar datos personales –datos especialmente protegidos, los escenarios en los que se puede aplicar una presunción a favor de la publicación de los mismos salvo demostración en contrario –datos meramente identificativos-, y los demás casos que estarán sujetos a una ponderación por parte del órgano que deba resolver la solicitud de acceso a la información pública que contenga los datos de carácter personal.

En conexión con lo anterior, el Capítulo VIII estará destinado a analizar la ponderación que sugiere la LTAIBG que se lleve a cabo en aquellos casos en que se determine que puede existir una afectación al derecho a la intimidad o la protección de datos de la persona cuyos datos constan en la información a la que se solicita el acceso. Asimismo, se analizarán los criterios de interpretación conjunta que al día de hoy han emitido tanto el CTBG y la AEPD en el uso de la facultad conjunta que les confirió la ley para dictar directrices que den seguridad jurídica en la aplicación de la excepción contenida en el artículo 15 de la LTAIBG.

Por último, se han destinado los dos capítulos finales de este trabajo al análisis de la aplicación práctica de la excepción contenida en el artículo 15 de la LTAIBG. Tanto el CTBG como la AEPD, dentro del ámbito de sus competencias, se encuentran interpretando la excepción del artículo 15 de la LTAIBG desde dos visiones muy distintas, que de momento, no llegan a ser contradictorias pero que si evidencian, en razón de las tareas encomendadas, posiciones más proclives al acceso a la información por parte del CTBG y posturas más garantistas del derecho a la protección de datos personales por parte de la AEPD, como es natural.

Cada capítulo consta de un apartado de cuestiones preliminares, en el que se da cuenta de forma general sobre el contenido del capítulo, seguido de un apartado introductorio y el desarrollo del tema, y, por último, un apartado final de recapitulación en el que se recogen las principales ideas de cada uno de ellos.

Primera Parte

Protección de datos en la Unión Europea: de la Directiva 95/46 al Reglamento General de Protección de Datos

Capítulo I. La contribución de la jurisprudencia del Tribunal de Justicia de la Unión Europea en la definición del derecho a la protección de datos personales a partir de la Directiva 95/46

SUMARIO: 1. Cuestiones preliminares. 2. La consolidación del marco normativo de la UE en materia de protección de datos personales. 3. La interpretación del derecho a la protección de datos personales por parte del TJUE. A. Concepto de dato de carácter personal. a) Nombres y apellidos de una persona en relación con otros datos. b) Término "vida privada" y datos laborales. c) Datos biométricos e imágenes. d) Direcciones IP. e) Datos en motores de búsqueda. f) Datos personales contenidos en documentos. B. Datos de personas jurídicas. C. Tratamiento de datos personales. a) Tratamiento de datos en sitios web y por motores de búsqueda. b) Tratamiento de datos con fines comerciales. c) Comunicación de datos a terceros. d) Toma de impresiones dactilares. e) Transmisión de datos entre autoridades. f) Transferencias internacionales de datos. g) Filtraciones de datos y comunicación posterior de los mismos. h) Tratamiento de datos para fines exclusivamente domésticos. i) Tratamiento de datos para fines periodísticos. D. Responsable del tratamiento de los datos. E. Consentimiento del interesado. F. Licitud del tratamiento: necesidad y proporcionalidad. G. Derechos de los interesados. a) Derecho de acceso y rectificación. b) derecho al olvido. H. Medidas de seguridad. I. Transferencias internacionales a países terceros. J. Garantía de total independencia de la autoridad de control. K. Balance frente a otros derechos e intereses tutelados por el ordenamiento comunitario. a) Derechos de autor y propiedad intelectual.

1. Cuestiones preliminares

En el presente Capítulo se abordará la especial trascendencia de la labor del TJUE en la interpretación y configuración del contenido esencial del derecho a la protección de datos de carácter personal contenido en la Directiva 95/46, posteriormente recogido en otras normas comunitarias como el Reglamento (CE) 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 (Reglamento 45/2001) y el artículo 8 de la CDFUE[5].

[5] Cabe advertir que pese a la configuración del derecho a la protección de datos de carácter personal como un derecho autónomo en el artículo 8 de la CDFUE, en los casos resueltos por el TJUE en los que se ha encargado de aplicar esta norma, lo ha hecho en relación con el artículo 7 del mismo texto normativo. Sobre

Para ello, se da inicio con una breve referencia de la consolidación del marco normativo de la Unión Europea (UE) en materia de protección de datos, teniendo en cuenta los antecedentes normativos existentes en el ámbito internacional en el momento de la aprobación del principal texto legal de la UE –la Directiva 95/46-, como por ejemplo, la Declaración Universal de Derechos Humanos (DUDH), el CEDH y el Convenio 108.

Posteriormente, se hará referencia a las cuatro etapas identificadas en la consolidación del marco regulatorio de la protección de datos personales en la UE, que comienza con la aprobación en 1995 de la Directiva 95/46 y que encuentra su etapa actual, casi 20 años después, con la aprobación del RGPD que será de aplicación a partir del 25 mayo de 2018.

Terminado ese repaso, se entrará de lleno a la jurisprudencia del TJUE en materia de protección de datos de carácter personal, en su mayoría a partir de la Directiva 95/46 y en un menor grado de las disposiciones contenidas en el Reglamento 45/2001 y la aplicación de los artículos 7 y 8 de la CDFUE. A modo general, como se verá, la labor ha sido de precisión del contenido del derecho, así como de actualización frente a los avances vertiginosos de las nuevas tecnologías que han supuesto retos y amenazas a este derecho, muchos de ellos imprevisibles en el momento de aprobación de la Directiva 95/46.

El análisis de la jurisprudencia se ha estructurado siguiendo el orden sistemático de los artículos de la Directiva 95/46, sin perjuicio de que por la evidente conexidad que tengan con alguna otra disposición de la propia Directiva 95/46 o de la normativa comunitaria, se haga referencia a otros artículos en el mismo epígrafe, y ha tenido como base las sentencias del TJUE publicadas en su sitio web al mes de abril de 2017[6].

2. La consolidación del marco normativo de la UE en materia de protección de datos personales

Desde sus inicios, el TJUE ha jugado un rol determinante en la definición y el continuo perfeccionamiento del derecho a la protección de datos de carácter personal. Han sido numerosas las oportunidades en las que el TJUE se ha pronunciado sobre el contenido de este derecho, cobrando así un papel determinante en la actualización del

este particular, puede verse una explicación detallada en: Lynskey, O. (2014). Deconstructing data protection: the 'added-value' or a right to data protection in the EU legal order. *The International and Comparative Law Quarterly*, 63(3). pp. 569-597.

[6] Disponible en: https://curia.europa.eu/jcms/

mismo frente al avance vertiginoso de las nuevas tecnologías y ante la demora en la reforma del marco normativo principal en materia de protección de datos en la UE, que ha tardado algo más de dos décadas en llegar.

Antes de estudiar la consolidación normativa del derecho a la protección de datos de carácter personal en la UE, y que el TJUE se ha encargado de perfilar, resulta necesario recurrir a los dos antecedentes normativos más relevantes que existen en el ámbito europeo.

En 1948, la DUDH plasmó en su artículo 12 el derecho de toda persona a no ser objeto de injerencias arbitrarias en su vida privada, familia, domicilio o correspondencia. Este derecho fue luego recogido en el CEDH, que en 1950 por primera vez proclamó, en un texto internacional jurídicamente vinculante, el derecho a la privacidad (artículo 8 del CEDH). Años después, el 28 de enero de 1981, conscientes de la necesidad de garantizar la tutela del derecho a la vida privada frente al auge de la circulación de los datos de carácter personal entre los diferentes Estados y su tratamiento automatizado, el Consejo de Europa aprobó el Convenio108. Desde la promulgación de estos textos, hasta el día de hoy, la protección de los datos de carácter personal se "ha convertido, sin duda alguna, en un objeto político y jurídico de la Organización europea como una manifestación más del respeto a los derechos humanos".[7]

El TEDH, al igual que el TJUE, ha cumplido un rol fundamental en la interpretación del artículo 8 del CEDH y el reconocimiento del derecho a la protección de datos de carácter personal como parte del derecho a la privacidad. En la Sentencia del TEDH (STEDH), de 26 de marzo de 1987, en el caso Leander contra Suecia, tuvo la primera oportunidad de referirse al derecho a la protección de datos de carácter personal, al indicar que la información mantenida en el registro secreto de la policía se refería a la vida privada del peticionario y, por tanto, el almacenamiento como la comunicación de los datos, aunado a la negativa de que el señor Leander los refutara, constituía una violación al artículo 8.1 del CEDH[8], pese a desestimar posteriormente el caso por ser una injerencia justificada y necesaria en una sociedad democrática.

[7] Pavón Pérez, J.A. (2002). La protección de datos personales en el Consejo de Europa: el Protocolo Adicional al Convenio 108 relativo a las autoridades de control y a los flujos transfronterizos de datos personales. *Anuario de la Facultad de Derecho*, núm. 19-20, 2001-2002. pp. 235-252.
[8] STEDH de 26 de marzo de 1987, caso Leander c. Suecia (rec. núm. 9248/81), apartado 48.

Otra sentencia especialmente notable dictada por el TEDH en sus inicios, fue la del caso Z v. Finlandia, en donde se pronunció sobre la revelación de datos de salud –condición de seropositiva de la peticionaria– en un proceso penal que se seguía en contra de su esposo. El TEDH mencionó en forma expresa al artículo 8 del CEDH y también se refirió por primera vez a la aplicación del Convenio 108. El TEDH reconoció la trascendencia de la protección de datos de carácter personal para el ejercicio del derecho a la privacidad contenido en el artículo 8 del CEDH, en especial cuando a datos de salud se refiere y señala que la legislación interna debe adoptar las garantías necesarias para impedir la divulgación de datos personales relativos a la salud[9].

En la medida en la que las nuevas tecnologías fueron avanzando, el TEDH tuvo que pronunciarse sobre la aplicación del artículo 8 del CEDH frente al uso de estas y sus incidencias en la privacidad de la persona y los datos personales, como por ejemplo: la utilización de sistemas GPS para vigilancia y el uso posterior de los datos en procesos penales[10]; el almacenamiento indefinido de huellas digitales, muestras celulares y perfiles de ADN después de finalizado el proceso penal para el cual fueron recabados[11], la intercepción masiva de datos para efectos de prevención y lucha contra el terrorismo[12], entre otros.

Ahora bien, en lo que se refiere a la consolidación normativa del derecho a la protección de datos de carácter personal, esta se originó en la UE con la Directiva 95/46[13]. Para ese entonces, algunos de los Estados miembros de la UE contaban ya con normativa de protección de datos; no obstante, los diferentes niveles de protección que se

[9] STEDH de 25 de febrero de 1997, caso Z. c. Finlandia (rec. núm. 9/1996), apartado 95.
[10] STEDH de 2 de septiembre de 2010, caso Uzun c. Alemania (rec. núm. 35623/05).
[11] STEDH de 4 de diciembre de 2008, caso S. y Marper c. Reino Unido (rec. núm. 30562/04 y 30566/04). Esta sentencia, como menciona Gonzáles Fuster, constituye un hito importante en la delimitación y aplicabilidad del artículo 8 de la CEDH al cada vez más frecuente tratamiento de datos biométricos, muestras celulares y perfiles de ADN en bases de datos. Ver: Gonzáles Fuster, G. (2009). TEDH – Sentencia de 04.12.2008, S. y Marper c. Reino Unido, 30562/04 y 30566/04 – Artículo 8 CEDH – Vida privada – Injerencia en una sociedad democrática – Los límites del tratamiento de datos biométricos de personas no condenadas. *Revista de Derecho Comunitario Europeo*, núm. 33, Madrid, mayo/agosto (2009). pp. 619-633.
[12] STEDH de 12 de enero de 2016, caso Szabó y Vissy c. Hungría (rec. núm. 37138/14).
[13] Sobre los antecedentes de la Directiva 95/46, además de los ya mencionados, como por ejemplo, el Convenio 108, Guerrero Picó menciona los importantes esfuerzos previos a la aprobación de la Directiva, entre ellos, la propuesta de directiva, COM (90) 314-SYN 287 y 288 de 24 de septiembre de 1990 y la propuesta COM (92) 422 final (DO núm. C. 311, de 27 de noviembre de 1992. Ver en: Guerrero Picó, M.C. (2005). El derecho fundamental a la protección de datos de carácter personal en la Constitución Europea. *ReDCE*, núm. 4, julio-diciembre de 2005. pp. 293-332

garantizaban en los distintos Estados podían suponer un obstáculo para la libre circulación de datos y el ejercicio de las actividades económicas en la Comunidad.[14]

Por este motivo, se adoptó una Directiva que contiene un nivel de detalle equiparable al de las legislaciones internas, en el tanto su cometido principal era, entre otros, armonizar las legislaciones nacionales existentes. Así lo ha reafirmado el TJUE, en su jurisprudencia, al reconocer que la Directiva 95/46 busca equiparar el nivel de protección de los datos de carácter personal en todos los Estados miembros. También ha reafirmado que dicha armonización no es de mínimos, sino que se trata en principio de una armonización completa, que permite garantizar de forma equitativa la libre circulación de datos personales y la protección de los derechos e intereses de las personas a que se refieren esos datos.[15]

Una segunda fase de consolidación de este derecho ocurrió en el 2001, con la adopción del Reglamento 45/2001, cuyo objeto es establecer las disposiciones vinculantes necesarias para garantizar el derecho a la protección de datos de carácter personal por parte de las instituciones y organismos de la UE. Sobre este Reglamento se ahondará más en el Capítulo III de este trabajo.

Un tercer momento que marcó la definición del derecho a la protección de datos de carácter personal en la UE ocurrió en el 2009, con la entrada en vigor del Tratado de Lisboa en diciembre de ese año, el cual otorgó a la CDFUE un carácter jurídico vinculante, lo que ha hecho al TJUE más proclive a la aplicación de los derechos fundamentales allí en consignados, incluyendo el derecho a la protección de datos personales[16]. La CDFUE adoptada en el 2000, había reconocido en su artículo 8 el derecho a la protección de datos de carácter personal como un derecho autónomo e independiente del derecho a la intimidad, reconocido en ese mismo texto en el artículo 7 bajo el título del derecho al respeto de la vida privada y familiar.

---

[14] Directiva 95/46/, considerando 7.

[15] STJUE (Sala Tercera) de 24 de noviembre de 2011, C-468/10 y C-469/10 (caso ASNEF), apartados 27-30.

[16] González Pascual, M. (2014). El TJUE como garante de los derechos en la UE a la luz de la sentencia Digital Rights Ireland. *Revista de Derecho Comunitario Europeo*, núm. 49. Madrid, septiembre/diciembre (2014). pp. 943-971. También, puede verse una apreciación similar en: Blanke-H. (2012). The protection of fundamental rights in Europe. En H. Blanke; S. Magiameli (Eds.), The European Union after Lisbon: constitutional basis, economic order and external action. Bruselas: Springer. pp. 159-232 y Gianfrancesco, E. (2012). The Charter of Fundamental Rights of the Union as a source of law. En: H. Blanke; S. Magiameli (Eds.), The European Union after Lisbon: constitutional basis, economic order and external action. Bruselas: Springer. pp. 295-310.

El artículo 8 de la CDFUE, además de sentar las bases jurídicas del derecho a la protección de datos personales, contempla el derecho que tiene toda persona a la protección de datos de carácter personal que le conciernen, y, asimismo, dispone que los datos deberán tratarse de modo leal, para fines concretos y sobre la base del consentimiento de la persona titular de los mismos, o de cualquier otro fundamento legítimo que se prevean en la ley.[17] Además, establece el derecho que tiene toda persona de acceder a los datos recogidos que le conciernan y la rectificación de estos. Por último, pero no menos importante, el artículo recoge la independencia de las autoridades de protección de datos, al señalar que el respeto de las normas en materia de protección de datos quedará sujeto al control de una autoridad independiente.

El cuarto y actual momento en la definición normativa del derecho a la protección de datos de carácter personal en el ámbito comunitario llegó al aprobarse el nuevo RGPD. Aproximadamente, transcurrieron 21 años para actualizar el marco normativo creado por la Directiva 95/46, que si bien ha sido una pieza esencial en la protección de los datos de carácter personal, fue aprobada en una época donde no se vislumbraban aún las dimensiones que el Internet y el uso de las nuevas tecnologías ha llegado a alcanzar en la actualidad.[18]

---

[17] En palabras de GUERRERO PICÓ, el artículo 8 de la CDFUE fija lo que podría definirse como el contenido básico o esencial del derecho a la protección de datos personales: el principio de finalidad, el consentimiento informado y la licitud en el tratamiento de los mismos, aunque quedan por fuera algunos elementos clave como el principio de calidad o las categorías de datos, que no obstante, pueden terminar de ser integrados aplicando el artículo 53 de la CDFUE que dispone que la Carta debe ser interpretada con atención a otras fuentes del derecho internacional y comunitario, lo que supondría la observancia del Convenio 108 y la Directiva 95/45. Ver en: Guerrero Picó, M.C. (2005). El derecho fundamental a la protección de datos… *op. cit*. pp. 293-332.

[18] Sobre este particular, KISS Y SZOKE explican de forma concisa el impacto de las nuevas tecnologías, en especial la incidencia de la Web 2.0 en la protección de datos personales y la necesaria adecuación del marco normativo para que fuese capaz de responder a estas nuevos retos de la privacidad y la protección de datos personales: "during the last 10-15 years, there have been further significant social, economic and cultural changes which EU legislation has had to face and respond to, and the Proposal for a Regulation can be seen as a milestone in the process. Its new trends have been summarized by many authors, some of whom highlight the role of Web 2.0 technologies, which clearly has had a great effect on privacy. On the one hand, it seems, that people like to "post and sear for personal, often intimate information online" about themselves, and so legislation has to focus on a "new generation of users", whose attitude to privacy may be different from that of earlier generations. On the other hand, user generated content my result in millions of users being regarded as data controllers, and so they are subjects of data protection legislation – but with some of the responsibilities imposed on data controllers. Some other trends should also be highlighted, such as ubiquitous computing, and the "internet of things", the growing importance of cloud computing, mobile data processing (including location tracking and third party applications) smart grid, robotics personalized medicine and biometrics. The spread of sophisticated methods of profiling, and then new technologies of marketing mostly behavioral advertising) should also be mentioned. It seems that current legislation cannot respond to these challenges. Many critical opinions have been published in the past few years – and voices heard urging significant changes or a new generation of regulation to appear. Both technology and users have changed much, and so these trends clearly call for a new data protection regime, new laws with new

Bajo el entendido de la necesidad de afrontar los retos que suponen los avances tecnológicos en materia de protección de datos y libre circulación de los mismos entre los Estados miembros, en el 2012 la Comisión Europea (CE) propuso una reforma extensiva y comprensiva al marco normativo comunitario, la cual se componía de una propuesta de RGPD para sustituir la Directiva 95/46 y una propuesta de Directiva relativa a la protección de datos de carácter personal en materia de cooperación policial y judicial en el ámbito penal.

Con estas propuestas, se pretendía "abordar nuevas problemáticas hasta la fecha no satisfactoriamente resueltas por la normativa vigente, especialmente, en cuanto al impacto de las nuevas tecnologías y de Internet en el tratamiento de los datos personales y en su incidencia en la privacidad de los ciudadanos"[19], quienes actualmente tienen una relación con las nuevas tecnologías muy diferente a la que se tenía cuando se aprobó la Directiva 95/46[20].

En 2016, cuando se aprobó del RGPD, se logró la culminación del proceso de actualización de la normativa, la cual ya ha entrado en vigencia pero será aplicable a partir del 25 de mayo 2018, teniendo los Estados miembros y responsables o encargados del tratamiento de datos personales, un plazo de dos años (contado desde su aprobación) para adaptarse a las nuevas regulaciones incluidas[21].

---

concepts, precisely as in the 70s and, later in the 90s". En: Kiss, A.; Szoke, G.L. (2015). Evolution or Revolution? Steps Forward to a new Generation of Data Protecion. En S. Gutwirth, R. Leenes y P. de Hert (Eds.), *Reforming European Data Protection Law. Law, Governance and Technology Series (20)*. Bruselas: Springer. pp. 311-332. Sobre estos y otros factores que incidieron en la necesidad de contar con un nuevo marco regulatorio, también puede verse: Robinson, N. et al (2009). Review of the European Data Protection Directive. Recuperado de: http://www.rand.org/content/dam/rand/pubs/technical_reports/2009/RAND_TR710.pdf

[19] Rallo Lombarte, A. (2012). Hacia un nuevo sistema europeo de protección de datos: las claves de la reforma. *UNED. Revista de Derecho Político,* núm. 85, septiembre-diciembre 2012, pp. 13-56.

[20] Inclusive hay quienes apuntan una interacción paradójica entre los ciudadanos, sus convicciones y el uso de las redes sociales, pues hay inconsistencia entre las actitudes frente a la privacidad en línea y las actitudes que finalmente se adoptan. En ese sentido, se puede ver: Trepte et al. (2015). Do people know about privacy and data protection strategies? Towards the "online privacy literacy scale" (OPLIS). En S. Gutwirth, R. Leenes y P. de Hert (Eds.), *Reforming European Data Protection Law. Law, Governance and Technology Series (20)*. Bruselas: Springer. pp. 333-365.

[21] Sobre este particular, la AEPD explica que el periodo de dos años hasta la aplicación del Reglamento tiene como objetivo permitir que los Estados de la Unión Europea, las Instituciones Europeas y también las organizaciones que tratan datos vayan preparándose para el momento en que el Reglamento sea aplicable. En esos dos años, por ejemplo, los Estados miembros pueden adoptar o iniciar la elaboración de determinadas normas que sean necesarias para permitir o facilitar la aplicación del Reglamento. Esas normas no pueden ser contrarias a las disposiciones de la vigente Directiva ni tampoco ir más allá de los poderes de actuación normativa que el propio Reglamento prevé de forma explícita o implícita. Información disponible en: https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2016/notas_prensa/news/2016_05_26-ides-idphp.php

Durante este tiempo de consolidación jurídica y hasta hoy, el TJUE ha tenido encomendada la tarea de mantener actualizado este derecho a través de la resolución de casos, los cuales van desde la definición del concepto de dato personal hasta la nulidad de acuerdos de transmisión de datos o el reconocimiento del llamado derecho al olvido y en ese sentido, los avances jurisprudenciales del TJUE más significativos han terminado por quedar plasmados en el RGPD.

Asimismo, el rol del TJUE ha servido para dar a la protección de datos su carácter de derecho y libertad fundamental frente a su concepción inicial, que partía primordialmente desde un punto de vista de libertad de mercado y circulación de datos[22]. Como bien lo menciona RODRÍGUEZ-IZQUIERDO SERRANO, "durante este recorrido de décadas, el Tribunal de Luxemburgo ha hecho jurisprudencia sobre derechos fundamentales, con un ojo mirando a Estrasburgo, y a la vez considerando los contenidos básicos de los derechos en las Constituciones nacionales y siempre afirmado su autonomía en el complejo normativo de la Unión".[23]

3. La interpretación del derecho a la protección de datos personales por parte del TJUE

A. Concepto de dato de carácter personal

(Artículo 2.a) de la Directiva 95/46)

El artículo 2.a) de la Directiva 95/46, considera que dato personal es toda aquella información referida a una persona física identificada o identificable, siendo que su identidad puede determinarse de forma directa o indirecta, ya sea mediante un número de identificación o varios elementos de su identidad física, fisiológica, psíquica, económica o cultural.

a) Nombres y apellidos de una persona en relación con otros datos

[22] Para autores como BAZZOCCHI, este tema vino a solventarse con el artículo 8 de la CDFUE que le concede al derecho a la protección de datos un ámbito de aplicación más amplio que el de la Directiva 95/46 que estaba dirigido y limitado esencialmente a cuestiones de mercado y libre circulación de los datos. En: Bazzocchi, V. (2011). The European Charter of Fundamental Rights and the Area of Freedom, Security and Justice. En G. Di Federico (Ed.), The EU Charter of Fundamental Rights: from declaration to binding instrument. Bruselas: Springer. pp. 177-197.

[23] Rodríguez-Izquierdo Serrano, M. (2015). El Tribunal de Justicia y los derechos en la sociedad de la información: privacidad y protección de datos frente a las libertades informativas. *ReDCE,* núm. 24, Julio-Diciembre de 2015. Recuperado de: http://www.ugr.es/~redce/REDCE24/articulos/10_RODRIGUEZ_IZQUIERDO.htm#uno

Desde sus primeras sentencias en materia de protección de datos, el TJUE se ha encargado de dar contenido y vigencia al concepto de dato de carácter personal que establece la Directiva 95/46. Así por ejemplo, ha entendido que la información relativa al nombre completo de una persona, sus funciones en una determinada organización, aficiones, situación familiar, número de teléfono e información, constituyen un dato de carácter personal según lo dispuesto en el artículo 2.a) de la Directiva 95/46[24].

Asimismo, ha indicado que los datos referentes al apellido y nombre de una persona física, cuyos ingresos sean superiores a un umbral determinado, así como los datos sobre rendimientos del trabajo y capital, son datos de carácter personal cubiertos por la Directiva 95/46[25]. En similar sentido, el TJUE ha considerado que los datos fiscales, en el tanto se refieren a información sobre una persona física identificada o identificable, constituyen un dato de carácter personal[26]. Incluso, ha llegado a reconocer que el nombre y los apellidos de una persona, por sí solos, están cubiertos por esta definición[27].

b) Término "vida privada" y datos laborales

En esa misma línea, es doctrina del TJUE que el término "vida privada" no es sujeto de una interpretación restrictiva, de forma que las actividades profesionales no quedan excluidas de dicho concepto[28]. En ese sentido, ha reafirmado en la sentencia del TJUE (STJUE) del caso Volker und Markus Schecke y Eifert que el hecho de que los datos publicados sobre una persona se refieran a sus actividades profesionales es irrelevante y no afecta el carácter de dato personal de los mismos[29]. Con base en lo anterior, no es de extrañar que el TJUE haya estimado que los datos contenidos en un registro de carácter laboral que se refieran a la jornada de trabajo diario y los periodos de descanso de cada trabajador, constituyen datos personales, en el tanto tratan de información sobre una persona física identificable o identificada[30].

[24] STJCE de 6 de noviembre de 2003, asunto C-101/01 (caso Lindqvist), apartado 34.
[25] STJCE (Gran Sala) de 16 de diciembre de 2008, asunto C-73/07 (caso Satakunnan Markkinapörssi y Satamedia), apartado 35.
[26] STJUE (Sala Tercera) de 1 de octubre de 2015, asunto C-201/14, (caso Bara), apartado 29.
[27] STJUE (Gran Sala) de 29 de junio de 2010, asunto C-28/08 P (caso Comisión/Bavarian Lager), apartado 68.
[28] STJCE de 20 de mayo de 2003, asuntos C-465/00, C-128/01 y C-139/01 (caso Österreichischer Rundfunk y otros), apartado 73-74.
[29] STJUE (Gran Sala) de 9 de noviembre de 2010, asuntos C-92/09 y C-93/09 (caso Volker und Markus Schecke y Eifert), apartado 59.
[30] STJUE (Sala Tercera) de 30 de mayo de 2013, asunto C-342/12, (caso Worten), apartado 19.

c) Datos biométricos e imágenes

El TJUE ha partido también de la premisa de que información única de una persona que permita su identificación precisa, constituye un dato de carácter personal. En ese sentido, ha estimado que datos biométricos[31], como por ejemplo las impresiones dactilares, están comprendidas dentro de la definición de dato de carácter personal, en el tanto contienen información única que permite la identificación precisa de una persona[32]. Asimismo, ha entendido que la imagen de una persona grabada por un sistema de video vigilancia, constituye un dato personal, en el tanto permite la identificación de quien ha sido grabado[33].

d) Direcciones IP

En relación con el uso de las tecnologías, el TJUE ha considerado que es un dato de carácter personal según el sentido de la Directiva 95/46, la dirección IP[34] de los usuarios de un servicio de acceso a Internet, en el tanto permite identificar a un usuario determinado[35]. De igual forma, en la STJUE del caso Breyer, 19 de octubre de 2016, determinó que una dirección IP dinámica que es registrada por un proveedor de servicios de medios en línea –en ese caso el gobierno de la República Federal alemana-, es un dato de carácter personal en el tanto la información adicional que solicita a la persona interesada, le permita por medios legales identificar a la persona física, en el sentido de lo dispuesto en el artículo 2.a) de la Directiva[36].

---

[31] Definidos estos por la AEPD en el Informe jurídico 0342/2009 como "aquellos aspectos físicos que, mediante un análisis técnico, permiten distinguir las singularidades que concurren respecto e dichos aspectos y que, resultando que es imposible la coincidencia de tales aspectos en dos individuos, una vez procesados, permiten servir para identificar al individuo en cuestión (tales como huellas digitales, el iris del ojo, la voz, etc.)". También es importante retomar que los datos biométricos han sido incorporados de forma expresa dentro del contenido del concepto de dato de carácter personal en el RGPD.

[32] STJUE (Sala Cuarta) de 17 de octubre de 2013, asunto C-291/12 (caso Schwartz), apartado 27.

[33] STJUE (Sala Cuarta) de 11 de diciembre de 2014, asunto C-212/13 (caso Rynes), apartado 22.

[34] Una dirección IP (*Internet Protocol)* ha sido conceptualizada por la AEPD como "un conjunto de números que identifica un ordenador cuando se conecta a la red. La dirección IP puede utilizarse para localizar geográficamente al usuario y, dado que se asigna unívocamente la línea de conexión por la compañía que nos presta el servicio de acceso, puede permitir en muchos casos la identificación del titular, y en consecuencia, del probable usuario. Muchos servicios de internet, como las redes sociales o los buscadores, conservan las direcciones IP de los usuarios que acceden a sus servicios". Recuperado de: http://www.agpd.es/portalwebAGPD/jornadas/dia_internet_2016/tus_datos_personales_en_internet-ides-idphp.php#seccion3

[35] STJUE (Sala Tercera) de 24 de noviembre de 2011, asunto C-70/10 (caso Scarlet), apartado 51.

[36] STJUE (Sala Segunda) de 19 de octubre de 2016, asunto C-582/14 (caso Breyer), apartado 49.

En sentido similar, en la sentencia del Tribunal de Justicia de la Comunidad Europea (STJCE), de 29 de enero de 2008, en el caso Promusicae, el TJCE señaló con claridad que la comunicación de los nombres y las direcciones de determinados usuarios de un programa de *file sharing*, constituye una comunicación de datos de carácter personal conforme a la definición que figura en la Directiva 95/46[37].

e) Datos en motores de búsqueda

Por su parte, en el caso Google consideró que los datos hallados, indexados, almacenados por motores de búsqueda de Internet y puestos a disposición de los usuarios de dicho motor, constituyen información relativa a personas físicas identificadas e identificables, y por consiguiente, se encuentran dentro de la noción de dato de carácter personal de la Directiva[38].

f) Datos personales contenidos en documentos

Es doctrina del TJUE también que los datos referentes a una persona, que figuran en una minuta redactada con carácter previo a la resolución de permiso de residencia temporal de nacionales de un tercer país como por ejemplo: nombre, fecha de nacimiento, sexo, etnia, religión e idioma son datos de carácter personal, en tanto permiten la identificación de quien solicita la residencia. No obstante, el TJUE precisa que no constituyen datos de carácter personal las consideraciones y el análisis jurídico contenido en la minuta, en el tanto no permiten la verificación de la exactitud de los datos ni pueden ser objeto de rectificación. En ese sentido, el TJUE estima que la Directiva 95/46 no contempla un derecho de acceso a los documentos administrativos, sino que garantiza el derecho a la intimidad del solicitante en cuanto al tratamiento de sus datos, así como que estos sean exactos, tratados de forma lícita, entre otros[39].

Por su parte, en el caso ClientEarth y PAN Europe/EFSA, STJUE de 16 de julio de 2015, el TJUE interpretó que de conformidad con lo dispuesto en el artículo 2.a), del Reglamento 45/2001, constituye un dato de carácter personal la información sobre cuál experto emitió determinada observación específica en un documento de trabajo de la Agencia Europea de Seguridad Alimentaria (EFSA). A criterio del Tribunal, el hecho de

[37] STJCE (Gran Sala) de 29 de enero de 2008, asunto C-275/06, (caso Promusicae), apartado 45.
[38] STJUE (Gran Sala) de 13 de mayo de 2014, asunto C-131/12 (caso Google), apartado 27.
[39] STJUE (Sala Tercera) de 17 de julio de 2014, asunto C-141/12 (caso YS y otros), apartado 38-39, 44-46.

que la información mencionada esté circunscrita en el contexto de una actividad profesional, o bien, que las observaciones y los nombres de los expertos hubieran sido publicados con anterioridad en el sitio web de la agencia, no priva a la información solicitada de su carácter de dato personal. Tampoco incide en su condición de dato personal que los expertos no se hayan opuesto a la publicación de sus datos, pues la noción de dato personal no depende de dicha oposición[40].

Un dato de carácter personal también lo constituyen aquellos datos personales relativos a extranjeros, que son almacenados en un registro central de extranjeros, como por ejemplo los datos relativos al nombre y apellidos de la persona, estado civil, documento de identidad, último lugar de residencia en el Estado de origen, información sobre religión y nacionalidad del cónyuge o pareja, información sobre entradas y salidas del país, resoluciones sobre autorización de trabajo, reconocimiento de la condición legal de refugiado por otro Estado, entre otros[41]. Igualmente, la información sobre el nombre y domicilio que obra en poder de un municipio, ha sido considerada por el TJUE como información de carácter personal[42].

Similar doctrina ha sentado el Tribunal General de la Unión Europea (TGUE) cuando ha señalado que los nombres y los apellidos de las personas que figuran en una lista de reserva de un concurso general para optar por un puesto en la UE, constituyen un dato de carácter personal[43]. Asimismo, ha considerado, y es doctrina, que los nombres y los apellidos de las personas integrantes de los órganos directivos del *European Centre for the Development of Vocational Training* (CEDEFOP), por ejemplo, no pierden su calidad de dato de carácter personal por haber participado la persona en los órganos de toma de decisión del CEDEFOP o sus actividades hayan sido resultado de una actividad pública y no desarrolladas en la esfera privada[44].

[40] STJUE (Sala Segunda) de 16 de julio de 2015, asunto C-615/14 P (caso ClientEarth y PAN Europe/EFSA), apartado 29-33.
[41] STJCE (Gran Sala) de 16 de diciembre de 2008, asunto C-524/06 (caso Huber), apartado 43.
[42] STJUE (Sala Tercera) de 7 de mayo de 2009, asunto C-553/07 (caso Rijkeboer), apartado 42.
[43] STGUE (Sala Octava) de 07 de julio de 2011, asunto T-161/04 (caso Valero Jordana/Comisión), apartado 91.
[44] STGUE (Sala Quinta) de 11 de junio de 2015, asunto T-496/13 (caso McCullough/CEDEFOP), apartado 66.

B. Datos de personas jurídicas

(Artículo 2.a) de la Directiva 95/46, artículo 2.a) del Reglamento 45/2001 y artículos 7 y 8 del CDFUE)

En relación con el derecho a la intimidad y la protección de datos de carácter personal que pueda llegar a cubrir a una persona legal o jurídica, el TJUE ha considerado que la protección que otorgan los artículos 7 y 8 de la CDFUE, únicamente aplica a personas físicas. Las personas jurídicas solo pueden entenderse cubiertas con la protección que brindan dichos artículos cuando a partir de la razón social de la persona jurídica se identifique a una persona física[45]. Igual consideración ha tenido a la hora de aplicar el Reglamento 45/2001, pues el TGUE ha considerado que una persona legal o jurídica no está cubierta dentro del ámbito de protección de dicho Reglamento, motivo por el cual se encuentra imposibilitada para reclamar un quebranto a la normativa[46].

C. Tratamiento de datos personales

(Artículo 2.b) de la Directiva 95/46, artículo 2.b) del Reglamento 45/2001)

Ha sido reiterada y constante la jurisprudencia del TJUE que define el concepto de tratamiento de datos de carácter personal contenido en el artículo 2.b) de la Directiva 95/46. En lo particular, al tenor de la disposición citada de la Directiva, constituye un tratamiento de datos la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por trasmisión, difusión, acceso, cotejo, interconexión, bloqueo, supresión o destrucción de datos, por medio de una operación o conjunto de operaciones automatizadas o manuales.

a) Tratamiento de datos en sitios web y por motores de búsqueda

En este sentido, en el caso Lindqvist señaló que la publicación de una serie de datos de carácter personal en una página web, constituye un tratamiento de datos a la luz de lo dispuesto en la Directiva 95/46[47]. En idénticos términos se pronunció en la STJUE de 1 de octubre de 2015, caso Weltimmo, en donde se consideró que hacer referencia a

[45] STJUE de 9 de noviembre de 2010, asuntos C-92/09 y C-93/09, apartado 53.
[46] STGUE (Sala Segunda), de 30 de mayo de 2006, asunto T-198/03, (caso Bank Austria Creditanstalt/Comisión), apartado 95.
[47] STJCE de 6 de noviembre de 203, asunto C-101/01, apartado 25.

datos personales en un sitio web de anuncios inmuebles, constituye un tratamiento de datos[48].

En el caso Google, el TJUE desarrolló a mayor profundidad el tratamiento de datos personales y su relación con los motores de búsqueda de Internet. En primer lugar, recordó la jurisprudencia del caso Lindqvist, por medio de la cual habían considerado que hacer referencia a datos de una persona en una página en Internet, constituye un tratamiento de datos. Seguidamente, indica que "al explorar Internet de manera automatizada, constante y sistemática en busca de la información que allí se publica, el gestor de un motor de búsqueda «recoge» tales datos que «extrae», «registra» y «organiza» posteriormente en el marco de sus programas de indexación, «conserva» en sus servidores y, en su caso, «comunica» y «facilita el acceso» a sus usuarios en forma de listas de resultados de sus búsquedas. Ya que estas operaciones están recogidas de forma explícita e incondicional en el artículo 2 de la Directiva 95/46, deben calificarse de «tratamiento» en el sentido de dicha disposición, sin que sea relevante que el gestor del motor de búsqueda también realice las mismas operaciones con otros tipos de información y no distinga entre éstos y los datos personales".[49]

b) Tratamiento de datos con fines comerciales

Asimismo, en la sentencia del Tribunal de Justicia de la Comunidad Europea (STJCE) del caso Satakunnan Markkinapörssi y Satamedia, indicó que recoger documentos púbicos de la administración fiscal relativos al rendimiento del trabajo y del capital y al patrimonio de las personas físicas y tratarlos para su publicación, publicarlos posteriormente por orden alfabético, tipos de renta y municipio, cederlos en un soporte digital para que sean tratados con fines comerciales y tratarlos en un servicio de mensajería que permita a los usuarios de telefonía móvil acceder a dicha información, constituyen actividades que encuadran en el concepto de tratamiento de datos de carácter personal, según el artículo 2.b) de la Directiva 95/46[50].

[48] STJUE (Sala Tercera) de 1 de octubre de 2015, C-230/14 (caso Weltimmo), apartado 37.
[49] STJUE de 13 de mayo de 2014, asunto C-131/12, apartado 31.
[50] STJCE de 16 de diciembre de 2008, asunto C-73/07, apartado 37.

c) Comunicación de datos a terceros

También ha considerado que la comunicación de datos personales como el nombre y la dirección de una persona, constituyen un tratamiento de datos de carácter personal. En la STJUE del caso Bavarian Lager/Comisión indicó que la comunicación de los nombres de las personas participantes en una reunión celebrada en un procedimiento de incumplimiento, constituye un tratamiento de datos de carácter personal[51]. Igualmente, el Tribunal ha estimado que la comunicación del nombre y la dirección de un abonado o usuario de Internet, quien usa una dirección IP de la cual en apariencia se intercambiaron de forma ilícita archivos que contenían obras protegidas, es un tratamiento de datos de carácter personal según la Directiva[52].

d) Toma de impresiones dactilares

Del mismo modo, resulta relevante mencionar el caso Schwartz, en el cual el TJUE consideró que la toma de impresiones dactilares por parte de las autoridades nacionales correspondientes, para su conservación en el dispositivo de almacenamiento integrado en el pasaporte, cabe dentro del concepto de tratamiento de datos de carácter personal, en el tanto consiste en una operación aplicada por un tercero destinada a la recogida, conservación, consulta o utilización de los datos personales[53].

e) Transmisión de datos entre autoridades

El TJUE ha considerado que la recogida, conservación y transmisión de datos de carácter por parte de una autoridad nacional constituye también un tratamiento de datos de carácter personal. En ese sentido, en la STJUE del caso Huber, estimó que la recogida, conservación y transmisión de los datos personales contenidos en un registro de extranjeros, constituía un tratamiento de datos de carácter personal en el sentido que expresa el artículo 2.b) de la Directiva 95/46[54].

En la STJUE del caso Bara, estimó que la transmisión de datos entre dos autoridades públicas, en el particular la comunicación de datos de carácter personal recogidos por una autoridad competente en materia de seguros de enfermedad a las

[51] STJUE de 29 de junio de 2010, asunto C-28/08 P, apartado 69.
[52] STJUE (Sala Tercera) de 19 de abril de 2012, asunto C-461/10 (caso Bonnier), apartado 51-52.
[53] STJUE de 17 de octubre de 2013, asunto C-291/12, apartado 29.
[54] STJCE de 16 de diciembre de 2008, asunto C-524/06, apartado 43.

autoridades de administración tributaria, constituye un tratamiento de datos de carácter personal[55].

f) Transferencias internacionales de datos

Más recientemente, en la STJUE, de 6 de octubre de 2015, caso Schrems, el TJUE señaló que transferir datos personales desde un Estado miembro a un tercer país, constituye en sí mismo un tratamiento de datos personales[56].

g) Filtraciones de datos y comunicación posterior de los mismos

Por su parte, el TGUE en los casos Nikolaou/Comisión y Valero Jordana, tuvo oportunidad de pronunciarse sobre el concepto de tratamiento de datos de carácter personal. En la STGUE de 12 de septiembre de 2007, caso Nikolaou/Comisión, consideró que la filtración de datos por parte de una persona de la OLAF que tenía acceso a los ellos y se los facilitó a un periodista, así como la posterior publicación de estos en un comunicado de prensa institucional, constituyen un tratamiento de datos de carácter personal[57], lo mismo que la comunicación de los nombres y los apellidos de personas que figuran en una lista de reserva de un concurso o los funcionarios mencionados en decisiones individuales de nombramiento, según lo estimó en la STJUE del caso Valero Jordana[58]. Similar postura ha mantenido, por ejemplo, en el caso Dennekamp/Parlamento, en donde dijo que la comunicación de los nombres de los diputados del Parlamento Europeo (PE) afiliados a un determinado plan de pensiones constituye un tratamiento de datos de carácter personal[59].

h) Tratamiento de datos para fines exclusivamente domésticos

(Artículo 3.2 de la Directiva 95/46)

El TJUE ha definido que la excepción contenida en artículo 3.2 de la Directiva 95/46, debe interpretarse en el sentido de que solo comprende las actividades que sean resultado de la vida privada o familiar de los particulares, como por ejemplo la correspondencia

[55] STJUE de 1 de octubre de 2015, asunto C-201/14, apartado 29.
[56] STJUE (Gran Sala) de 6 de octubre de 2015, asunto C-362/14 (caso Schrems), apartado 45.
[57] STGUE (Sala Segunda) de 12 de septiembre de 2007, asunto T-259/03 (caso Nikolaou/Comisión), apartado 204.
[58] STGUE de 07 de julio de 2011, asunto T-161/04, apartado 91.
[59] STGUE (Sala Segunda) de 23 de noviembre de 2011, asunto T-82/09 (caso Dennekamp/Parlamento), apartado 29.

doméstica o un repertorio de direcciones. Partiendo de lo anterior, en la STJUE del caso Lindqvist, indicó que la difusión de datos personales por Internet que resulten accesibles a un grupo indeterminado de personas, no constituye un tratamiento meramente para actividades personales o domésticas; por lo tanto, no está cubierto por la excepción mencionada[60].

En línea con lo anterior, en la STJUE del caso Rynes consideró que en tanto un sistema de video vigilancia operado por una persona física para fines de seguridad personal y de su familia, y que cubre al menos en parte el espacio público, abarca una zona ajena a su esfera privada, no puede considerarse que el tratamiento de los datos obtenidos sea única y exclusivamente para fines personales o domésticos, según el artículo 3.2 de la Directiva[61].

i) Tratamiento de datos para fines periodísticos

(Artículo 9 de la Directiva 95/46)

En la STJCE del caso Satakunnan Markkinapörssi y Satamedia, el TJCE consideró que el tratamiento para fines periodísticos depende de que la actividad del tratamiento se ejerza, única y exclusivamente con la finalidad de divulgar al público información, opiniones o ideas, por cualquier medio de transmisión.

El hecho de que los datos sean publicados con ánimo de lucro no impide que el tratamiento sea una actividad exclusivamente para fines periodísticos, pues toda empresa persigue obtener un beneficio de su actividad y el periodismo profesional puede llegar a depender de un cierto éxito comercial. Tampoco es determinante en dicha consideración el soporte por medio del cual se transmiten los datos; pues puede ser a través de medios clásicos como el papel o las ondas de radio, o por medios electrónicos como el Internet[62].

[60] STJUE de 6 de noviembre de 2003, asunto C-101/01, apartado 45-46.
[61] STJUE de 11 de diciembre de 2014, asunto C-212/13, apartado 33.
[62] STJCE de 16 de diciembre de 2008, asunto C-73/07, apartado 58-62.

D. Responsable del tratamiento de los datos

(*Artículo 2.d) de la Directiva 95/46)*

El artículo 2.d) y e) de la Directiva 95/46, contiene las definiciones de responsable del tratamiento y encargado del tratamiento de datos. El primero está definido como la persona física o jurídica, la autoridad pública, el servicio o cualquier otro organismo que determine, separada o conjuntamente, los fines y los medios del tratamiento de los datos; mientras que el encargado, es quien trata los datos por cuenta del responsable del tratamiento.

Una de las sentencias del TJUE más relevantes en la interpretación de la definición de responsable del tratamiento ha sido la STJUE del caso Google. En dicho caso, el Tribunal considera que al determinar un motor de búsqueda los fines y los medios de su actividad y el tratamiento de datos que se efectúa en el marco del mismo, debe necesariamente considerarse responsable del tratamiento de los datos, según lo dispuesto en el artículo 2.d) de la Directiva. Asimismo, señala que la noción de "responsable del tratamiento", debe ser interpretada de forma amplia, de acuerdo con el objetivo de la Directiva 95/46 para garantizar una protección eficaz y completa de los derechos de los interesados y, por ende, no permite excluir al gestor de un motor de búsqueda, en razón de que no ejerce un control sobre los datos publicados en las páginas web de terceros.

En ese sentido, como responsable del tratamiento, el motor de búsqueda debe asegurar que sus actividades satisfacen y cumplen con todas las exigencias de la Directiva 95/46. Aún y cuando el motor de búsqueda determinara los fines y los medios del tratamiento de forma conjunta con los editores de los sitios en Internet, ello no implica que se elimine su responsabilidad; pues el artículo 2.d) de la Directiva 95/46 resulta clara en prever que la determinación de tales condiciones puede ser realizada de forma sola o en conjunto con otros.

En conclusión, el TJUE estima que el motor de búsqueda es responsable del tratamiento de la actividad que lleva a cabo, la cual consiste en hallar información publicada o puesta a disposición en Internet, indexarla de manera automática, almacenarla

de forma temporal y ponerla a disposición de los internautas a través de listas de resultados[63].

E. Consentimiento del interesado

(*Artículo 2.h) y artículo 7.f de la Directiva 95/46)*

El consentimiento del interesado es uno de los aspectos claves del derecho a la protección de datos de carácter personal ha sido abordado en varias sentencias por el TJUE. La Directiva 95/46 es clara en su artículo 2. h) en indicar que el tratamiento de datos debe partir del consentimiento del interesado, salvo las excepciones previstas y entiende que este consentimiento es la manifestación de voluntad, libre, específica e informada, mediante la cual se acepte el tratamiento de los datos personales que le conciernen.

Sobre el consentimiento informado como manifestación inequívoca de la voluntad del interesado, el TJUE ha precisado que informar al interesado de que sus datos personales serán tratados, no es suficiente para entender que el tratamiento de los mismos se basa en el consentimiento. En estos casos, los interesados se limitan a reconocer haber sido informados, mas dicha información del tratamiento no constituye un consentimiento en los términos previstos en la Directiva 95/46[64].

Por otra parte, ha establecido el TJUE que no cabe entender que el interesado ha otorgado el consentimiento para el tratamiento de sus datos, cuando el tratamiento deriva de una exigencia legal, como por ejemplo, la toma de impresiones dactilares para la obtención de un pasaporte[65].

Asimismo, ha señalado en la sentencia del caso ASNEF que el artículo 7.f) de la Directiva 95/46 establece dos supuestos acumulativos para que un tratamiento de datos personales sin consentimiento del interesado sea lícito, a saber, que sea necesario para la satisfacción de un interés legítimo perseguido por el responsable del tratamiento o por el tercero a quien se comuniquen los datos, y, no prevalezcan los derechos y las libertades fundamentales del interesado. Este artículo debe ser interpretado de forma exhaustiva y

[63] STJUE de 13 de mayo de 2014, asunto C-131/12, apartado 33-41.
[64] STJUE de 9 de noviembre de 2010, asuntos C-92/09 y C-93/09, apartado 63-64.
[65] STJUE de 17 de octubre de 2013, asunto C-291/12, apartado 32.

taxativa, de manera que se opone a toda normativa que exija, en caso de que no exista el consentimiento del interesado, requisitos adicionales a los mencionados[66].

F. Licitud del tratamiento: necesidad y proporcionalidad

(Artículo 7.e) de la Directiva 95/45 y artículos 7 y 8 de la CDFUE)

Sobre la proporcionalidad y la necesidad en el tratamiento de los datos, el TJUE se ha pronunciado en reiteradas ocasiones. El artículo 7.e) de la Directiva 95/46 señala que el tratamiento de datos puede ser lícito si es necesario para cumplir 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. Es doctrina del TJUE que el concepto de necesidad no tiene un contenido variable en función de los Estados miembros, en virtud de la función armonizadora de la Directiva 95/46[67].

Además, ha interpretado que por ejemplo un registro de extranjeros centralizados resulta necesario en el sentido del artículo 7.e) de la Directiva 95/46, siempre y cuando contribuya a una aplicación más eficaz de la normativa en derecho de residencia[68].

En relación con este mismo tema, el TJUE ha considerado que el establecimiento de un sistema de filtrado que implique un análisis de todos los contenidos y la recopilación e identificación de las direcciones IP de los usuarios que hayan originado el envío de contenidos ilícitos en la red, sin que distinga entre contenidos lícitos e ilícitos, no respeta el principio de proporcionalidad y no garantiza un justo equilibro entre el derecho a la propiedad intelectual y el derecho a la protección de datos, así como a la libertad para recibir o comunicar informaciones[69].

En el caso Schwartz, por ejemplo, consideró que la toma de impresiones dactilares, con el fin de prevenir la falsificación de pasaportes e impedir la entrada ilegal de personas en el territorio de la UE, es un mecanismo idóneo y no va más allá de lo necesario para la consecución de tal fin. Asimismo, en el caso concreto, estima que no se demostró la existencia de medidas menos invasivas de los derechos reconocidos en los artículos 7 y 8 de la CDFUE y que contribuyan con suficiente eficacia al objetivo

[66] STJUE de 24 de noviembre de 2011, asuntos C-468/10 y C-469/10, apartado 37-39.
[67] STJCE de 16 de diciembre de 2008, asunto C-524/06, apartado 52.
[68] *Ibíd.* apartado 62.
[69] STJUE de 24 de noviembre de 2011, asunto C-70/10, apartado 51-52.

perseguido. Si bien existen medidas alternativas como la captación de una imagen del iris del ojo, no se garantiza que dicha medida sea menos invasiva.[70].

También, ha señalado que determinados datos de tráfico pueden ser transmitidos por parte del responsable del tratamiento a un cesionario de créditos para que efectúe el cobro de créditos impagados, siempre y cuando lo haga bajo la autoridad del proveedor de los servicios –sea bajo las órdenes y control de este– y se limite solo al tratamiento de los datos de tráfico estrictamente necesarios[71].

De igual forma, el Tribunal ha dispuesto que el tratamiento de datos personales puede resultar necesario para dar cumplimiento a las obligaciones del empleador y para la ejecución de las inspecciones por parte de las autoridades en materia laboral. Puede que resulte necesario otorgar un acceso de forma inmediata a los datos contenidos en el registro a la autoridad competente, siempre y cuando ello contribuya a una aplicación más eficaz de la normativa sobre condiciones laborales[72].

Cabe mencionar la STJUE, de 8 de abril de 2014, por medio de la cual se anuló la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados, en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o redes públicas de comunicaciones, que obligaba a los proveedores de servicios de comunicaciones telefónicas a conservar los datos de tráfico y localización de las comunicaciones, durante un plazo determinado, con el fin de prevenir, investigar y enjuiciar delitos, así como para garantizar la seguridad del Estado.

En esta ocasión, el TJUE consideró que la Directiva 2006/24 incluía de manera generalizada a todas las personas, medios de comunicación electrónica y datos relativos al tráfico, sin que existieran diferencias, limitantes o excepciones en función del objetivo perseguido de lucha contra el terrorismo y crimen organizado. La omisión de establecer reglas claras y precisas que regularan la injerencia que tenía la Directiva sobre los artículos 7 y 8 de la CDFUE así como la falta de medidas que limitaran la injerencia a lo estrictamente necesario, hicieron que la Directiva deviniera en una injerencia

[70] STJUE de 17 de octubre de 2013, asunto C-291/12, apartado 41, 48-53.
[71] STJUE (Sala Tercera) de 22 de noviembre de 2012, asunto C-119/12 (caso Probst), apartado 17, 19-21.
[72] STJUE de 30 de mayo de 2013, asunto C-342/12, apartado 35-38, 41.

especialmente grave sobre los derechos fundamentales tutelados por el ordenamiento de la UE[73] que únicamente podría tener como consecuencia su anulación.

Similar razonamiento siguió el TJUE en el caso Schrems en el que se cuestionó la Decisión 2000/520/CE, de 26 de julio de 2000, sobre la adecuación de la protección conferida a los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas frecuentes publicadas por el Departamento de Comercio de los Estados Unidos de América. Al no limitarse a la Decisión a lo estrictamente necesario y permitir el tratamiento de datos de forma generalizada y sin prever la posibilidad de que el afectado ejerciera sus derechos, estimó que no respetaba lo dispuesto en el artículo 8 de la CDFUE. Asimismo, consideró que vulneraba el artículo 7 de la CDFUE al permitir a las autoridades públicas el acceso al contenido de las comunicaciones electrónicas de forma generalizada[74].

En idénticos términos se pronunció en su reciente STJUE del caso Tele2 Sverige, por medio del cual enjuició el requerimiento de la autoridad sueca de control de los servicios de correos y telecomunicaciones a Tele2 Sverige, de conservar los datos de tráfico y localización de sus abonados y usuarios registrados y la Ley inglesa de 2014 sobre conservación de datos y facultades de investigación. Según el criterio del TJUE, se opone al artículo 15 de la Directiva 2002/58, en relación con los artículos 7, 8, 11 y 52 de la CDFUE, una normativa nacional que permite la conservación generalizada e indiferenciada de datos de tráfico y localización de todos los abonados y los usuarios registrados, de acuerdo con todos los medios de comunicación electrónica.

De igual manera, consideró que se opone a dicha normativa comunitaria una norma nacional que regule el acceso de las autoridades nacionales competentes a todos los datos conservados, sin limitar dicho acceso en el marco de la lucha contra la delincuencia organizada, a los casos graves y sin supeditar el acceso a un control previo por parte de un órgano jurisdiccional o una autoridad administrativa independiente[75].

[73] STJUE (Gran Sala) de 8 de abril de 2014, asuntos C-293/12 y C-594/12 (caso Digital Rights Ireland y Seitlinger y otros), apartado 52, 65.
[74] STJUE de 6 de octubre de 2015, C-362/14, apartado 93-95.
[75] STJUE (Gran Sala) de 21 de diciembre de 2016, asuntos C-203/15 y C-698/15 (caso Tele2Sverige), apartado 112, 125.

Más adelante nos ocuparemos de otros casos en los que se ha pronunciado sobre la proporcionalidad y la necesidad de determinadas medidas, según la consecución de la transparencia y el acceso a los documentos.

G. Derechos de los interesados

(*Artículos 11, 12 y 14 de la Directiva 95/46*)

a) Derecho de acceso y rectificación

De acuerdo con el catálogo de derechos que establece la Directiva 95/46, el TJUE ha definido que la exigencia del tratamiento leal de los datos previsto en el artículo 6 de la Directiva 95/46, obliga a una administración pública a informar a los interesados de la transmisión de tales datos a otra administración pública para su tratamiento, sin que pueda entenderse que una obligación legal necesariamente constituye una información previa que dispense al responsable del tratamiento de su obligación de informar a las personas sobre el tratamiento y cesión de sus datos[76].

También, ha reconocido que el derecho a la intimidad comprende el derecho de toda persona a cerciorarse de la exactitud y la licitud del tratamiento de sus datos personales, en especial, que los datos sean exactos y comunicados únicamente a los destinatarios autorizados. Para efectuar dicha comprobación, toda persona debe disfrutar del derecho de acceso a los datos que le conciernen y son objeto de un tratamiento.

En ese sentido, el TJUE ha reconocido que el derecho de acceso a los datos contenido en el artículo 12.a) de la Directiva 95/46 resulta indispensable para que el interesado pueda ejercer los derechos de rectificación, supresión, bloqueo y la notificación a los terceros de toda rectificación, supresión o bloqueo de datos (artículo 12.b) y c) de la Directiva). El derecho de acceso es también necesario para el ejercicio de otros derechos, como por ejemplo el derecho de oposición al tratamiento de los datos personales y a recurrir judicialmente, según lo dispuesto en el artículo 14 de la Directiva 95/46[77].

Asimismo, como ya se mencionó en el caso YS y otros, donde se reclamaba el acceso a una minuta redactada con carácter previo a la resolución de permiso de

[76] STJUE de 1 de octubre de 2015, asunto C-201/14, apartado 34-38.
[77] STJCE de 7 de mayo de 2009, asunto C-553/07, apartado 49-52.

residencia temporal de nacionales de un tercer país, así como las consideraciones jurídicas de la autoridad competente sobre el caso concreto, el TJUE entendió que siendo que la Directiva 95/46 no tutela un derecho de acceso a los documentos, como para facilitar la totalidad de la minuta (consideraciones jurídicas y datos personales), el derecho de acceso del interesado a sus datos, para el correcto ejercicio de los derechos de rectificación, bloqueo o supresión, se puede garantizar por medio de una comunicación en donde se detalle de forma inteligible, los datos personales que le conciernen y estén siendo tratados. En estos casos, el derecho de acceso se ve satisfecho con una comunicación que ofrezca una idea completa de los datos y permita verificar la exactitud y licitud del tratamiento[78].

Igualmente, ha definido que la comunicación que debe hacer el responsable del tratamiento de los datos sobre la identidad del encargado, los fines del tratamiento y la información necesaria para garantizar un tratamiento leal de los datos, debe incluir también la notificación de la existencia de derechos de acceso y rectificación de los datos que le conciernen al interesado, según lo dispuesto en el artículo 11.1.b) y c) de la Directiva 95/46[79].

Sobre el derecho de acceso, ha reconocido que las autoridades públicas que se encargan del tratamiento pueden percibir gastos con ocasión de garantizar el ejercicio del derecho de acceso a los datos, siempre y cuando los mismos no representen un importe excesivo, tal y como lo contempla el artículo 12.a) de la Directiva 95/46, ni constituya un impedimento u obstáculo para el ejercicio del derecho de acceso garantizado por esa misma disposición[80].

b) Derecho al olvido

Sin lugar a dudas una de las sentencias más relevantes del TJUE sobre los derechos de los interesados es el reconocimiento del derecho al olvido en el caso Google. Dado el impacto mediático que ha tenido esta STJUE así como la relevancia que tiene para el caso español, se hará un análisis más extenso del mismo.

En sentencia de 13 de mayo de 2014, asunto C-131/12 (caso Google), el TJUE conoció de una cuestión prejudicial planteada por la Audiencia Nacional y que tiene su

[78] STJUE de 17 de julio de 2013, asuntos C-141/12 y C-372/12, apartado 57-59.
[79] STJUE de 1 de octubre de 2015, asunto C-201/14, apartado 42.
[80] STJUE (Sala Octava) de 12 de diciembre de 2013, asunto C-486/12 (caso X), apartado 28-29.

origen en un proceso judicial en el que se discuten "las obligaciones que tienen los gestores de los motores de búsqueda en la protección de datos personales de aquellos interesados que no desean que determinada información, publicada en páginas web de terceros, que contiene sus datos personales y permite relacionarles con la misma, sea localizada, indexada y sea puesta a disposición de los internautas de forma indefinida".[81]

El TJUE reitera su jurisprudencia en el caso Lindqvist y recuerda que hacer referencia a datos personales en una página web, es considerado un tratamiento de datos de conformidad con lo dispuesto en el artículo 2.b) de la Directiva 95/46. En ese sentido, el gestor de un motor de búsqueda, al explorar Internet de manera automatizada, constante y sistemática en búsqueda, recoge los datos que extrae, registra posteriormente mediante el uso de sus programas de indexación, conserva en sus servidores, y, comunica y facilita el acceso a usuarios en forma de lista de resultados de sus búsquedas. Todo lo anterior constituye tratamiento de datos, según la Directiva 95/46, con independencia de que el motor de búsqueda lleve a cabo las mismas operaciones con otros tipos de información y no distinga entre datos personales y estos, así como que la información haya sido objeto de publicación en Internet sin modificación alguna por parte del gestor. Señala, al igual que en la sentencia del caso Markkinapörssi y Satamedia, que aún y cuando se trate de información ya publicada en medios de comunicación, dichas operaciones se consideran tratamiento de datos.[82]

Asimismo, define que el gestor del motor de búsqueda debe ser considerado como responsable del tratamiento de conformidad con el artículo 2.d) de la Directiva 95/46 y no procede excluir de dicha norma al gestor de búsqueda debido a que no ejerce un control sobre los datos personales publicados en las páginas web de terceros.[83]

Continúa indicando el TJUE que la organización y agregación de la información que se publica en Internet efectuada por los motores de búsqueda para facilitar a los usuarios el acceso a la misma, puede conducir a que cuando la búsqueda sea realice a partir del nombre de una persona física, a que se obtenga, mediante la lista de resultados, una visión de la información relativa a esa persona y que le permite establecer, en mayor o menor medida, un perfil del interesado. Es por esa razón, que los gestores de los motores de búsqueda, en la medida en que pueden afectar el derecho fundamental a la privacidad

[81] STJUE de 13 de mayo de 2014, asunto C-131/12, apartado 17.
[82] *Ibíd.* apartados 27-30.
[83] *Ibíd.* apartados 32-34.

y la protección de datos de carácter personal, debe garantizar, dentro de sus competencias y posibilidades, que la actividad que realiza satisfaga las exigencias de la Directiva 95/46 y se garantice asimismo los derechos e intereses de los interesados, en especial el derecho a la protección de datos de carácter personal y el respeto de la vida privada.[84]

Igualmente, a criterio del TJUE, el hecho de que los editores de los sitios de internet dispongan de la facultad de indicar a los gestores de los motores de búsqueda que determinada información sea excluida total o parcialmente de los índices automáticos de los motores, ello no implica que la falta de indicación por parte de los editores, exima al gestor de su responsabilidad por el tratamiento de datos personales que lleva a cabo el motor.[85]

A la luz de lo anteriormente expuesto, en resumen el TJUE indica que las "letras a) y b), que el artículo 2, letras b) y d), de la Directiva 95/46 debe interpretarse en el sentido de que, por un lado, la actividad de motor de búsqueda, que consiste en hallar información publicada o puesta en Internet, por terceros, indexarla de manera automática, almacenarla temporalmente, y por último, ponerla a disposición de los internautas según un orden de preferencia determinado, debe calificarse de 'tratamiento de datos personales', en el sentido de dicho artículo 2, letra b), cuando esa información contiene datos personales y, por otro, el gestor de un motor de búsqueda debe considerarse 'responsable de dicho tratamiento, en el sentido del mencionado artículo, letra d)."[86]

En relación con el artículo 4.1.a), de la Directiva 95/46, el TJUE considera que el tratamiento de datos personales que se realiza por medio del funcionamiento de un motor de búsqueda como Google Search, que a su vez es gestionado por una empresa domiciliada en un Estado tercero pero que dispone de un establecimiento en un Estado miembro, se efectúa en el marco de las actividades del establecimiento, si ese establecimiento está destinado a la promoción y venta de servicios publicitarios del motor de búsqueda en ese Estado miembro, y dicha actividad sirve para rentabilizar económicamente el servicio que ofrece el motor de búsqueda.[87]

Asimismo, el TJUE considera que en la medida en que el motor de búsqueda, a través de sus listas de resultados realizadas a partir del nombre de una persona física,

[84] *Ibíd.* apartados 37, 38.
[85] *Ibíd.* apartado 39-40.
[86] *Ibíd.* apartado 41.
[87] *Ibíd.* aparato 57.

facilita en gran medida la accesibilidad de la información contenida en páginas web a cualquier internauta que realice una búsqueda sobre el interesado y puede desempeñar un papel decisivo para la difusión de dicha información, puede resultar en una injerencia en los derechos e intereses de una persona que la publicación que efectuó el editor de la página web. En ese sentido, siempre y cuando concurran los presupuestos legales de los artículos 12 y 14 de la Directiva 95/46, un motor de búsqueda, en el caso concreto Google Search, está obligado a eliminar de su lista de resultados, vínculos a páginas web publicadas por terceros y que contengan información relativa a una persona física, aún y cuando esta información sea lícita y no se borre previa o simultáneamente de la página web del editor.[88]

En relación con la solicitud de eliminación de vínculos a páginas web en la lista de resultados de un buscador, el TJUE considera que de conformidad con lo dispuesto en el artículo 12.b) de la Directiva 95/46, en aquellos supuestos en que la información sea inadecuada, no sea pertinente, o sea excesiva en relación con los fines del tratamiento realizado por el motor de búsqueda, la información y los vínculos de la lista del buscador deben ser eliminados. El interesado puede de conformidad con los artículos 7 y 8 de la CDFUE, solicitar que la información que le afecta ya no se ponga a disposición del público mediante la inclusión de la misma en las litas de resultados, prevaleciendo estos derechos frente al interés económico del gestor del motor de búsqueda y del interés del público que lo utiliza en encontrar la información en una búsqueda sobre el nombre del interesado; lo contrario sucedería, sin en el caso concreto, prevalece el interés del púbico en tener información a la información de que se trate.[89]

Concluye, en el caso concreto que "en relación con una situación como la del litigio principal, que se refiere a la presentación, en la lista de resultados que el internauta obtiene al efectuar una búsqueda a partir del nombre del interesado con ayuda de Google Search, de vínculos a dos páginas de archivos en línea de un periódico que contienen anuncios que mencionan el nombre de esta persona y relativos a una subasta inmobiliaria vinculada a un embargo por deudas a la seguridad social, es preciso considerar que, teniendo en cuenta el carácter sensible de la información contenida en dichos anuncios para la vida privada de esta persona y de que su publicación inicial se remonta a 16 años atrás, el interesado justifica que tiene derecho a que esta información ya no se vincule a

[88] *Ibíd.* apartados 87-88.
[89] *Ibíd.* apartado 94.

su nombre mediante esa lista. Por tanto, en la medida en que en el caso de autos no parece existir razones concretas que justifiquen un interés preponderante del público en tener acceso a esta información en el marco de tal búsqueda, lo que no obstante incumbe comprobar al órgano jurisdiccional remitente, el interesado puede, en virtud de los artículos 12, letra b), y 14, párrafo primero, letra a), de la Directiva 95/46, exigir que se eliminen estos vínculos de la lista de resultados."[90]

En resumen, de acuerdo con lo establecido por el TJUE, lo dispuesto en el artículo 12.b) de la Directiva 95/46 implica que en los supuestos en que la información sea inadecuada, no sea pertinente o resulte excesiva en relación con los fines del tratamiento realizado por el motor de búsqueda, la información y los vínculos de la lista del buscador deben ser eliminados. De forma que el interesado puede solicitar que la información que le concierne y le afecta ya no se ponga a disposición del público mediante la inclusión de la misma en las listas de resultados del motor de búsqueda, en cuyo caso prevalecen estos derechos frente al interés económico del motor de búsqueda y el interés del público que lo utiliza en encontrar la información en una búsqueda sobre el nombre del afectado; lo contrario sucedería, si en el caso concreto, prevalece el interés del público en tener acceso a la información de que se trate.[91]

La STJUE del caso Google y sus implicaciones han sido ampliamente discutidas doctrinalmente[92]. En palabras de POLLICINO Y BASSINI, se trata básicamente de la potestad de toda persona de recuperar la posesión de su propia historia personal así como recuperar

[90] *Ibíd.* apartado 98.
[91] *Ibíd.* , apartado 94.
[92] In extenso, puede consultarse: Cobas Cobiella, M.E. (2017). Derecho al olvido: de la STJUE de 2014 al Reglamento europeo de Protección de Datos. *Actualidad civil*, núm. 1, 2017. pp. 98-116; Berrocal Lanzarot, A.I. (2017). El derecho de supresión de datos o derecho al olvido en el Reglamento General de Protección de Datos. *Revista general de legislación y jurisprudencia, núm.* 1, 2017. pp. 7-71; Chéliz Inglés, M.C. (2016). El "derecho al olvido digital". Una exigencia de las nuevas tecnologías recogida en el futuro Reglamento General de Protección de Datos. *Actualidad Jurídica Iberoamericana*, núm. 5, agosto 2016. pp.255-271; Martínez Otero, J.M. (2015). El derecho al olvido en Internet: debates cerrados y cuestiones abiertas tras la STJUE Google vs AEPD y Mario Costeja. *Revista de Derecho Político, núm.* 93, mayo-agosto 2015. pp. 103-142; Pazos Castro R. (2015). El funcionamiento de los motores de búsqueda en Internet y la política de protección de datos personales, ¿una relación imposible? Recuperado de: http://www.indret.com/pdf/1118_es.pdf ; Azurmendi, A. (2015). Por un "derecho al olvido" para los europeos: aportaciones jurisprudenciales de la sentencia del Tribunal de Justicia europeo del caso Google Spain y su recepción por la sentencia de la audiencia nacional española de 29 de diciembre de 2014. *Revista de Derecho Político*, núm. 92, enero-abril 2015. pp. 273-310; López Portas, B. (2015). La configuración del derecho al olvido en el Derecho español al tenor de la doctrina del TJUE. *Revista de Derecho Político*, núm. 93, 2015. pp. 143-175; Martínez Caballero, J. Cómo conjugar el derecho al olvido. *Revista Jurídica de Castilla-La Mancha*, núm. 57 – Enero/Diciembre 2015. pp.143-185; Rallo Lombarte, Artemi. (2014). El derecho al olvido en Internet Google versus España. Madrid: Centro de Estudios Políticos y Constitucionales.

el dominio relativo a hechos personales después de que estos hubiesen sido legítimamente divulgados. Es, "*sostanzialmente, una reintegrazione del potere di disponere"*.[93] Esta facultad se ejerce ante el motor de búsqueda, quien estaría en la obligación de eliminar de las listas de resultados, los enlaces que conduzcan a la información que se pretende cancelar, pero no constituye en sí, una eliminación de la información de la página web que lo contiene. Es decir, con el ejercicio del derecho lo que el interesado obtiene es que a través de un motor de búsqueda no se obtengan dentro de los resultados los enlaces que conducen a las noticias que contienen información inexacta, pero no obliga a quien trata los datos en la página que los contiene a que elimine la información.

Si bien es un derecho que no aparecía mencionado de forma expresa en la Directiva 95/46 y ha sido incluido dentro del catálogo de derechos del RGPD, algunos autores consideran que no se trata más que de la concreción en el ámbito del Internet de derechos ya reconocidos por la normativa comunitaria[94]. Sin perjuicio de lo anterior, como menciona ÁLVAREZ CARO, dejando de lado cuestiones semánticas, existe una importante relevancia de la inclusión de este derecho dentro del RPGD, en el tanto "coloca al interesado en una posición de control de sus datos personales y es el resultado de la constatación de una necesidad de adaptar el derecho de la cancelación de datos a la Era digital, permitiendo el ejercicio del mismo en el entorno de Internet, de los

[93] Pollicino, O.; Bassini, M. (2013). Diritto all'oblio: I piu recenti spunti riconstruttivi nella dimensione comparada ed europea. En F. Pizzetti (Coord.) *Il caso del diritto all'oblio*. ____: Giappichelli. pp. 186-228.
[94] En ese sentido, PAZOS CASTRO menciona: "A decir verdad, con la simple lectura de la sentencia podría mantenerse que se ha otorgado un nuevo nombre a derechos ya conocidos como son los de oposición y cancelación, si bien este nuevo nombre se emplearía para una aplicación particular de los mismos. Esto es fácilmente apreciable mediante una simple comparación entre cómo explica el Tribunal de Justicia la cuestión prejudicial relativa a los derechos de oposición y cancelación de forma concreta, y cómo resume la cuestión prejudicial en la que se encuentra implícito el derecho al olvido". Ver: Pazos Castro, R. (2015). EL mal llamado "derecho al olvido" en la era de Internet. *Boletín del Ministerio de Justicia, a*ño LXIX, Núm. 2183, noviembre de 2015. p. 40. En similar sentido MINERO ALEJANDRE indica: "El TJUE no crea un derecho nuevo. El denominado derecho al olvido digital no es otra cosa que la aplicación al tratamiento de datos realizado en Internet de los derechos de cancelación y oposición, presentes en los artículos 12.b) y 14.a) de la Directiva 95/46/CE y, con mayor profundidad, en el artículo 17 del Reglamento General para la protección de datos. Lo pionero del pronunciamiento del TJUE es la identidad del sujeto contra el que se dirige la reclamación para el ejercicio del derecho al olvido: la filial española de la compañía estadounidense gestora del buscador Google, en el entendido de que la empresa española, dedicada a la venta de espacios publicitarios en el conocido motor de búsqueda, es fuente de financiación de su matriz y, por ello, ha de responder en la Unión Europea del cumplimiento de la Directiva y de las normas nacionales que la transponen". Ver en: Minero Alejandre, G. (2017). Presente y futuro de la protección de datos personales. Análisis normativo y jurisprudencial desde una perspectiva nacional y europea. *Anuario Jurídico y Económico Escurialense,* L (2017). pp. 13-58.

prestadores de servicios de la sociedad de la información, y, de una Red, que se caracteriza por los enlaces."[95]

H. Medidas de seguridad

(Artículo 17.1 de la Directiva 95/46)

En relación con la obligación contenida en el 17.1 de la Directiva 95/46, sobre adopción de medidas de seguridad, el TJUE ha señalado que corresponde a los Estados establecer la obligación de adoptar las medidas técnicas y de organización, con el fin de garantizar un nivel adecuado de seguridad en el tratamiento de los datos y corresponde a los responsables del tratamiento, que las medidas adoptadas sean las idóneas en relación con los riesgos que representa el tratamiento y con la naturaleza de los datos que deben protegerse, teniendo siempre en cuenta los conocimientos técnicos existentes y el coste de su aplicación.[96]

I. Transferencias internacionales a países terceros

(Artículo 25 de la Directiva 95/46)

La STJUE del caso Schrems, constituye el principal referente en cuanto a las condiciones necesarias para llevar a cabo una transmisión de datos a un tercer país. En esta sentencia el TJUE interpretó, entre otras, la noción de *"nivel de protección adecuado"* contenido en el artículo 25 de la Directiva 95/46. A criterio del TJUE, si bien no se requiere un nivel de protección idéntico al que garantiza el ordenamiento jurídico de la UE, sí se exige que el país tercero garantice en forma efectiva, por su legislación interna o compromisos internacionales, un nivel de protección de las libertades y los derechos fundamentales sustancialmente equivalente al que garantiza la Directiva 95/46. Es decir, que si bien los medios de garantía de protección en ese tercer país pueden ser diferentes, deben ser eficaces en la práctica para garantizar un nivel de protección equivalente al de la UE. Para efectos de determinar el nivel de protección, cabe observar

[95] Álvarez Caro, M. (2016). El derecho a la supresión o al olvido. En J.L. Piñar Mañas (Dir.), *Reglamento General de Protección de Datos: hacia un nuevo modelo europeo de privacidad*. Madrid: Editorial Reus. pp. 241-256.
[96] STJUE de 7 de mayo de 2009, asunto C-553/07, apartado 62; STJUE de 30 de mayo de 2013, asunto C-342/12, apartado 24-25.

la legislación interna, compromisos internacionales, así como la práctica seguida para asegurar el cumplimiento de esas reglas[97].

J. Garantía de total independencia del a autoridad de control

(Artículo 28.1 de la Directiva 95/46)

Se hará referencia en este apartado a la independencia de las autoridades de control en materia de protección de datos, según la interpretación que ha dado el TJUE a la garantía de independencia establecida en el artículo 28.1 de la Directiva 95/46, que establece que las autoridades de control deben ejercer sus funciones con total independencia.

La garantía de total independencia que contiene la Directiva pretende asegurar un control eficaz y fiable de la normativa de protección de datos. Resalta el TJUE que más que un estatuto a las autoridades de control, se perfila como una garantía que refuerza la protección de los datos personales de las personas y los organismos afectados por las decisiones de esta autoridad. En razón de lo anterior, las autoridades de control deben actuar con objetividad e imparcialidad, lo que necesariamente pasa por la garantía de independencia, que es un resguardo de toda influencia externa[98].

Asimismo, ha dicho el TJUE que el término *"con total independencia"* debe atender a su significado habitual y, en el caso de un órgano público, se refiere al estatuto que le permite y garantiza actuar con plena libertad, sin ningún tipo de instrucciones o presiones. El término "independencia" está reforzado por el objetivo "total", lo lleva implícito un poder de decisión sin ningún tipo de influencia externa hacia la autoridad de control, sea de forma directa o indirecta[99].

El Tribunal ha desarrollado también que la mera posibilidad de que las autoridades de tutela lleguen a ejercer una influencia política sobre las decisiones de las autoridades de control, obstaculiza el ejercicio de sus funciones de forma independiente y podría darse el caso de una "*obediencia anticipada*" por parte de las autoridades de control. El papel de garantes de la protección del derecho a la intimidad y la protección de datos de carácter

[97] STJUE de 6 de octubre de 2015, asunto C-362/14, apartado 73-75.
[98] STJUE (Gran Sala) de 9 de marzo de 2010, asunto C-518/07 (caso Comisión/Alemania), apartado 25.
[99] *Ibíd.* apartado 18-19

personal que asumen las autoridades de control, requiere que tanto sus funciones como sus decisiones, estén exentas de cualquier sospecha de parcialidad[100].

Con base en las consideraciones anteriores, ha estimado que someter a una autoridad de control a la tutela del Estado, no respeta la garantía de total imparcialidad que exige la Directiva 95/46[101]. Dicha garantía de independencia tampoco se respeta una normativa que dispone que el administrador de la autoridad de control sea un funcionario federal sometido a la supervisión de un jerarca, que la secretaría de la autoridad de control esté integrada a la Cancillería federal y que el Canciller federal tenga un derecho incondicional a informarse de todos los aspectos de la gestión de la autoridad de control[102]. Igualmente, dicha garantía de independencia se ve irrespetada con una disposición transitoria que ponga fin antes de tiempo al mandato del presidente de la autoridad de control, así como una normativa que contemple numerosas posibilidades de dar terminación al mandado del encargado de la autoridad de control y que permitan al poder ejecutivo influir sobre las decisiones de la autoridad de control[103].

K. Balance frente a otros derechos e intereses tutelados por el ordenamiento comunitario

En varias ocasiones el TJUE se ha encargado de resolver la cuestión del balance del derecho a la protección de datos de carácter personal cuando debe coexistir con otros derechos y fines legalmente válidos y también tutelados y perseguidos por el ordenamiento comunitario, como por ejemplo, el derecho a la propiedad intelectual, la libertad de expresión, o el acceso a la información, tema del que nos ocuparemos en un capítulo aparte.

a) Derechos de autor y propiedad intelectual

En la STJUE del caso Promusicae, el TJUE recordó que es obligación de los Estados miembros, a la hora de adaptar a su ordenamiento las normas comunitarias, procurar una interpretación que garantice un equilibrio entre los distintos derechos fundamentales que tutela el ordenamiento comunitario. También, debe procurarse que las interpretaciones que tomen no entren en conflicto con los demás derechos fundamentales

[100] *Ibíd.* apartado 36.
[101] STJUE de 9 de marzo de 2010, asunto C-518/07.
[102] STJUE (Gran Sala) de 16 de octubre de 2012, asunto C-614/10 (caso Comisión/Austria).
[103] STJUE (Gran Sala) de 8 de abril de 2014, asunto C-288/12 (caso Comisión/Hungría).

y principios generales del Derecho comunitario. Partiendo de ello, en esta caso consideró que, si bien la normativa comunitaria no obliga a los Estados miembros a imponer el deber de comunicar datos personales con el fin de garantizar la protección efectiva de los derechos de autor en un procedimiento civil, si están en la obligación de garantizar un justo equilibrio entre este derecho y el derecho a la protección de datos de carácter personal[104].

En el caso Scarlet, STJUE de 24 de noviembre de 2011, el TJUE estimó que el requerimiento judicial por medio del cual se obligaba a un proveedor de servicios de internet a implementar un sistema de filtrado de la totalidad de los contenidos de las comunicaciones electrónicas y la recopilación e identificación de las direcciones IP, con el fin de identificar determinados usuarios que estén infringiendo los derechos de autor y la propiedad intelectual, no garantiza un justo equilibrio entre la propiedad intelectual y los derechos de autor y el derecho a la protección de datos de carácter personal y la libertad de recibir o comunicar informaciones[105].

Por otra parte, en la STJUE de 19 de abril de 2012, caso Bonnier, estimó que se garantiza el justo equilibrio de los derechos en juego por medio de una normativa nacional que exige para que pueda emitirse un requerimiento judicial de comunicar datos personales a particulares en el marco de un procedimiento civil en el que se reclame la infracción a los derechos de autor y de propiedad intelectual, la existencia de indicios reales de vulneración de los derechos de propiedad intelectual sobre una obra, que los datos solicitados puedan facilitar la investigación, y que el fin perseguido por el requerimiento sea más importante que el daño o perjuicio que se puede causar a la persona afectada o a otros intereses contrapuestos[106].

Por otra parte, la coexistencia del derecho a la protección de datos de carácter personal con el derecho a la libertad de expresión, ha ocupado la atención del TJUE en varios casos. En la STJUE del caso Lindqvist, señaló que el justo equilibrio entre los derechos y los intereses en juego debe buscarse en el ámbito nacional, al aplicar a los casos concretos la normativa que adapta al Derecho interno la Directiva 95/46, así como

[104] STJUE de 29 de enero de 2008, asunto C-275/06, apartado 70.
[105] STJUE de 24 de noviembre de 2011, asunto C-70/10, apartado 53.
[106] STJUE de 19 de abril de 2012, asunto C-461/10, apartado 58.

que las disposiciones de protección de datos de esta última norma no conllevan, por sí solas, una restricción al principio general de libertad de expresión[107].

En la STJUE del caso Digital Rights Ireland y Seitlinger y otros, reconoció que si bien la Directiva 2006/24 no autorizaba la conservación del contenido de la comunicación ni de la información consultada al utilizar una red de comunicaciones electrónicas, no se excluye que la conservación de datos para rastrear e identificar el origen de una comunicación y su destino, para identificar fecha, hora y duración de la comunicación, entre otros, puedan causar una injerencia grave en el derecho a la libertad de expresión[108].

Recapitulación

El derecho a la protección de datos de carácter personal en el marco normativo europeo, ha encontrado su pilar fundamental en la Directiva 95/46, la cual refleja, en cierta medida, algunos de los antecedentes que ya existían al nivel del Consejo de Europa, como el CEDH y el Convenio 108, así como a la interpretación que había dado el TEDH a ambos instrumentos jurídicos y del cual desprendía, del artículo 8 del CEDH, un derecho a la protección de datos de carácter personal.

Han sido numerosos los avances de la tecnología y la sociedad de la información desde que se comenzara a discutir la merecedora y necesaria protección de los datos de carácter personal, y cada vez, con más frecuencia, suelen ser más rápidos, radicales y con capacidad de afectar casi la totalidad de ámbitos de nuestra vida diaria.

Surge entonces así la pregunta de cómo se mantiene la vigencia de un derecho cuando está expuesto a cambios drásticos, repentinos y continuos, en especial, cuando está íntimamente ligado con los avances tecnológicos, la informática, el uso del Internet, las redes sociales, las transferencias globalizadas de datos, entre muchos otros factores a los que se exponen nuestros datos personales.

[107] STJCE de 6 de noviembre de 2003, asunto C-101/01, apartado 85-89.
[108] STJUE de 8 de abril de 2014, asuntos C-293/12 y C-594/12, apartado 28.

Desde la Directiva 95/46 y hasta la aprobación del RGPD, esta labor de actualización y vigencia del derecho ha estado a cargo del TJUE, quien a través de su jurisprudencia ha actualizado el derecho y le ha dado contenido frente a los abusos que se pueden desprenderé de los avances tecnológicos, haciendo de este derecho, concebido inicialmente con un carácter de libre circulación de los datos, un verdadero derecho fundamental, especialmente después de la promulgación de la CDFUE –artículo 8 sobre protección de datos personales- y la entrada en vigencia del Tratado de Lisboa en 2009.

La jurisprudencia del TJUE refleja esta situación de cambios constantes. Evidencia de ello es el camino que ha recorrido desde sus primeras sentencias, en las que se encargó de la definición de dato de carácter personal o la correcta trasposición de la Directiva 95/46, hasta sentencias más recientes que han tenido por objeto el análisis de la tutela del derecho a la protección de datos personales en los flujos transfronterizos de información o el derecho de toda persona a "ser olvidado" en los motores de búsqueda de Internet bajo determinadas circunstancias, cuestiones propias de una sociedad globalizada y constantemente expuesta al uso de nuevas tecnologías y el Internet.

Sus más de 15 años interpretando el derecho a la protección de datos personales en diferentes contextos, han valido para que parte de su doctrina haya sido incorporada al nuevo RGPD, ya sea mediante el refuerzo de principios y derechos ya existentes, así como a través de la positivización de derechos, como el llamado derecho al olvido, reconocido en la STJUE del caso Google/Spain.

Aún y con la entrada en vigencia del RGPD, la labor que seguirá desarrollando el TJUE será trascendental, pues porque si bien es cierto a través de este Reglamento se actualiza la normativa vigente, los cambios tecnológicos irán muy por delante a la normativa –nótese que la actualización de la Directiva 95/46 tardó poco más de 15 años-, siendo para ello necesario el constante y continuo redimensionamiento del derecho a la protección de datos de carácter personal, a través de la jurisprudencia, en este caso, del TJUE.

Capítulo II. Adecuación de la normativa europea en materia de protección de datos: el Reglamento General de Protección de Datos

SUMARIO: 1. Cuestiones preliminares. 2. Recuento general del nuevo marco normativo. 3. Principales cambios. A. Reconocimiento expreso del principio de transparencia y el principio de minimización. B. Exigencias sobre el consentimiento informado. C. El principio de responsabilidad proactiva. D. Seudonimización de los datos de carácter personal. E. Consentimiento informado en caso de menores. F. Categorías especiales de protección de datos. G. Reconocimiento de derechos del interesado. a) Derecho de supresión (derecho al olvido). b) Derecho a la limitación del tratamiento. c) Derecho a la portabilidad de datos. H. Decisiones individuales automatizadas y elaboración de perfiles. I. Responsabilidad del responsable del tratamiento de datos y *privacy by design*. J. Notificación de una violación de seguridad a la autoridad de control. K. Evaluación de impacto y comunicación a interesados. L. Delegado de protección de datos. M. Disposiciones sobre transferencias internacionales de datos. N. Sanciones y multas. 4. Acceso a la información y protección de datos personales a la luz del RGPD.

1. Cuestiones preliminares

Este capítulo contiene un análisis del nuevo marco normativo en materia de protección de datos de la UE: el RGPD. Como mencionábamos ya en el capítulo anterior, han pasado más de 15 años desde que entró en vigencia la Directiva 95/46, pilar fundamental del derecho a la protección de datos personales en la UE, hasta que en 2015 se aprobara finalmente el RGPD por medio del cual no sólo se pretende homogeneizar la protección de datos personales en la UE, sino que también actualizar el marco normativo a los nuevos retos que suponen los avances de la tecnología.

Para ello, se hará un análisis de los aspectos más relevantes de esta nueva regulación, especialmente en lo que se refiere al cambio de paradigma de un enfoque de la protección de datos personales reactivo a una protección de datos proactiva, en la que los responsables y encargados del tratamiento de los datos, están en todo momento en la obligación de demostrar su cumplimiento con la normativa de protección de datos personales.

Este nuevo RGPD contiene una serie de disposiciones, algunas novedosas, otras que se derivan de la jurisprudencia del TJUE, así como normas que constituyen un reforzamiento de las ya existentes en la Directiva 95/46, o bien, una reiteración de las mismas en el nuevo marco normativo.

Centraremos nuestro análisis en algunas de las disposiciones que hemos considerado más relevantes, sea por su trascendencia o porque resultan del todo novedosas –al menos

en su positivización- en el ordenamiento jurídico comunitario, con independencia de que algunos autores, como se verá, consideren que se trata de los principios del derecho a la protección de datos personales que siempre han existido pero adaptados al contexto de las nuevas tecnologías (como por ejemplo, el derecho al olvido para algún sector doctrinal). Para una comprensión más clara de las novedades que representa el nuevo RGPD, se ha realizado el análisis siguiendo el orden sistemático de artículos que tiene el propio RGPD, titulando eso sí, cada categoría, según el aspecto de la protección de datos personales que regule.

Por último, hemos incluido un apartado en el que nos referiremos a la casi inexistente regulación de la relación entre transparencia y protección de datos en el nuevo RGPD, lo que a su vez permite conectar con el siguiente capítulo, en el que se abordará en específico la cuestión de la transparencia y la protección de datos en el ordenamiento comunitario, relación que sin duda alguna, como casi todos los aspectos de la vida cotidiana que dependen del tratamiento de datos, se verá afectada, al menos en términos generales por el RGPD. Ante la ausencia de una regulación clara o expresa, o de al menos la positivización de algún criterio interpretativo en el RGPD que permitiese dar mayores luces a la solución del inevitable conflicto entre transparencia, acceso a los documentos y protección de datos de carácter personal, parece que el legislador comunitario prefirió no regular en detalle la cuestión, quedando su tratamiento supeditado a la jurisprudencia del TJUE, como ha venido sucediendo hasta ahora, pero eso sí, que tendrá nuevos matices a partir de mayo de 2018.

2. Recuento general del nuevo marco normativo

El RGPD que ha entrado en vigor en 2016 y aplicará a partir del 25 de mayo de 2018, es el resultado de una combinación de nuevas reglas, prácticas y de algunos derechos ya presentes en la Directiva[109], y en algunos casos, de la incorporación de la jurisprudencia y doctrina del TJUE. Estos cambios, suponen tanto para los encargados como para los responsables de tratar los datos de carácter personal, sean personas físicas, organizaciones públicas o privadas[110], mayores obligaciones y compromisos con la protección y

[109] Blume, P. (2014).The myths pertaining to the proposed General Data Protection Regulation. *International Data Privacy Law*, 2014. Vol. 4, núm. 4. pp. 269-273

[110] En el caso de las organizaciones privadas, algunos autores ya se mostraban preocupados del impacto económico que tendría en las empresas la entrada en vigor del RGPD. En ese sentido, CIPRIANI menciona: "moreover, with the exception of the GDPR's impact assessment conducted by the European Commission, the literature we have examined shows that the costs of GDPR's adoption might offset the efficiency gains.

salvaguarda de este derecho, con el fin de devolverle al ciudadano el control de sus datos personales, porque "si la historia de la privacidad nos ha enseñado algo, es que la pérdida del individuo del control de sus datos personales conlleva a mayores abusos en su privacidad, no pocos ni pequeños".[111]

Sin duda alguna, una de sus principales implicaciones viene dada del cambio de paradigma de un enfoque reactivo a un enfoque proactivo por parte de los responsables y encargados del tratamiento de datos, tal y como se explicará más adelante.

Ese enfoque, a través del principio de responsabilidad activa, es el que para algunos autores como ALHADEFF ET AL, permitirá responder y poder manejar los retos que se incrementan con la globalización de los flujos de información, los retos del comercio electrónico, la nube, entre otros que puedan ir surgiendo. Se trata de una obligación de buscar mecanismos novedosos que permitan implementar las disposiciones sustantivas de la normativa vigente –RGPD- ante los nuevos retos que puedan surgir.[112]

Por otra parte, una de las principales insignias del RGPD es que trae consigo un refuerzo en el control que los ciudadanos tienen sobre sus datos de carácter personal, en especial en aspectos que constituyen las bases del tratamiento de datos personales, como lo es el consentimiento del titular. Sobre este aspecto, resulta enfático el RGPD en establecer que el consentimiento, con carácter general, debe ser libre, informado, específico e inequívoco, dependiendo este último elemento de una acción o manifestación clara y positiva que permita sin lugar a duda, comprobar el consentimiento del titular de los datos. Por el contrario, no puede desprenderse que se ha otorgado el consentimiento para el tratamiento de los datos, del silencio o la simple inacción del interesado; en la

---

The limitations imposed on the processing of personal data could hamper the capacity of the European companies to monetize them. Further economic analysis of the dynamic trade-off between costs and benefits of the GDPR is needed. The European reform proposal should achieve a balance between privacy protection requirements and business opportunities, while imposing the extraterritorial application of the European data protection law. Increasing the administrative burden might not help improve the competitiveness of European digital service providers. An efficient European policy should take more into account the pros and cons of successful personal data-based business models all over the world. It must rebalance the rules with more room given to flexibility and ex-post effects-based accountability in order to support the role of the European industry in this new economy of innovative services to the benefit of the European users". Ver en: Ciriani, S. (2015). The Economic Impact of the European Reform of Data Protection. *Digiworld Economic Journal*, núm. 97, 1st, Q. 2015. pp. 41-58.

[111] Cavoukian, A. (2015) Evolving FIPPs: *Proactive Approaches to Privacy*, Not Privacy Paternalism. En S. Gutwirth, R. Leenes y P. de Hert (Eds.) *Reforming European Data Protection Law. Law, Governance and Technology Series (20)*. Bruselas: Springer. pp.293-310.

[112] Alhadeff et al (2012). The Accountability Principle in Data Protection Regulation: Origin, Development and Future Decisions. En D. Guagnin et al (Eds.) Managing Privacy Trough Accountability. Recuperado de: http://www.palgrave.com/us/book/9780230369320.

práctica esto implica que no puedan utilizarse fórmulas de consentimiento tácito para el tratamiento de datos.

Asimismo, se requiere del consentimiento explícito en algunos casos, por ejemplo, para el tratamiento de datos sensibles. Supone un requisito más estricto, en el tanto al requerirse el consentimiento de forma expresa para estos supuestos, no puede entenderse como concebido de forma implícita mediante una acción positiva del titular de los datos. Para tratar estos datos se requiere de una declaración expresa o manifestación inequívoca que se refieran explícitamente al consentimiento y el tratamiento de datos comprendidos en las categorías especiales de datos personales.

De igual forma, incorpora una serie de reglas especiales en aquellos casos en los que se otorgue el consentimiento para el tratamiento de los datos por parte de un menor de edad.

De ahora en adelante, el encargado o responsable del tratamiento de los datos personales está en la obligación, en virtud del principio de responsabilidad proactiva que incorpora el RGPD, de estar en la capacidad de demostrar que el interesado otorgó su consentimiento para el tratamiento de los datos de carácter personal. Esto supone una obligación del encargado o responsable del tratamiento de llevar los registros y la documentación necesarios que permitan verificar esta obligación ante cualquier evento.

Se incorporan una serie de obligaciones que señalan la información que debe facilitar el encargado o el responsable del tratamiento de los datos en el momento en que obtenga el consentimiento del interesado, como por ejemplo, la información de la recogida o utilización de los datos personales, el tratamiento que recibirán, las categorías de destinatarios la identidad del responsable del tratamiento o del delgado de protección de datos en aquellos casos que resultase procedente, los plazos de conservación de los datos, la existencia de derechos, entre otros.

De acuerdo con el principio de transparencia que incorpora el RGPD, esta información debe ser facilitada de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en especial si van dirigidas a un niño.

En los casos en que la información no sea obtenida directamente del interesado, el responsable o encargado de tratamiento deberá facilitar información, por mencionar alguna, relativa a la identidad y contacto del responsable del tratamiento o del delegado

de protección de datos si resultara procedente, los fines y el tratamiento que recibirán los datos, la existencia de una intención de transferirlos a un tercer país y organización internacional, entre otros.

Adicionalmente, el RGPD incluye un principio de minimización de datos, el cual implica que adicional a la pertinencia y la adecuación de los datos, el tratamiento debe limitarse a los datos necesarios para los fines para los cuales son recabados.

Los datos, según el RGPD, en todo momento deben ser exactos y si resultara necesario, actualizados. Deben adoptarse todas las medidas necesarias y razonables para suprimir o rectificar sin dilación los datos personales que sean inexactos según los fines para los cuales son tratados.

Se exige a los responsables o encargados del tratamiento, la utilización de un lenguaje claro y comprensible en las cláusulas de privacidad. Esto resulta especialmente relevante y pertinente en situaciones donde, tal y como lo reconoce el RGPD, la proliferación de agentes y la complejidad tecnológica, hagan en la práctica que sea difícil para el interesado saber y comprender si se están recogiendo datos, quién es el encargado o responsable de tratarlos y con qué fin serán usados.

El RGPD recoge una serie de derechos como el derecho al olvido y el derecho a la portabilidad de datos. El primero de ellos deriva de la facultad que tienen todas las personas de solicitar y obtener de los responsables o encargados del tratamiento, que los datos personales sean suprimidos cuando, entre otras razones, estos ya no sean necesarios para la finalidad con la que fueron recogidos, cuando se haya retirado el consentimiento o se hayan recogido de forma ilícita. Este derecho ya había sido reconocido por la STJUE de 13 de mayo de 2014, caso Google, en donde indicó que una persona tiene el derecho a solicitar que se bloqueen en las listas de resultados de los buscadores, los vínculos que conduzcan a informaciones que le afecten y resulten obsoletas, incompletas, falsas, irrelevantes, que no sean de interés público, entre otros.

Por su parte, el derecho a la portabilidad implica que el interesado que haya proporcionado sus datos a un responsable o encargado de tratamiento, puede solicitar recuperar tales datos en un formato que le permita su traslado a otro responsable. Si fuera técnicamente posible, el responsable o encargado del tratamiento deberá transferir los datos en forma directa al nuevo responsable designado por el interesado.

Con el fin de garantizar la protección de los datos personales, el RGPD contiene además una serie de disposiciones dirigidas a cumplir con las exigencias de la nueva normativa en materia de seguridad y protección de la información. Entre ellas, destacan medidas como por ejemplo, las de protección de datos por defecto y *by design*, mantenimiento de registros de tratamiento, realización de evaluaciones de impacto, disposiciones relativas a notificación en caso de que existan violaciones de seguridad de los datos personales, así como códigos de conducta y certificaciones, entre otras.

3. Principales cambios

A. Reconocimiento expreso del principio de transparencia y el principio de minimización

El artículo 5.1.a) del RGPD, relativo a los principios del tratamiento de los datos, incluye el principio de transparencia, el cual dispone expresamente que "los datos personales serán tratados de manera lícita leal y transparencia en relación con el interesado ("licitud, lealtad y transparencia")".

Según el considerando 39 del RGPD, este principio de transparencia supone que se le facilite al ciudadano información sobre el tratamiento de sus datos de carácter personal, de una manera que resulte accesible y fácil de entender, por medio del uso de un lenguaje sencillo y claro. En particular, la información debe versar sobre la identidad del responsable del tratamiento y los fines, así como a la información para garantizar un tratamiento leal y transparente respecto de las personas físicas afectadas y su derecho a obtener confirmación y comunicación sobre sus datos personales que están siendo objeto de tratamiento. Como menciona HERNÁNDEZ CORCHETE, esto demuestra la plena conciencia del legislador europeo "de en un entorno tecnológico complejo el mero cumplimiento por el responsable de los indicados deberes no garantiza de un modo efectivo que el interesado sea consciente de la lógica a que obedece el tratamiento de sus datos personales, de modo que crece su percepción de no tener un poder efectivo de disposición sobre ellos, lo que es particularmente grave porque amplios e importantes ámbitos de su actuar se materializan a través de cauces en los que quedan registrados su datos personales"[113], apreciación también recogida en el considerando 58 del RGPD.

[113] Hernández Corchete, J.A. (2016). Transparencia en la información al interesado del tratamiento de sus datos personales y en el ejercicio de sus derechos. En Piñar Mañas, J.L. (Dir.) *Reglamento General de Protección de Datos: hacia un nuevo modelo europeo de privacidad*. Madrid: Editorial Reus. pp. 205-226.

Asimismo, el artículo 12 del RGPD dentro de los derechos del interesado, recoge la obligatoriedad del responsable del tratamiento de tomar las medidas necesarias para facilitar al interesado toda la información sobre sus datos, así como la relativa a los derechos de acceso, rectificación y supresión, limitación del tratamiento, derecho a la portabilidad y derecho a la oposición, todos ellos contenidos en los artículos 15 al 22 del RGPD.

Toda esa información, debe facilitarse ya sea por medios escritos u otros medios, incluidos los electrónicos, de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje que resulte claro y sencillo. Cuando la información se dirija a un niño, se resalta esta exigencia.

Por su parte, el principio de minimización aparece reconocido en el artículo 5.1.c) del RGPD, el cual menciona que los datos serán "adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados (minimización de datos)". Esto supone no solo que los datos sean tratados en función de su vinculación con ese elemento de necesidad, sino que únicamente deben tratarse si la finalidad del tratamiento no puede conseguirse de forma razonable por otros medios.

B. Exigencias sobre el consentimiento informado

El artículo 4.11 del RGPD define el consentimiento informado como "toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen*"*. Como se verá más adelante, el propio RGPD aclara en su parte considerativa que la expresión *"inequívoca"* comprende cualquier declaración u acción positiva, mientras que las omisiones o los silencios no constituyen consentimiento informado en el sentido de este artículo. La inclusión de la expresión inequívoca en el RGPD ha sido catalogada como una de las modificaciones más importantes en este sentido[114], en el tanto refuerza el carácter fundamental del consentimiento como presupuesto –salvo excepciones- para el tratamiento de los datos.

Por su parte, el artículo 7 del RGPD señala las condiciones para el consentimiento e indica que el responsable debe ser capaz de demostrar que el titular de los datos consintió

[114] Asduara Varela, B. (2016). El consentimiento. En J.L. Piñar Mañas (Dir.), *Reglamento General de Protección de Datos: hacia un nuevo modelo europeo de privacidad*. Madrid: Editorial Reus. pp. 151-167.

el tratamiento. En caso de que el consentimiento haya sido en una declaración escrita que se refiera también a otros asuntos, este debe distinguirse de los demás aspectos de la declaración. En todo momento el interesado tiene derecho a retirar su consentimiento informado, sin que esto afecte la licitud del tratamiento basado en el consentimiento previo a que el interesado lo retirara. Resulta interesante que el RGPD dispone textualmente que el consentimiento será tan fácil retirarlo como darlo, reforzando así su objetivo general de que los ciudadanos retomen un control sobre sus datos personales.

Sobre este particular se refiere el considerando 32 del RGPD, el cual señala que el consentimiento debe darse mediante un acto afirmativo que deje clara esa voluntad libre, específica, informada e inequívoca de la persona de aceptar el tratamiento de sus datos de carácter personal. Esta manifestación de voluntad clara e inequívoca puede lograrse mediante una declaración por escrito, por medios electrónicos, una declaración verbal, marcar una casilla en un sitio web o cualquier otra conducta que indique de forma indubitable que el interesado aceptó el tratamiento de sus datos. Por el contrario, el silencio, casillas ya marcadas o la inacción, no constituyen una aceptación del tratamiento ni deben constituir, en ese sentido, consentimiento. Señala el considerando que en supuestos de un tratamiento para varios fines, el consentimiento debe darse para cada uno de ellos.

Los considerandos 42 y 43 incluyen también aclaraciones sobre el otorgamiento del consentimiento informado y señalan que el responsable del tratamiento debe estar en la capacidad de demostrar el consentimiento del titular de los datos. Igualmente, mencionan que la garantía de un consentimiento otorgado libremente implica que este no constituya un fundamento jurídico válido para el tratamiento de los datos en donde exista un desequilibrio entre el titular y el responsable. Ejemplo de lo anterior es la dependencia de la prestación de un servicio a que se otorgue el consentimiento informado para el tratamiento de los datos, aun y cuando los mismos no sean necesarios para la prestación del servicio.

C. El principio de responsabilidad proactiva

El artículo 5.2 del RGPD, incorpora uno de los aspectos centrales del RGPD que deriva de la exigencia directa de este texto normativo a cualquier persona que realice un

tratamiento de datos personales –salvo excepciones-[115]: el llamado principio de responsabilidad activa, por medio del cual se le obliga al responsable del tratamiento de los datos, no solo el cumplimiento de los principios relativos al tratamiento de estos, sino también se le exige que esté en la capacidad de demostrar que cumple con ellos y la normativa en materia de protección de datos de carácter personal.

Es decir, que más que una posición reactiva frente al cuestionamiento del cumplimiento de la normativa, el responsable o encargado del tratamiento debe ser proactivo y demostrar en todo momento su cumplimiento. Inclusive, autores como CAVOUKIAN, quienes señalan una relación directa de este principio con el de *privacy by design*, en aquellos casos en que no esté claro la necesidad o el uso de la información relativa a una persona, debe aplicarse un principio precautorio y presumirse la privacidad de la información, lo que implica que se debe adoptar la posición que resguarde mayormente la privacidad de los datos.[116]

D. Seudonimización de los datos de carácter personal

El RGPD incluye como garantía de la protección de datos de carácter personal y respuesta a la observación hecha por el Supervisor Europeo de Protección de Datos (SEPD) en la Opinión 3/2015 "*EDPS recommendations on the EU's options for data protection reform*"[117], una clara definición sobre seudonimización de los datos. Este concepto de seudonimización se traduce, según el artículo 4.5 del RGPD, en "el tratamiento de datos personales de manera tal que ya no pueden 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".

Según el considerando 28 del RGPD, la seudonimización de los datos puede representar una medida que ayude a reducir los riesgos para los interesados y, a su vez, coadyuva a las obligaciones de los responsables del tratamiento de los datos en el cumplimiento de sus obligaciones. Esta medida tiene un carácter complementario a las

[115] Buttarelli, G. (2016). The EU GDPR as a clarion call for a new global digital gold standard. *International Data Privacy Law*, 2016, Vol. 6, núm. 2. pp. 77-78.
[116] Cavoukian, A. (2010). *Implementation and mapping of fair information practices.* Recuperado de: https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-implement-7found-principles.pdf
[117] SEPD (2015). Opinion 3/2015: Europe's big opportunity. EDPS recommendations on the EU's options for data protection reform. Recuperado de: https://edps.europa.eu/

demás medidas de protección de datos personales a las que se puede encontrar obligado el responsable del tratamiento de datos.

E. Consentimiento informado en caso de menores

Con la incidencia de las nuevas tecnologías y el Internet en casi todos los espacios de la vida cotidiana, el espacio vital de los menores se ha visto modificado y como menciona PEREZ LUÑO, ha pasado de estar definido por un espacio físico reducido como su colegio o casa, a estar delimitado por las redes que a su vez le abre las puertas a un mundo de posibilidades y conocimientos pero también de riesgos. Esta nueva dimensión y tutela del menor ha hecho que deban considerarse en el ámbito de la protección de datos, una serie de reglas aplicables, las cuales en el RGPD quedan de manifiesto por medio de exigencias específicas cuando el consentimiento sea exigido a un menor, como una medida dentro de un balance delicado en el que debe buscarse su protección pero no puede limitarse su libertad ni autonomía.[118]

Aunado a lo anterior, debe sumarse a la consideración que "la red es un entorno idóneo para que los menores se encuentren expuestos al uso de su información personal, debido a que sus datos personales son muy apreciados en la utilización de fines comerciales y en el ámbito del ocio, aunque también con otro tipo de fines".[119]

Frente a este panorama, resultaba necesaria la adopción de normas en el ámbito de la protección de datos que protegieran a esta "categoría de afectados que requieren una mayor protección" [120] y que se veía "sometido a un especial riesgo en el mundo *online* a causa de su masivo acceso a Internet y de la obtusidad de sus reglas y políticas de privacidad".[121]Ya en ese sentido, el WP 29[122] en su Documento 1/2008 de 18 de febrero,

[118] Pérez Luño, A.E. (2009). La protección de los datos personales del menor en Internet. *Anuario Facultad de Derecho, Universidad de Alcalá*, 2009. pp. 143-175.
[119] Fernández Pérez, A. (2016). La protección de los derechos fundamentales de los menores en internet desde la perspectiva europea. *Revista Ius et Praxis*, Año 22, núm. 1, 2016. pp. 377-416.
[120] Gil Antón, A.M. (2013). El derecho a la propia imagen del menor en internet. Madrid: Dykinson. p. 145.
[121] Rallo Lombarte, A. (2012). Hacia un nuevo sistema europeo de protección de datos… *op. cit.* pp. 13-56.
[122] El WP 29 o Grupo de Trabajo del Artículo 29, es, según lo indica la AEPD "un órgano consultivo independiente [creado por la Directiva 95/46] integrado por las Autoridades de Protección de Datos de todos los Estados miembros, el Supervisor Europeo de Protección de Datos y la Comisión Europea- que realiza funciones de Secretariado (...) Las funciones del GT29 reconocidas por la Directiva incluyen estudiar toda cuestión relativa a la aplicación de las disposiciones nacionales tomadas para la aplicación de la Directiva, emitir dictámenes sobre el nivel de protección existente dentro de la Comunidad y en países terceros, asesorar a la Comisión sobre cualquier proyecto de modificación de la Directiva, y formular recomendaciones sobre cualquier asunto relacionado con la protección de datos en la Unión Europea. El GT29 se pronuncia a través de Dictámenes, Documentos de Trabajo, Informes o Recomendaciones, aunque también manifiesta su posición en cartas o comunicados de prensa. Las decisiones del Grupo no son

sobre la protección de datos de los menores, había indicado que en su condición de persona tiene el derecho a gozar de la protección de todos los derechos, incluido el derecho a la protección sus datos de carácter personal[123], consideración a la que debe añadirse que durante su desarrollo integral "en tanto sujeto en tránsito hacia la plena madurez"[124], el ordenamiento debe protegerle especialmente.

En ese sentido, el artículo 8 del RGPD establece una serie de consideraciones que deben aplicarse cuando el consentimiento deba ser otorgado por menores, partiendo de la ya explicada necesidad de proteger de forma específica a este grupo de la población[125] que también está inmerso y participa de las nuevas tecnologías pero que pueden llegar a ser menos conscientes de los riesgos y las consecuencias, así como de las garantías y los derechos que le asisten en relación con el tratamiento de sus datos personales

La norma establece un mínimo de 16 años como requisito para entender que un tratamiento de datos de personas menores de edad es lícito, además de que la información sobre el tratamiento de los datos y relativa al consentimiento le sea transmitida de forma clara e inteligible. En los casos donde la edad del menor sea inferior a los 16 años, solo se entenderá como lícito el tratamiento de sus datos cuando haya sido otorgado o autorizado por quien ejerza la patria potestad o tutela sobre el menor y, únicamente, se podrá realizar el tratamiento en la medida y para los efectos en que fue consentido.

No obstante, se concede un margen de aplicación de la norma a los Estados miembros y permite que se fije una edad inferior a los 16 años para prestar el consentimiento por menores de edad, pero no puede ser, bajo ningún supuesto, inferior a los 13 años. Contiene también una cláusula de salvaguarda en el sentido de que los preceptos no afectaran las

jurídicamente vinculantes, pero tienen un importante valor doctrinal y son frecuentemente utilizados y citados por los legisladores y los tribunales nacionales y europeos". Recuperado de: http://www.agpd.es/portalwebAGPD/internacional/Europa/grupo_29_europeo/index-ides-idphp.php

[123] Textualmente dispone: "A child is a human being in the complete sense of the word. For this reason, a child must enjoy all the rights of a person, including the right to the protection of their personal data".

[124] Gil Antón, A.M. (2015). El menor y la tutela de su entorno virtual a la luz de la reforma del Código Penal LO 1/2015. *Revista de Derecho UNED*, núm. 16. pp. 275-319.

[125] Si bien en el RGPD se hace alusión concreta al tratamiento de datos de personas menores de edad, hay autores como GOMEZ-JUÁREZ SIDERA, para quien debe hablarse de personas especialmente vulnerables, lo que incluye no sólo niños sino también a personas mayores, que por la brecha que tienen con la tecnología, son particularmente propensos a situaciones de riesgo en lo que se refiere al tratamiento de sus datos de carácter personal. Ver en: Gómez-Juárez Sidera, I. ((2015). Hacia un nuevo derecho de protección de datos para las personas especialmente vulnerables en la sociedad digital del Siglo XXI: los niños y las personas mayores. *Revista CESCO de Derecho de Consumo*, núm. 14/2015. pp. 217-240.

disposiciones generales del Derecho contractual de los Estados miembros, en relación con las normas sobre validez, formación o efectos de los contratos con menores de edad.

Adicional a esta referencia expresa en el artículo 8, existen otros artículos que hacen referencia al tratamiento especial de datos sobre menores, por ejemplo, el artículo 6.1.f), 12.1, 40.2.g), y 57.1.b), relativas a la licitud del tratamiento, la obligación de transmitir la información relativa al tratamiento de forma clara, concisa, transparente e inteligible por medio de un lenguaje claro y sencillo, entre otras[126].

F. Categorías especiales de protección de datos

(STJUE de 11 de diciembre de 2014, asunto C-212/13 (caso Rynes) sobre tratamiento de imágenes grabadas por sistemas de videovigilancia y STJUE de 17 de octubre de 2013, asunto C-291/12, caso Schwartz sobre la toma de impresiones dactilares)

El artículo 9 del RGPD añade a las categorías especiales de datos ya existentes (origen étnico o racial, opiniones políticas, convicciones religiosas o filosóficas, o la afiliación sindical, datos relativos a la salud, la vida sexual y sobre la orientación sexual), los datos de carácter genéticos y los biométricos, quedando prohibido su tratamiento salvo las excepciones que señal el artículo 9.1 del RGPD[127].

Según las definiciones contenidas en el artículo 4.13 y 14 respectivamente, los datos genéticos son aquellos "datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una

[126] En este sentido, ver: Piñar Mañas, A. (2016). Tratamiento de datos de menores de edad. En J.L. Piñar Mañas (Dir.), *Reglamento General de Protección de Datos: hacia un nuevo modelo europeo de privacidad*. Madrid: Editorial Reus. pp. 187-203.

[127] Si bien estos datos no aparecían menciondos de forma expresa, la doctrina los incluía dentro del concepto amplio de datos de salud por lo que gozaban de una protección reforzada. No obstante lo anterior, coincidimos con la profesora GÓMEZ SÁNCHEZ, quien de forma acertada enfatiza sobre el necesario reconocimiento como un dato especialmente protegido por sí solo y no únicamente por su vínculo con los datos de salud. Sobre este particular menciona: "La doctrina no viene objetando sobre la pertenencia de los datos de salud a la categoría de datos sensibles y, en mi opinión, tampoco cabe objetar nada respecto de la pertenencia de los datos genéticos a dicha categoría, pero no porque todos los datos genéticos deban ser considerados datos de salud –y, por ello, datos sensibles- o deban asimilarse a aquéllos- tesis que se mantiene actualmente y aparece recogida en diversos documentos- sino porque todo dato genético es, por la naturaleza de la información que revela o pudiera revelar, un dato merecedor de una protección reforzada, aunque sus diferentes aplicaciones pudieran modular su regulación". En extenso puede verse en: Gómez Sánchez, Y. (2008). La protección de los datos genéticos: el derecho a la autodeterminación informativa. *DS: Derecho y salud*, núm. 16. pp.59-78.

muestra biológica de tal persona"; mientras que los datos biométricos[128] son "datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos".

Tanto las huellas dactilares como las imágenes –ambos comprendidos dentro del concepto de "dato biométrico-, habían sido reconocidas como datos de carácter personal en la STJUE del caso Schwartz y la STJUE del caso Rynes respectivamente, actuando una vez más el RGPD como mecanismo de positivización de la jurisprudencia del TJUE.

G. Reconocimiento de derechos del interesado

a) Derecho de supresión (derecho al olvido)

(STJUE de 13 de mayo de 2014, asunto C-131/12, caso Google)

Una de las principales novedades del RGPD –"en un mundo en el que cada quien es lo que Google dice que es"[129]- es la positivización en una norma de la UE del derecho de supresión o *"derecho al olvido"*, tema que ha sido tratado ampliamente por la doctrina[130]. Este derecho ya había sido reconocido en la STJUE de 13 de mayo, caso

[128] Una definición más amplia de dato biométrico se encuentra en las opiniones del WP 29, por ejemplo en la Opinión 3/2012 de 27 de abril, sobre desarrollo de las tecnologías biométricas, en la que define el dato biométrico como "biological properties, behavioral aspects, physiological characteristics, living traits or repeatable actions where those features and/or actions are both unique to that individual and measurable, even if the patterns used in practice to technically measure them involve a certain degree of probability' Biometric data changes irrevocable the relation between body and identity because they make the c characteristics of the human body 'machine-readable' and subject to further use. Biometric data can be stored and processed in different forms. Sometimes the biometric information captured from a person is stored and processed in a raw form that allows recognizing the source it comes from without special knowledge e.g. the photograph of a face, the photograph of a finger print or a voice recording. Some other times, the captured raw biometric information is processed in a way that only certain characteristics and/or features are extracted and saved as a biometric template". Ver en: WP 29 (2012). Opinion 3/2012 on developments in biometric technologies. Recuperado de: ec.europa.eu/justice/data-protection/.../opinion.../wp193_en.pdf.

[129] Korenhonf et al (2015) Timing the right to be forgotten, a study into "time" as a factor in deciding about retention or erasure of data. En S. Gutwirth, R. Leenes y P. de Hert (Eds.) *Reforming European Data Protection Law. Law, Governance and Technology Series (20)*. Bruselas: Springer. pp.171-201.

[130] Entre otros, puede verse: Cobas Cobiella, M.E. (2017). Derecho al olvido: de la STJUE de 2014 al Reglamento europeo de Protección de Datos. *Actualidad civil*, núm. 1, 2017. pp. 98-116; Berrocal Lanzarot, A.I. (2017). El derecho de supresión de datos o derecho al olvido en el Reglamento General de Protección de Datos. *Revista general de legislación y jurisprudencia, núm.* 1, 2017. pp. 7-71; Chéliz Inglés, M.C. (2016). El "derecho al olvido digital". Una exigencia de las nuevas tecnologías recogida en el futuro Reglamento General de Protección de Datos. *Actualidad Jurídica Iberoamericana*, núm. 5, agosto 2016. pp.255-271; Martínez Otero, J.M. (2015). El derecho al olvido en Internet: debates cerrados y cuestiones abiertas tras la STJUE Google vs AEPD y Mario Costeja. *Revista de Derecho Político, núm.* 93, mayo-agosto 2015. pp. 103-142; Pazos Castro R. (2015). El funcionamiento de los motores de búsqueda en Internet y la política de protección de datos personales, ¿una relación imposible? Recuperado de:

Google, en la que el TJUE declaró que un interesado puede solicitar que se bloqueen en las listas de resultados de los buscadores, los vínculos que conduzcan a informaciones que le conciernen y que resulten obsoletas, incompletas, falsas o irrelevantes y no sean de interés público, entre otros motivos.

Por su parte, el RGPD, el considerando 65 señala que los interesados deben tener el derecho de rectificar los datos que les conciernen y se supriman si la retención de estos infringen las normas comunitarias o la legislación de los Estados miembros aplicable al responsable del tratamiento de los datos.

Seguidamente, el artículo 17 del RGPD dispone textualmente que el interesado tiene derecho a obtener, sin dilación alguna, la supresión de sus datos personales. En estos casos, el responsable del tratamiento está obligado a suprimir los datos cuando ocurran las circunstancias mencionadas en dicho artículo, por ejemplo, en aquellos casos en que los datos ya no sean necesarios en relación con los fines para los cuales fueron recogidos, se retire el consentimiento en que se basa el tratamiento, los datos hayan sido tratados de forma ilícita, el interesado se oponga al tratamiento, entre otros. Cuando hubiera hecho públicos tales datos, el responsable está en la obligación de indicar a quienes los estén tratando, que suprima todo enlace, copia o réplica de tales datos.

Básicamente, el "Reglamento reconoce un derecho de los interesados a que sus datos sean suprimidos por el responsable del tratamiento en determinadas circunstancias y salvo que se den otros supuestos contemplados en el ámbito de las excepciones de este derecho. Asimismo, se recoge una obligación de informar a otros responsables del tratamiento que estén tratando los datos, con el fin de que tomen medidas y supriman toda réplica, copia o enlace a los mismos."[131]

---

http://www.indret.com/pdf/1118_es.pdf ; Azurmendi, A. (2015). Por un "derecho al olvido" para los europeos: aportaciones jurisprudenciales de la sentencia del Tribunal de Justicia europeo del caso Google Spain y su recepción por la sentencia de la audiencia nacional española de 29 de diciembre de 2014. *Revista de Derecho Político*, núm. 92, enero-abril 2015. pp. 273-310; López Portas, B. (2015). La configuración del derecho al olvido en el Derecho español al tenor de la doctrina del TJUE. *Revista de Derecho Político*, núm. 93, 2015. pp. 143-175; Martínez Caballero, J. Cómo conjugar el derecho al olvido. *Revista Jurídica de Castilla-La Mancha*, núm. 57 – Enero/Diciembre 2015. pp.143-185; Rallo Lombarte, Artemi. (2014). El derecho al olvido en Internet Google versus España. Madrid: Centro de Estudios Políticos y Constitucionales.

[131] Álvarez Caro, M. (2016). El derecho a la supresión o al olvido. En J.L. Piñar Mañas (Dir.), *Reglamento General de Protección de Datos: hacia un nuevo modelo europeo de privacidad*. Madrid: Editorial Reus. pp. 241-256.

No obstante lo anterior, se establecen una serie de limitaciones al derecho al olvido que derivan de su relación con otros derechos y principios reconocidos en el Derecho comunitario o la normativa de los Estados miembro, por ejemplo, cuando se trate del ejercicio del derecho a la libertad de expresión e información, para el cumplimiento de obligaciones legales o en el ejercicio de poderes públicos, por razones de interés público en el ámbito de la salud pública, con fines de archivo en interés público, investigación científica o histórica, fines estadísticos, o bien, formulación, ejercicio o defensa de reclamaciones.

b) Derecho a la limitación del tratamiento

El RGPD confiere al interesado en su artículo 18 una nueva facultad de limitar el tratamiento de los datos personales en los supuestos tasados que menciona: cuando se impugne la exactitud de los mismos, el tratamiento sea ilícito y el interesado se oponga a la supresión de los mismos, el responsable ya no los necesite pero el interesado los requiera para la formulación, ejercicio o defensa de reclamaciones, o bien, que el interesado haya ejercido su derecho de oposición.

Sobre este particular, el considerando 67 del RGPD de manera expresa dispone que, entre los métodos para limitar el tratamiento, cabe incluir los que consistan en trasladar los datos seleccionados a otro sistema de tratamiento, impedir el acceso de los usuarios a los datos seleccionados, o retirar de forma temporal los datos publicados en un sitio web. En el caso de que se trate de ficheros automatizados, el responsable debe adoptar las medidas necesarias para que los datos no sean objeto de operaciones de tratamiento ulterior ni puedan modificarse. En forma adicional, debe indicarse claramente en los sistemas, que el tratamiento de los datos personales está limitado.

c) Derecho a la portabilidad de datos

El artículo 20 del RGPD incorpora al catálogo de derechos del interesado, el derecho a recibir los datos personales que le conciernen y haya facilitado a un responsable de tratamiento, con el fin de transmitirlos a otro responsable. Para efectos de que el interesado pueda recuperar sus datos, con el fin de transmitirlos a un nuevo responsable en el tratamiento, el responsable anterior está en la obligación de facilitarlos al interesado en un formato estructurado, de uso común y lectura mecánica. En palabras del SEPD, BUTTARELLI, "el derecho a la portabilidad de datos debe permitir a empoderar a los

individuos para que elijan a quién quieren confiar su información, así como a cambiar de parecer y mover sus datos a otro proveedor de servicios".[132]

Asimismo, cuando sea técnicamente posible, se encuentra en la obligación de transmitir los datos de forma directa al nuevo responsable del tratamiento. El RGPD entiende que el ejercicio de este derecho puede llevarse a cabo sin perjuicio del derecho de supresión que le asiste al interesado. En todo caso, no podrá el derecho a la portabilidad afectar de forma negativa los derechos y libertades de otros, y no aplica cuando se esté ante la aplicación de una medida necesaria para el cumplimiento del interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. Según señala el considerando 68 del RGPD, debe alentarse a los responsables del tratamiento de los datos a crear formatos interoperables que permitan su portabilidad. Esto implica que en la medida posible deben si bien no usar formatos compatibles, si al menos en formatos estructurados y de uso común que permitan la portabilidad de los datos de un responsable a otro.

Para autores como RALLO LOMBARTE, este derecho tiene como origen poder dar una respuesta a los servicios que prestan las redes sociales y permitir que los usuarios de estas puedan en cualquier momento cancelar sus cuentas en una red determinada y pueda trasladar toda su actividad e historial generado a una nueva red social. Indica que "de la trascendencia de este nuevo derecho da buena cuenta una realidad en la que miles de millones de usuarios de redes sociales acumulan sus cuentas on line un auténtico historial de vivencias y relaciones personales y sociales que resultaría abortado si se les negara tal derecho a la portabilidad o generaría un insufrible sometimiento del usuario a los designios de la red social de acogida que resultaría difícilmente conciliable con los estándares básicos de protección de datos y su misma dignidad".[133]

H. Decisiones individuales automatizadas y elaboración de perfiles

Según el artículo 22 del RGPD, todo interesado tiene derecho a no ser objeto de una decisión que se base únicamente en el tratamiento automatizado de datos, lo cual incluye la elaboración de perfiles que produzcan efectos jurídicos o le afecten de forma sustancial. Este derecho no aplica cuando la decisión automatizada sea necesaria para la celebración

[132] Buttarelli, G. (2016) One giant leap for digital rights. Recuperado de: https://edps.europa.eu/press-publications/press-news/blog/one-giant-leap-digital-rights_fr

[133] Rallo Lombarte, A. (2012). Hacia un nuevo sistema europeo de protección de datos… *op. cit.* pp. 13-56.

y ejecución de un contrato, esté autorizada por el Derecho de la Unión o de los Estados miembros, o bien, el interesado haya dado expresamente su consentimiento

I. Responsabilidad del responsable del tratamiento de datos y *privacy by design*

El artículo 24 del RGPD establece una serie de obligaciones aplicables al responsable del tratamiento de los datos personales. Bajo el entendido de este artículo, el responsable del tratamiento está obligado a adoptar las medidas técnicas y organizativas con el fin de proteger los datos. Para el cumplimiento de lo anterior, siempre debe tener en cuenta para estos efectos la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos y la gravedad para los derechos y las libertades de los interesados. Entre estas medidas se encuentra la aplicación por parte del responsable de las políticas de protección de datos.

Esto como indica LÓPEZ ÁLVAREZ resulta trascendental en el nuevo paradigma de la protección de datos que cobija el RGPD pues implica la transición del simple cumplimiento de la normativa de forma reactiva por parte de los responsables y encargados de tratamiento de los datos personales, a un sistema en que se exige que estas personas demuestren efectivamente la diligencia en la adopción de medidas tendientes al cumplimiento de las obligaciones dispuestas en la nueva regulación[134].

Las medidas que se adopten deberán ser revisadas y actualizadas cuando así resulte necesario. La adhesión a códigos de conducta o a mecanismos de certificación aprobados, constituyen elementos demostrativos del cumplimiento de las obligaciones por parte del responsable según indica explícitamente el RGPD.

Por su parte, el artículo 25 del RGPD establece la protección de datos desde el diseño y por defecto, que como bien lo menciona DUASO CALDÉS, "encarnan un modelo de protección de la privacidad que en el futuro deberá estar basado en un modo de operar por defecto de toda organización"[135] y cita a CAVOUKIAN, para quien el aseguramiento de

[134] López Álvarez, L.F. (2016). La responsabilidad del responsable. En J.L. Piñar Mañas (Dir.), *Reglamento General de Protección de Datos: hacia un nuevo modelo europeo de privacidad*. Madrid: Editorial Reus. pp. 275-293.
[135] Duaso Caldés, R. (2016). Los principios de protección de datos desde el diseño y protección de datos por defecto. En J.L. Piñar Mañas (Dir.), *Reglamento General de Protección de Datos: hacia un nuevo modelo europeo de privacidad*. Madrid: Editorial Reus. pp. 295-320.

la protección de la privacidad, debe convertirse por *default* en el modelo de operación de toda persona que trate datos de carácter personal.[136]

En ese sentido, el RGPD dispone que teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como sus riesgos y gravedad, el responsable del tratamiento aplicará en todo momento las medidas técnicas y organizativas apropiadas, como por ejemplo, la seudonimización y la minimización de datos, así como integrar las garantías necesarias en el tratamiento para cumplir tanto con lo dispuesto en el RGPD y proteger los derecho de las personas. Asimismo, las medidas deberán aplicarse para garantizar que, por defecto, solo sean objeto de tratamiento los datos necesarios para los fines del tratamiento, así como que los datos no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas.

Sobre este particular, el considerando 68 del RGPD cita que entre las medidas para cumplir con los principios de protección de datos desde el diseño y por defecto, además de las mencionadas de seudonimización y minimización, se encuentra el dar transparencia a las funciones y tratamiento de datos, lo cual permite a los interesados supervisar su tratamiento y al responsable crear y mejorar elementos de seguridad.

J. Notificación de una violación de seguridad a la autoridad de control

El RGPD en su artículo 33 establece que el responsable del tratamiento de los datos está obligado a informar a las autoridades de control, la violación de la seguridad de los datos personales. Esta comunicación debe ser en un plazo que no exceda las 72 horas después de que se haya tenido constancia de la violación a la seguridad, salvo que en atención al principio de responsabilidad proactiva, se determine que la violación no constituya un riesgo para los derechos y las libertades de las personas. En caso de que se exceda el plazo de 72 horas, el encargado deberá justificar la condición que originó el retraso, por ejemplo, que se estaban adoptando las medidas adecuadas para impedir violaciones continuas o similares a la seguridad de los datos.

La notificación según el artículo 3.3 del RGPD debe incluir como mínimo la descripción de la naturaleza de la violación, el nombre y los datos del delegado de protección de datos o el punto de contacto, así como describir las posibles consecuencias,

[136]Cavoukian, A. (2009). Privacy by desing. Recuperado de: https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf

indicar las medidas adoptadas para remediar la violación de la seguridad y las medias para mitigar los posibles efectos negativos, y, facilitar la información de forma simultánea o de forma gradual sin dilación indebida.

Adicionalmente, el artículo 34 del RGPD impone junto con esta obligación, la exigencia de comunicar al interesado, en un lenguaje claro y sencillo de una violación a la seguridad de los datos que entrañe un riesgo para los derechos y las libertades de las personas físicas. Este comunicado debe realizarlo sin demora indebida y deberá describir la naturaleza de la violación de la seguridad y la información y medidas adaptadas para remediar la situación y mitigar los posibles efectos negativos.

No obstante lo anterior, la comunicación no será necesaria cuando el responsable del tratamiento haya adoptado las medidas de protección técnicas y organizativas y también se hayan aplicado a los datos personales afectados por la violación de la seguridad, se hayan tomado medidas que garanticen que no existe la probabilidad de que se concretice un alto riesgo para los derechos y libertades del interesado, o bien cuando suponga un esfuerzo desproporcionado, en cuyo caso se optará por una comunicación pública o medida similar para informar a los interesados.

Sobre este particular, el considerando 86 del RGPD indica que las comunicaciones en la medida en que sea razonablemente posible, deben hacerse en cooperación con la autoridad de control, siguiendo tanto sus indicaciones como las de otras autoridades competentes, por ejemplo, las policiales.

K. Evaluación de impacto y comunicación a interesados

El RGPD señala que cuando un tratamiento de datos, en razón de su alcance, contexto o fines, conlleve un potencial alto riesgo para los derechos y las libertades de las personas físicas, de conformidad con el artículo 35 del RGPD, el responsable deberá realizar una evaluación de impacto de las operaciones del tratamiento, que tiene por función no sólo asegurar la protección de los datos personales, sino que también, como lo indican HEMPEL Y LAMMERANT[137], aportar algo de racionalidad al proceso de toma de decisiones en lo que a ello se refiere.

[137] Hempel, L.; Lammerant, H. (2015). En S. Gutwirth, R. Leenes y P. de Hert (Eds.) *Reforming European Data Protection Law. Law, Governance and Technology Series (20)*. Bruselas: Springer. pp. 125-145.

Según señala el considerando 84 del RGPD, el resultado de la evaluación de impacto deberá ser tomada en cuenta para la adopción de las medidas adecuadas, con el fin de cumplir con lo dispuesto en el RGPD. En los casos donde se determine que el tratamiento entraña un alto riesgo que el responsable no puede mitigar con medidas adecuadas en términos de tecnología y costes de aplicación, debe consultarse previo a la realización del tratamiento a la autoridad de control competente.

Este proceso consultivo se recoge en el artículo 36 del RGPD. En los casos en que se lleve a cabo la consulta mencionada en el artículo 35 del RGPD y no se haya identificado o mitigado el riesgo por parte del responsable del tratamiento, la autoridad de control debe, en un plazo de 8 semanas después de recibida la consulta, dar asesoría por escrito al responsable.

L. Delegado de protección de datos

En su artículo 37 el RGPD crea la figura del delegado de protección de datos, para los casos en que el tratamiento lo lleve cabo una autoridad u organismos públicos, con excepción de los tribunales que actúen en ejercicio de su función judicial, cuando el tratamiento de datos, en virtud de su naturaleza, alcance los fines requiera de una observación habitual y sistemática de datos de interesados a gran escala, o, las actividades consistan en el tratamiento de categorías especiales de datos y datos relativos a condenas e infracciones penales. Como bien lo indica la AEPD, este constituye uno de los elementos claves del Reglamento y es un garante a su vez de la normativa de protección de datos sin que ello llegue a suponer un relevo en las funciones encomendadas a las autoridades independientes de control[138].

Es obligación del responsable y el encargado del tratamiento de datos procurar que el delegado participe de forma adecuada y oportuna en todos aquellos aspectos relacionados con la protección de datos personales. Además, deberán facilitar los recursos necesarios para el desempeño de las labores, así como acceso a los datos personales y las operaciones de tratamiento. Adicionalmente, el artículo 39 garantiza al delegado no recibir instrucciones en el desempeño de sus funciones y únicamente rendir cuentas al más alto nivel jerárquico del responsable o encargado del tratamiento.

[138] AEPD (2017). Qué es un delegado de protección de datos. Recuperado de: http://www.agpd.es/blog/que-es-un-delegado-de-proteccion-de-datos-ides-idPhp.php

Dentro de las funciones del delegado se encuentran las mencionadas en el artículo 39, las cuales comprenden informar y asesorar al responsable, encargado y empleados que realicen el tratamiento, de sus obligaciones en virtud del RGPD y las disposiciones locales; supervisar el cumplimiento de lo dispuesto en el RGPD; ofrecer asesoramiento sobre la evaluación de impacto relativa a la protección de datos; cooperar con la autoridad de control; y, actuar como punto de contacto de la autoridad de control competente.

M. Disposiciones sobre transferencias internacionales

(STJUE de 6 de octubre de 2015, asunto C-362/14, caso Schrems)

El RGPD introduce un nuevo capítulo de regulaciones a las transferencias de datos personales a terceros países u organizaciones internacionales, que busca que el nivel de protección de datos garantizado por el RGPD no se vea menoscabado ante dichas transferencias. Lo anterior, en consonancia con la doctrina establecida en la STJUE, de 6 de octubre de 2015, caso Schrems y los requisitos necesarios para que la transferencia internacional de datos sea acorde al marco normativo comunitario.

En ese sentido, el artículo 45 del RGPD autoriza la transferencia de datos a un tercer país u organización internacional, cuando la CE haya tomado una decisión favorable sobre la garantía de un nivel adecuado de protección en atención al respeto del tercer país al Estado de Derecho, los derechos humanos y las libertades fundamentales, así como a la legislación en materia de protección de datos, la existencia y el funcionamiento de una o varias autoridades de control independientes, con capacidad de garantizar el cumplimiento de la normativa en materia de protección de datos, los compromisos asumidos por el tercer país a través de acuerdos o instrumentos jurídicamente vinculantes en materia de protección de datos. En particular, señala el considerando 105, debe valorarse la adhesión del país al Convenio 108. La CE se encargará de supervisar los acontecimientos que puedan afectar la decisión y podrá revocarla previo aviso y declaración motivada.

En casos de no existir una decisión por parte de la CE, el responsable o el encargado del tratamiento de datos personales, solo podrá transmitirlos a un tercer país u organización internacional si hubieran ofrecido garantías adecuadas y bajo la condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas. Asimismo señala que las garantías adecuadas pueden ser aportadas por medio de un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos

públicos; normas corporativas vinculantes; cláusulas tipo de protección de datos adoptadas por la CE; clausulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la CE; códigos de conducta; o bien, un mecanismo de certificación aprobado.

N. Sanciones y multas

El RGPD señala que las autoridades de control deben garantizar la imposición de multas administrativas efectivas, proporcionadas y disuasorias, por las infracciones al RGPD, como un mecanismo de reforzamiento de la aplicación de estas normas. Según se explica en el considerando 150 del RGPD, la inclusión de estas disposiciones pretende reforzar y armonizar el régimen de sanciones y multas por infracción a la normativa de protección de datos.

El artículo 83.4 del RGPD indica que tratándose de infracciones relacionadas con las condiciones aplicables al consentimiento del niño (artículo 8), tratamientos que no requieren identificación (artículo 11) y obligaciones del responsable y encargado del tratamiento (artículos 25 a 39), las obligaciones de los organismos de certificación (artículos 42 y 43) y la supervisión de códigos de conducta aprobados (artículo 41), podrá imponerse una multa administrativa de 10.000.00 EUR como máximo, o en el caso de empresas, una multa equivalente a la cuantía del 2% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, siendo que debe optarse en todo momento por la de mayor cuantía.

El apartado 5, del mismo artículo del RGPD, impone una multa administrativa de 20.000.000 EUR o la cuantía equivalente al 4% como máximo del volumen del negocio total anual global del ejercicio financiero anterior, en los casos en donde se cometan infracciones a los principios básicos para el tratamiento de los datos, incluidas las condiciones para el consentimiento (artículos 5, 6, 7 y 9), los derechos de los interesados (artículos 12 a 22), transferencias de datos personales a un destinatario en un tercer país o una organización internacional (artículos 44 a 49), el incumplimiento de una resolución o una limitación temporal o definitiva del tratamiento o la suspensión de los flujos de datos por parte de la autoridad de control, o bien, no facilitar el acceso a una autoridad de control en el ejercicio de sus poderes (artículo 58).

Cuando corresponda imponer alguna de las multas mencionadas a personas físicas, cabe valorar la cuantía de la multa de acuerdo con el nivel general de ingresos

prevaleciente en el Estado miembro, así como la situación económica de la persona, según explica en el considerando 151 del RGPD.

Todo lo anterior sin perjuicio de lo dispuesto en el artículo 84 del RGPD, el cual dispone que los Estados miembros deben establecer otras sanciones distintas a las multas administrativas por infracción al RGPD.

4. Acceso a la información y protección de datos personales a la luz del RGPD

La tensa relación existente entre transparencia, acceso a la información y protección de datos en el marco normativo de la UE no aparece claramente definido en la Directiva 95/46, que únicamente contiene una disposición en el considerando 72 que "autoriza que se tenga en cuenta el principio de acceso público a los documentos oficiales a la hora de aplicar los principios expuestos en la presente Directiva".

Ante esta falta de precisión y de norma expresa, ha sido labor del TJUE buscar el balance entre estos derechos e intereses tutelados por el ordenamiento comunitario, ya sea mediante la interpretación de la relación existente entre los reglamentos comunitarios sobre acceso a los documentos y protección de datos en las instituciones, o bien, mediante la aplicación directa del artículo 8 de la CDFUE como se verá más adelante.

Pese a que en el momento de aprobación del RGPD existía jurisprudencia del TJUE consolidada en esta materia, el RGPD aborda de manera tímida este conflicto de derechos. El Capítulo IX del RGPD sobre disposiciones relativas a situaciones específicas de tratamiento[139], incluye en su artículo 86 una disposición que indica que "los datos personales de documentos oficiales en posesión de alguna autoridad pública u organismo público o una entidad privada para la realización de una misión de interés público podrán ser comunicados por dicha autoridad, organismo o entidad de conformidad con el Derecho de la Unión o de los Estados miembros que se les aplique a f in de conciliar el acceso del público a documentos oficiales con el derecho a la protección de datos

[139] Sobre otras disposiciones especiales, como por ejemplo, la relativa al tratamiento de datos y libertad de expresión e información (art. 85 del RGPD, puede consultarse: Muñoz-Machado-Cañas, J. (2016). Tratamiento de datos y libertad de expresión e información. En J.L. Piñar Mañas (Dir.), *Reglamento General de Protección de Datos: hacia un nuevo modelo europeo de privacidad*. Madrid: Editorial Reus. pp. 587-599. También, puede consultarse: Pauner Chilvi, C. (2015). La libertad de información como límite al derecho a la protección de datos personales: la excepción periodística. *Teoría y Realidad Constitucional*, núm. 36, 2015. pp. 377-395.

personales en virtud del presente Reglamento". En similar sentido se expresa el considerando 154 del Reglamento.

Para RAMS RAMOS, la inclusión de forma expresa de la disposición contenida en el artículo 86 del RGPD, hace que aparezca definido en una norma reglamentaria la posibilidad de acceder documentos públicos que contengan datos personales, la necesaria conciliación de ambos derechos y el reconocimiento del interés público que existe en el acceso a los documentos públicos. De forma que "el Reglamento no sólo establece la posibilidad de comunicación de documentos oficiales que contengan datos de carácter personal, sino también determina que en la necesaria ponderación que se lleve a cabo entre los derechos de acceso y protección de datos debe tenerse en cuenta que el acceso a la información se considera de interés público (y por tanto legítimo). En consecuencia, será lícita la comunicación de datos que obren en documentos públicos-como parte de su tratamiento- a terceros, cuando exista ese interés legítimo, que se presupone por lo anteriormente establecido y que llama a una ponderación directa entre la protección de ambos intereses: de un lado, el del solicitante de acceso en que le sea comunicada la información pública pedida, cuyo interés ya se presupone, y de otro, el de los afectados o titulares de los datos que figuren en la información solicitada, en que se protejan sus derechos y libertades a través de la protección de dichos datos".[140]

En similar sentido, TRONCOSO REIGADA menciona que junto con la previsión del artículo 86 del RGPD debe tenerse en consideración el artículo 6 de ese mismo texto normativo, de forma que se tienen "dos previsiones que justifican los tratamientos de datos personales necesarios para garantizar el derecho de acceso a la información administrativa cuando ésta contenga datos personales, de forma que la trasparencia administrativa suponga un límite al derecho fundamental a la protección de datos de carácter personal: la primera previsión es la relativa a los supuestos de licitud de los tratamientos –art. 6- y la segunda sería la regulación del tratamiento y acceso del público a documentos oficiales –art. 86-".[141] Por tanto, el acceso a la información pública puede

[140] Rams Ramos, L. (2016). Tratamiento y acceso público a documentos oficiales. En J.L. Piñar Mañas (Dir.), *Reglamento General de Protección de Datos: hacia un nuevo modelo europeo de privacidad*. Madrid: Editorial Reus. pp. 601-619.

[141] Troncoso Reigada, A. (2016). Los límites al acceso a la información: la protección de datos personales. *Revista Iberoamericana de Derecho Informático (Segunda Época)*, Fundación Iberoamericana de Asociaciones de Derecho e Informática, Año 1, núm. 1, 2016. pp. 45-53.

configurarse como un límite al derecho a la protección de datos de carácter personal, en el entendido de tales presupuestos.

Si bien hubiese podido incorporar alguna regla o criterio que permitiese la mejor solución en los casos en los que se pretenda el acceso a información que contenga datos de carácter personal, ello no implica que el RGPD no vaya a tener incidencia en el derecho de acceso a la información y la protección de datos personal, la cual, una vez más, tendrá que ser definida por el TJUE en su jurisprudencia.

Sobre este particular, ya la AEPD en un documento titulado "El impacto del Reglamento General de Protección de Datos sobre la actividad de las Administraciones Públicas"[142], da cuenta de ello, cuando indica textualmente que "en muchos casos, los efectos del RGPD serán los mismos que para cualquier otro responsable o encargado", haciendo especial énfasis en una serie de disposiciones que tienen especial incidencia en el ámbito de la gestión y Administración Pública.

Entre ellas destacan las relativas a la finalidad y base jurídica sobre la que se realiza el tratamiento de datos personales por parte de la Administración, los mecanismos de ejercicio de derechos, la información que se ofrece a los interesados –la cual podría hacerse mediante el sistema de capas que la misma AEPD ha sugerido para entes privados[143]- el ofrecimiento de garantías de cumplimiento de la normativa de protección de datos, análisis de riesgos para los tratamientos de datos que se lleven a cabo, el necesario establecimiento de un registro de actividades de tratamiento de datos según las exigencias del RGPD, la necesaria revisión de las medidas de seguridad en concordancia con la nueva legislación, la designación del delegado de protección de datos cuando corresponda así como la necesidad de adaptar las transferencias internacionales de datos a los nuevos requerimientos. Todo ello, como bien lo menciona la AEPD, labor que corresponde hacer, básicamente, a todos los encargados y responsables de tratamiento de datos, sin excepción, sean entes públicos o privados.

[142] AEPD (s.f.). El impacto del Reglamento General de Protección de Datos sobre la Actividad de las Administraciones Públicas. Recuperado de: http://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/Impacto_RGPD_en_AAPP.pdf

[143] AEPD (2017). La importancia de la información por capas en el Reglamento General de Protección de Datos. Recuperado de: http://www.agpd.es/blog/la-importancia-de-la-informacion-por-capas-en-el-reglamento-general-de-proteccion-de-datos-ides-idPhp.php

Recapitulación

El RGPD supone una actualización trascendental en la normativa de protección de datos, y como se ha apuntado, un cambio de paradigma en la tutela de este derecho, que pasa de un enfoque reactivo, a un enfoque proactivo por parte de los encargados y responsables del tratamiento de datos de carácter personal, lo que permitirá, en principio, responder de una mejor forma a los retos que presenten las nuevas tecnologías. Además, pretende una homogeneización de la normativa en los Estados miembro, que si bien avanzó con la Directiva 95/46, no logró alcanzarse al punto esperado.

También, ha supuesto un momento oportuno para incorporar la doctrina y jurisprudencia del TJUE, que en algunos casos se traduce en el reforzamiento de los principios y derechos existentes en la Directiva 95/46, la ampliación de conceptos, como por ejemplo el de dato de carácter personal, la inclusión de los datos genéticos y biométricos, así como la incorporación de nuevos artículos al catálogo de derechos, como lo es el caso del derecho al olvido.

De igual forma representa un avance en cuanto a obligaciones para los encargados y responsables del tratamiento de datos personales, como por ejemplo, el privacy by design o privacy by default, las obligaciones de notificar a la autoridad de control cuando existan violaciones de seguridad, así como la obligación de contar con un delegado de protección de datos en los casos en que el tratamiento de los datos así lo requiera.

Pese a todos estos avances, hay cuestiones que han quedado sin resolver en la medida esperada, como por ejemplo, el conflicto constante que genera la protección de datos en su relación con el derecho de los ciudadanos de acceder a la información pública que está en poder de las autoridades. Sobre este particular, únicamente ha llevado a un artículo una disposición que ya estaba contenida en los considerandos de la Directiva 95/46 y que someramente menciona que los datos personales que consten en documentos oficiales en poder de una autoridad u organismo público podrán ser comunicados siempre y cuando se concilie dicho acceso con el derecho a la protección de los datos personales.

Ello nos lleva una vez más a recurrir a la jurisprudencia y los criterios que vaya definiendo el TJUE, que hasta ahora y como se analizará de seguido, ha tenido una línea clara en lo que entiende es la solución a este conflicto, lo que sin duda alguna, en la práctica se verá moldeado y perfilado por las nuevas disposiciones generales del RGPD.

Segunda parte

Transparencia, acceso a los documentos y protección de datos en el ámbito comunitario

Capítulo III. Transparencia y protección de datos en el ámbito comunitario

SUMARIO: 1. Cuestiones preliminares. 2. El derecho de acceso a los documentos en el ámbito de las instituciones de la UE. A. Antecedentes del Reglamento 1049/2001. B. Objeto del Reglamento 1049/2001. 3. El derecho a la protección de datos en las instituciones de la UE. A. Antecedentes del Reglamento 45/2001. B. Objeto del Reglamento 45/2001. 4. La tensión entre la transparencia, acceso a los documentos públicos y protección de datos de carácter personal.

1. Cuestiones preliminares

Ante una percepción de opacidad y poca transparencia en el seno de las instituciones comunitarias en la década de los noventa, surgió la necesidad de promover una institucionalidad transparente y abierta hacia la ciudadanía, la cual terminó por quedar plasmada en el Reglamento (CE) 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 (Reglamento 1049/2001)[144].

[144] Desde el 30 de mayo de 2008, la CE presentó una Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión, como parte de la imperiosa necesidad, a su criterio, de revisar el Reglamento existente (1049/2001) que en el momento de emitirse la Propuesta llevaba ya 6 años de aplicación y había dado lugar a jurisprudencia del TJUE y criterios del Defensor del Pueblo Europeo a través de las quejas que ha resuelto. Una segunda propuesta fue presentada por la CE el 21 de marzo de 2011, con el fin de adaptar el Reglamento 1049/2001 a los requisitos del Tratado de Lisboa, ampliando el ámbito de aplicación del Reglamento a todas las instituciones, órganos, oficinas y agencias de la UE, con ciertas restricciones en lo que respecta al TJUE, al Banco Central Europeo y al Banco Europeo de Inversiones. Al día de hoy no existen los consensos necesarios para la aprobación de ninguna Propuesta de reforma al Reglamento 1049/2001, siendo que uno de los puntos más controversiales ha sido el tratamiento de la excepción de acceso a la información en virtud de los datos personales que consten en los documentos. Sobre este particular, AUGUSTYN Y MONDA comentan: "as a part of its 'European Transparency Initaive' launched in November 2005, the Commission started a review of Regulation 1049/2001, eventually adopting a proposal for a new regulation in April 2008, aimed at achieving more transparency in legislation and bringing EU provisions into alignment with the Århus Convention. The proposal was based on views of the European Parliament expressed in its resolution of April 2006, the outcome of a public consultation exercise launched by a Commission Green Paper and the case law of the General Court and the Court of Justice of the EU interpreting Regulation 1049/2001. The Commission's proposal provoked a vivid debate amongst the institutions. The European Parliament was not happy with the choice of a recast procedure of the regulation as well as some of its content. And although it voted in March 2009 on a report containing a great number of amendments, it decided not to adopt a legislative resolution, as it considered that this dossier should be referred to the next parliamentary term. As a result, no formal position of the European Parliament was forged at first reading. Some of the most controversial issues of the proposal concerned: the definition of 'document' [Article 3(a)] and the scope of application [Article 2(5),(6)]; the exception of legal advice

Para esas mismas fechas, se había aprobado ya la Directiva 95/46 que obligaba a los Estados miembros a adoptar la legislación doméstica necesaria con el fin de trasponer dicha directiva reguladora de la protección de datos personales, pero se estaba ante el inconveniente de que se exigía la trasposición a los Estados miembro pero no a las instituciones comunitarias. Ante este vacío, existió desde un primer momento un compromiso de dichas instituciones por atender la Directiva 95/46 y finalmente, para disipar toda duda sobre su aplicación a dichas instituciones, se determinó la aprobación del Reglamento 45/2001, relativo al tratamiento de datos personales en el seno de las instituciones.

Ambos Reglamentos persiguen fines distintos, por un lado, el Reglamento 1049/2001, pretende asegurar el derecho de acceso a los documentos, mientras que por otro lado, el Reglamento 45/2001 busca tutelar la intimidad y la protección de datos personales. La tensión resulta evidente, más cuando se deben aplicar dichos reglamentos en un mismo contexto.

En esta Segunda Parte daremos cuenta de la solución que ha dado el TJUE a dicho conflicto, para lo cual resulta necesario hacer un análisis, al menos breve, de la normativa que regula el conflicto en cuestión. Para estos efectos, en este Capítulo se hará un análisis de los antecedentes de cada marco normativo y de su objeto primordial, con el fin de poder abordar con mayor claridad en el último apartado la tensión de la relación entre la transparencia, el acceso a los documentos y la protección de datos personales, y así estudiar en el Capítulo siguiente, a las claves de solución del conflicto que ha dado la jurisprudencia del TJUE.

---

provided by the legal services of the EU institutions [Article 4(2c)]; relation between the right of access to documents and the right to personal data protection [Article 4(5)]; and 4) Members States' documents and Member States' rights to restrict access [Article 5(2)]". Ver en: Augustyn, M.; Monda, C. (2011). Transparency and access to documents in the EU: ten years from the adoption of Regulation 1049/2001. *EIPAScope*, 2011 (1). pp. 17-20. En este mismo sentido, PIÑAR MAÑAS comenta que: "la propuesta de reforma del Reglamento modifica sustancialmente el régimen de las excepciones. Por un lado abandona la distinción entre excepciones absolutas y relativas, eliminando cualquier referencia a que la divulgación de la información revista un interés público superior. Por otro, lo que nos interesa especialmente, reelabora la excepción relativa a la privacidad, que se reconduce mucho más a la protección de datos, en estos términos: Los nombres títulos y funciones de los cargos públicos, de los empleados y de los representantes de intereses, en relación con sus actividades serán facilitados salvo que, en casos particulares, el acceso pueda afectar a dichas personas. Cualquier otro dato personal será suministrado de acuerdo con las condiciones del tratamiento legítimo de tales datos, tal como se prevé en la legislación de la Comunidad Europea sobre esta materia". Ver en: Piñar Mañas, J.L. (2014). Transparencia y protección de datos. Una referencia a la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información y buen gobierno. En J.L. Piñar Mañas (Dir.), Transparencia, acceso a la información y protección de datos. Madrid: Editorial Reus. pp. 45-57.

2. El derecho de acceso a los documentos en el ámbito de las instituciones de la UE

A. Antecedentes del Reglamento 1049/2001

El antecedente más incipiente de la normativa comunitaria en materia de acceso a la información pública data de 1983, con la Decisión 359/83/CECA de la Comisión, de 8 de febrero y el Reglamento (CEE, EUROATOM) 354/83 del Consejo, ambos relativos a la apertura al público de los archivos históricos de la Comunidad Económica Europea y de la Comunidad Europea de la Energía, por medio de la cuales se comprometía a ambas instituciones a la creación de archivos históricos que estarían abiertos al público una vez transcurridos 30 años a partir de la fecha de elaboración de los documentos y unidades archivísticas. En 1984, el Parlamento Europeo, el Consejo y la Comisión depositaron sus archivos históricos en el Instituto Universitario Europeo de Florencia, donde quedarían a disposición del público.

Es hasta 1992 con el Acta Final del Tratado de la EU, con el fin de resguardar a las instituciones europeas de las críticas en torno a su tono mercantilista y opacidad de la construcción comunitaria tal y como lo menciona GUICHOT[145], incluyó una declaración expresa relacionada con el derecho de acceso a la información y su intrínseca naturaleza con el funcionamiento y carácter democrático de las instituciones europeas. En ese sentido, la Declaración 17 del Tratado de Maastricht, expresamente dispone:

> "La conferencia estima que la transparencia del proceso de decisión refuerza el carácter democrático de las Instituciones, así como la confianza del público en la Administración. La Conferencia recomienda, por consiguiente, que la Comisión presente al Consejo, a más tardar en 1993, un informe sobre medidas destinadas a mejorar el acceso del público a la información que disponen las Instituciones".

Describe NIETO que desde ese momento se volvió un tema recurrente acercar la UE a los ciudadanos[146] y por ello no es de extrañar que numerosos Consejos Europeos se dedicaran a tratar el tema.

Así por ejemplo, en la Declaración de Birmingham de 16 de octubre de 2012, el Consejo Europeo señaló la importancia de contar con una Comunidad más abierta y

[145] Guichot, E. *Transparencia y acceso a la información en el Derecho europeo.* Sevilla: Cuadernos Universitarios de Derecho Administrativo – Editorial Derecho Global, p. 78.
[146] Nieto Garrido, E. (2014). Transparencia y acceso a los documentos *versus* el derecho a la protección de datos de carácter personal en la reciente jurisprudencia de TJUE. En Piñar Mañas, J. L. (Dir.), *Transparencia, acceso a la información y protección de datos*. Madrid: Editorial Reus. pp. 63-96.

cercana a los ciudadanos[147]. Varios meses después, en el Consejo de Edimburgo de 11 y 12 de diciembre de 1992 reiteró el compromiso adquirido en Birmingham y propuso una serie de medidas en el ámbito de la transparencia que incluían la presentación del programa anual de trabajo, la ampliación de consultas antes de la presentación de las propuestas, la publicación de los documentos de la CE en todas las lenguas comunitarias, entre otras[148].

Seguido a estos Consejos, surgieron adicionalmente una serie de trabajos preparatorios entre los que destacan la Comunicación titulada "Una mayor transparencia en el trabajo de la Comisión"[149], de 5 de marzo de 1993 y la Comunicación de 5 de mayo de 1993 denominada "Acceso de los ciudadanos a los documentos de las Instituciones"[150], ambas enfocadas a resaltar la importancia de la transparencia en el ámbito comunitario.

En junio de 1993, después de concluido el análisis comparativo del marco normativo comunitario que le había sido encomendado a la CE en las Conclusiones del Consejo de Edimburgo, se emitió la Comunicación al Consejo, al Parlamento y al Comité Económico y Social titulada "Transparencia en la Comunidad". En dicha Comunicación indica que en principio debería permitirse el acceso a los documentos, salvo con determinadas excepciones y apunta a una serie de principios básicos que la CE debería establecer, con el fin de garantizar dicho acceso. Estos principios buscan definir la finalidad perseguida, la necesidad de que las garantías de acceso sean adoptadas por todas las instituciones y el necesario balance que se debe lograr respecto de otros derechos:

> "-la importancia de reforzar una relación abierta entre las instituciones comunitarias y sus ciudadanos;
>
> - las medidas adicionales tendrían un mayor efecto si fuesen adoptadas por todas las instituciones, teniendo en cuenta la función específica de cada institución y sus costumbres de trabajo específicas;
>
> - deberá encontrarse un equilibrio entre los intereses de una mayor apertura y transparencia y otras consideraciones como la protección de intereses públicos y

[147] Declaración de Birmingham, Consejo Europeo de Birmingham de 16 octubre de 1992 (EC 10-1992), p. 4.
[148] Conclusiones de la Presidencia, Consejo Europeo de Edimburgo de 11-12 de diciembre de 1992 (EC 12-1992) p. 7.
[149] Comunicación de 5 de marzo de 1993, *Mayor transparencia en el trabajo de la Comisión*, DOCE *núm.* C 63/8, p. 8.
[150] Comunicación al Consejo, al Parlamento Europeo y al Comité Económico y Social, de 8 de junio de 1993, *Acceso a los ciudadanos a los documentos de la instituciones*, DOCE *núm*. C156/5, p. 5.

> privados y la importancia de garantizar que el trabajo de las instituciones pueda realizarse de forma oportuna y eficaz".[151]

Cabe destacar que ya desde ese momento, en el Anexo 2 de la Comunicación se señala que el acceso a los documentos puede negarse cuando sea necesario para salvaguardar, entre otros, la protección de la intimidada personal e individual.

Seguido a esta Comunicación, el 22 de junio de 1992 en el Consejo Europeo de Copenhague se invitó a la CE a continuar su trabajo, partiendo de la base de que los ciudadanos deben tener el acceso más completo posible a la información que está en poder de las instituciones europeas[152].

En diciembre de 1993, este proceso preparatorio culminó con la aprobación del llamado Código de Conducta relativo al acceso del público a los documentos del Consejo y de la Comisión, que si bien carecía de efectos jurídicos, no es menos cierto como menciona GUICHOT REINA que constituía ya la base para la posterior positivización del derecho por cada institución comunitaria[153]. Para autores como NIETO GARRIDO, el Código de Conducta presentaba una serie de desventajas adicionales como por ejemplo, no contener "ninguna indicación sobre quienes tenían acceso a los documentos, cómo hacer la solicitud y si el solicitante podía serlo no sólo respecto de documentos del Consejo y de la Comisión, sino también respecto de documentos de organismos y agencias. Además, el Código contenía una lista amplia de supuestos en los que el acceso a los documentos podía ser denegado".[154] No obstante lo anterior, debe siempre reconocerse el avance que supone en este tipo de casos hacer la transición de un espacio sin regulación a los primeros esfuerzos que potencialmente desencadenan en la concreción de normativas sólidas de acceso a la información.

Durante ese tiempo y hasta la aprobación del TCE, la normativa administrativa adoptada por cada institución europea constituyó un marco jurídico suficiente para reconocer un derecho subjetivo de acceso a los documentos a los ciudadanos. Como apunta GUICHOT[155], esto generó una polémica, pues era evidente que las normas de acceso a los documentos que habían sido adoptadas por las instituciones europeas escapaban del

[151] Comunicación al Consejo, al Parlamento y al Comité Económico y Social, *Transparencia en la comunidad.* COM (1993) 258 final, p. 5.
[152] Conclusiones de la Presidencia, Consejo Europeo de Copenhague de 21-22 de junio de 1993 (Doc. SN 180/93, p. 19.
[153] Guichot Reina, E. (2011), *op cit.* p. 80.
[154] Nieto Garrido, E. (2014), *op. cit.* p. 67.
[155] Guichot Reina, E. (2011), *op. cit.* p. 82.

ámbito normativo de establecimiento de su organización interna y consagraban un derecho subjetivo de acceso a los documentos en toda regla. Este tema lo vino a definir el TJUE en la STJUE de 30 de abril 1996, caso Países Bajos/Consejo, en que la reconoció que:

> "Debe admitirse que, mientras que el legislador comunitario no haya adoptado una normativa general sobre el derecho de acceso al público a los documentos que obran en poder de las Instituciones comunitarias, éstas deben adoptar las medidas que tengan por objeto la tramitación de tales solicitudes en virtud de su facultad de organización interna, que las habilita para adoptar medidas apropiadas con vistas a garantizar s funcionamiento interno en interés de una buena administración".

Todos estos esfuerzos por garantizar el acceso a los documentos y acercar las instituciones europeas a los ciudadanos se consolidaron en el TCE, que en el artículo 255 reconoce a todo ciudadano de la UE, así como de toda persona física o jurídica que resida o tenga su domicilio social en un Estado miembro, un derecho de acceder a los documentos del Parlamento Europeo, del Consejo y de la Comisión:

> "Artículo 255.
>
> 1. Todo ciudadano de la Unión, así como toda persona física o jurídica que resida o tenga su domicilio social en un Estado miembro, tendrá derecho a acceder a los documentos del Parlamento, del consejo y de la Comisión, con arreglo a los principios y as condiciones que se establecerán de conformidad con los apartados 2 y 3.
>
> 2. El Consejo, con arreglo al procedimiento previsto en el artículo 251, determinará los principios generales y los límites, por motivos de interés público o privado, que regulan el ejercicio de este derecho de acceso a los documentos, en el plazo de dos años a partir de la entrada en vigor del Tratado de Ámsterdam-
>
> 3. Cada una de las instituciones mencionadas elaborará en su reglamento interno disposiciones específicas sobre el acceso a sus documentos".

Seguido de la aprobación del TCE, varios Consejos Europeos continuaron profundizando sobre este tema. En el Consejo Europeo de Cardiff celebrado entre el 15 y 16 de junio de 1998 se resaltó nuevamente la necesidad del esfuerzo que debían llevar a cabo las instituciones europeas para conseguir un acercamiento a los ciudadanos, mediante el compromiso de conceder el mayor acceso posible a la información sobre sus actividades[156]. El tema fue abordado de nuevo en el Consejo Europeo de Köln en 1999[157].

[156] Conclusiones de la Presidencia, Consejo Europeo de Cardiff de 15 y 16 de junio de 1998, apartado 28-31. (Doc. SN 150/1/98 REV 1).
[157] Conclusiones de la Presidencia, Consejo Europeo de Köln de 3 y 4 de junio de 1999 (Doc. 9064/99).

Más adelante, en el 2000, la CDFUE –la cual se tornaría jurídicamente vinculante con la adopción del Tratado de Lisboa- reconoció en el artículo 42 el derecho de acceso a los documentos, al disponer:

> "Artículo 42.
>
> Todo ciudadano de la Unión o toda persona física o jurídica que resida o tenga su domicilio social en un Estado miembro tiene derecho a acceder a los documentos del Parlamento Europeo, del Consejo y de la Comisión".

En ese orden, el desarrollo normativo al que se hacía referencia en el artículo 255 del TCE se concretó con la aprobación del Reglamento 1049/2001, el cual constituye a la fecha la principal regulación del derecho de acceso a los documentos que están en poder de las instituciones europeas y se fundamenta, como bien lo apunta GUICHOT, "en los principios de transparencia, apertura y proximidad, participación, democracia y respeto a los derechos fundamentales".[158]

Vale aclarar que con la adopción del TFUE, el artículo 255 del TCE fue sustituido por el artículo 15 de dicho texto, que establece un marco normativo más completo y recoge el principio de apertura como forma de fomentar una buena gobernanza y garantizar la participación de la sociedad civil en los procesos de las instituciones comunitarias:

> "Artículo 15 (antiguo artículo 255 TCE)
>
> 1. A fin de fomentar una buena gobernanza y de garantizar la participación de la sociedad civil, las instituciones, órganos y organismos de la Unión actuarán con el mayor respecto al posible al principio de apertura.
>
> 2. Las sesiones del Parlamento Europeo serán públicas, así como las del Consejo en las que éste se delibere y vote sobre un proyecto de acto legislativo.
>
> 3. Todo ciudadano de la Unión, así como toda persona física o jurídica que resida o tenga su domicilio social en un Estado miembro, tendrá el derecho de acceder a los documentos de las instituciones, órganos y organismos de la Unión, cualquiera que sea su soporte, con arreglo a los principios y las condiciones que se establecerán de conformidad con el presente apartado.
>
> El Parlamento Europeo y el Consejo, con arreglo al procedimiento legislativo ordinario, determinarán mediante reglamentos los principios generales y los límites, por motivos de interés público o privado, que regulan el ejercicio de este derecho de acceso a los documentos.
>
> Cada una de las instituciones, órganos u organismos garantizará la transparencia de sus trabajos y elaborará en su reglamento interno disposiciones específicas sobre el acceso a sus documentos de conformidad con los reglamentos contemplados en el párrafo segundo.

[158] Guichot, E (2011). *op cit.* p. 86.

> El Tribunal de Justicia de la Unión Europea, el Banco Central Europeo y el Banco Europeo de Inversiones sólo estarán sujetos al presente apartado cuando ejerzan funciones administrativas.
>
> El Parlamento Europeo y el Consejo garantizarán la publicidad de los documentos relativos a los procedimientos legislativos en las condiciones establecidas por los reglamentos contemplados en el párrafo segundo".

B. Objeto del Reglamento 1049/2001

El Reglamento introduce, según lo exponen sus considerandos, un principio de apertura que busca acercar las instituciones a los ciudadanos, así como de garantizar una mayor participación en la toma de decisiones y una mayor legitimidad, eficacia y responsabilidad de cara a los ciudadanos en un sistema democrático. Asimismo, reconoce que esta apertura contribuye al reforzamiento de los principios de democracia y respeto a los derechos fundamentales que persigue la CDFUE y el Tratado UE.

Por otra parte, dispone que todos los documentos de las instituciones deben ser accesibles al público, lo que incluye tanto los documentos elaborados por las instituciones europeas como aquellos que han sido recibidos, eliminando así la regla de autor bajo la cual cabría alegar que si un documento no fue elaborado por las instituciones europeas pero se halla en poder de estas, la solicitud de acceso debe dirigirse a quien elaboró el documento y no accederse a través de las instituciones europeas. Sobre este particular, en STPI de 30 de noviembre de 2004, el TJCE dispuso con claridad:

> "53. (…) Por lo tanto, con arreglo a la regla del autor, una institución no estaba facultada para divulgar los documentos originarios de una amplia categoría de terceros, que incluía entre otros a los Estados miembros, y el solicitante de acceso estaba obligado, en su caso, a dirigirse directamente al tercero en cuestión.
>
> 54. El Reglamento no recoge la regla de autor y confirma que, en principio, todos los documentos de las instituciones deben ser accesibles al público (decimoprimer considerando del Reglamento".[159]

Añade también que si bien todos los documentos en principio deben ser accesibles al público, mediante el establecimiento de excepciones se pueden proteger otros intereses públicos y privados.

Su fin primordial, según lo dispone el artículo 1, es garantizar el acceso más amplio posible a los documentos, establecer las normas que garanticen el ejercicio más

[159] STPI (Sala Quinta ampliada) de 30 de noviembre de 2004, asunto T-168/02 (caso IFAW Internationaler Tierschtz-Fonds/Comisión, apartado 53-54).

fácil posible de este derecho y promover buenas prácticas administrativas para el acceso a los documentos.

Por su parte, el artículo 2 define tanto los beneficiarios como el ámbito de aplicación de la normativa. Sobre los beneficiarios, como ya se ha señalado previamente, tiene derecho de acceso a los documentos todo ciudadano persona física o jurídica que resida o tenga su domicilio social en un Estado miembro. Respecto del ámbito de aplicación, el artículo indica que aplica a todos los documentos que obren en poder de una entidad europea, con independencia de sí son sus autores o los han recibido y están en su posición. Tampoco hace distinción el ámbito de actividad de la UE a la que se refieran los documentos. El acceso a los documentos se debe hacer a través de una solicitud previa por escrito o en forma electrónica por medio de un registro.

El artículo 4, es uno de los artículos que más interesa para el tema de este trabajo. Establece de forma taxativa las excepciones al acceso a los documentos en virtud de la protección de intereses públicos o privados, los cuales son igualmente tutelados por el marco normativo comunitario, por ejemplo, "la protección de la intimidad y la integridad de la persona, en particular de conformidad con la legislación comunitaria sobre protección de los datos personales".

Estas excepciones, según lo ha entendido el TJUE, por ejemplo en la STPI de 7 de febrero de 2002, caso Kuijer/Consejo y STPI de 23 de noviembre de 2004, caso Turco/Consejo, deben ser interpretadas y aplicadas de forma restrictiva, de forma que no se frustre la aplicación del principio general de acceso a los documentos, así como a la luz del principio del derecho a la información y del principio de proporcionalidad[160].

Disposición también relevante es la contenida en el artículo 6 del Reglamento, por medio de la cual se indica que el solicitante no está obligado a justificar su solicitud. Posición que como bien lo indica PIÑAR MAÑAS,[161] el TPI ha reconocido en varias sentencias, como por ejemplo, la STPI de 6 de julio de 2006, caso Franchet y Byk/Comisión, en la que señaló expresamente:

> "Debe recordarse que, según el artículo 6, apartado 1, del Reglamento 1049/2001, el que solicita acceso no está obligado a justificar su solicitud y no tiene, por ello,

[160] STPI (Sala Cuarta) de 7 de febrero de 2002, asunto T-211/00 (caso Kuijer/Consejo), apartado 55-57; STPI (Sala Quinta) de 23 de noviembre de 2004, asunto T-84/03 (caso Turco/Consejo), apartado 60.
[161] Piñar Mañas, J.L. (2009). Seguridad, transparencia y protección de datos: el futuro de un necesario e incierto equilibrio. Documento de trabajo núm.147/2009. Laboratorio Alternativas, Fundación Alternativas, p. 40.

> que demostrar interés alguno en tener acceso a los documento solicitados (véase en relación con la aplicación de la Decisión 94/80, las sentencias del Tribunal de Primera Instancia de 6 de febrero de 1998, Interporc/Comisión, T-124/96, REC. p. II-231, apartado 48, e Interporc II, apartado 44). (…)".[162]

3. El derecho a la protección de datos en las instituciones de la UE

A. Antecedentes del Reglamento 45/2001

Previo a la regulación expresa del derecho a la protección de datos de carácter personal en lo que se refiere al tratamiento de los datos por parte de las instituciones comunitarias, este derecho había sido reconocido ya anteriormente por parte de la jurisprudencia del TEDH y en la Directiva 96/46[163], siendo que esta última en especial, obligaba a los Estados miembro a la implementación de este derecho en sus legislaciones domésticas.

La aprobación de la Directiva 95/46 y su obligatoria trasposición por parte de los Estados miembros a sus ordenamientos internos, condujo a que se creara como lo menciona RUIZ MIGUEL, una paradoja en tanto el derecho comunitario reconocía el derecho a la protección de datos de carácter personal de toda persona frente a los Estados miembros de la UE, pero no frente a las instituciones comunitarias[164].

Por otra parte, el artículo 286 del TCE incluyó una disposición que obligaba a la observancia de la protección de datos de carácter personal en el ámbito del funcionamiento de las instituciones y organismos de la UE, así como a la adopción de la normativa específica para las instituciones europeas y el establecimiento de un organismo de control independiente, con la finalidad de garantizar el respeto de este derecho por parte de las instituciones comunitarias. Textualmente, el artículo 286 del TCE disponía en forma expresa lo siguiente:

> "1. A partir del 1 de enero de 1999, los actos comunitarios relativos a la protección de las personas respecto del tratamiento de datos personales y a la libre circulación de dichos datos serán de aplicación a las instituciones y organismos establecidos por el presente Tratado o sobre la base del mismo.

[162] STPI (Sala Tercera) de 6 de julio de 2006, asuntos T-391/03 y T-70/04 (caso Franchet y Byk/Comisión), apartado 82.
[163] Nieto Garrido, E. (2014). Transparencia y acceso a los documentos *versus* el derecho a la protección de datos de carácter personal… *op. cit.* p. 73.
[164] Ruiz Miguel, C. (2003). El derecho a la protección de los datos personales en la Carta de Derechos Fundamentales de la Unión Europea: análisis crítico. *Revista de Derecho Comunitario Europeo*, Año 7, Núm. 14, Enero-Abril 2003. pp. 7-43

> 2. Con anterioridad a la fecha indicada en el apartado 1, el Consejo establecerá, con arreglo al procedimiento previsto en el artículo 251, un organismo de vigilancia independiente, responsable de controlar la aplicación de dichos actos comunitarios a las instituciones y organismos de la Comunidad y adoptará, en su caso, cualesquiera otras disposiciones pertinentes".

La redacción de este artículo explica RUIZ MIGUEL, suscito en su momento conflicto por parte de la doctrina, pues básicamente implicaba la sujeción de las instituciones comunitarias al cumplimiento de la Directiva 95/46 sin que fuese necesaria una medida de trasposición de este instrumento jurídico, problema que vino a ser solucionado con la aprobación del Reglamento 45/2001, que como se detallará más adelante no sólo transcribe casi que por completo la Directiva 95/46, sino que añade elementos novedosos como la creación del SEPD.

Posteriormente, el artículo 286 del TCE fue reemplazado por el actual artículo 16 del TFUE que de forma más amplia señala:

> "1. Toda persona tiene derecho a la protección de datos de carácter personal que le conciernan.
>
> 2. El Parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estado miembro en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. El respeto de dichas normas estará sometido al control de autoridades independientes.
>
> Las normas que se adopten en virtud del presente artículo se entenderán sin perjuicio de las normas específicas previstas en el artículo 39 del Tratado de la Unión Europea".

Adicionalmente, debe recordarse que en el 2000, con la aprobación de la CDFUE, se reconoció el derecho a la protección de datos de carácter personal como un derecho autónomo e independiente del derecho a la intimidad contenido en el artículo 7 de ese mismo texto normativo.

> "Artículo 8. Protección de datos de carácter personal
>
> 1. Toda persona tiene derecho a la protección de datos de carácter personal que la conciernan.
>
> 2. Estos datos se tratan de un modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.
>
> 3. El respeto de estas normas quedará sujeto al control de una autoridad independiente".

B. Objeto del Reglamento 45/2001

El objeto del Reglamento aparece claramente explicado en su parte considerativa, en la que se indica que este texto normativo busca adoptar una serie de disposiciones vinculantes y de derechos jurídicamente protegidos en lo que respecta al tratamiento de los datos por parte de las instituciones y los organismos comunitarios, así como el establecimiento de una autoridad de control independiente encargada de vigilar dichos tratamientos de datos por parte de las instituciones comunitarias.

Todas las instituciones y organismos comunitarios deben aplicar las disposiciones contenidas en el Reglamento, en la medida en que el tratamiento se lleve a cabo en el ejercicio de las funciones. Asimismo, establece que no se afectan los derechos y las obligaciones de los Estados miembros derivados de la Directiva 95/46/CE.

La parte considerativa del Reglamento dispone que los principios de la protección de datos deben aplicarse a toda persona identificada o identificable y a todo tratamiento que se efectúe por parte de las instituciones comunitarias. Asimismo, establece que la materia relativa al acceso a los documentos, incluidas las condiciones de acceso a los documentos que contengan datos de carácter personal, depende de la normativa aplicable al tenor del artículo 255 del TCE (Reglamento 1049/2001).

Por su parte, pese a que ya lo hemos explicado, el objeto del Reglamento 45/2001 aparece claramente definido en el artículo 1, el cual menciona en forma expresa que las instituciones y los organismos comunitarios deberán garantizar la protección de los derechos y libertades de las personas físicas, en especial el derecho a la intimidad y la protección de datos de carácter personal, sin prohibir la libre circulación de datos personales entre los Estados miembros.

En su artículo 3, se refiere al ámbito de aplicación de la norma, al igual que la parte considerativa, menciona que las disposiciones contenidas en el Reglamento aplican a todas las instituciones comunitarias, en cuanto el tratamiento de datos al que se refiere se lleve a cabo para el ejercicio de actividades que pertenecen al ámbito de aplicación del Derecho comunitario.

El artículo 4, que se refiere a los principios relativos a la calidad de los datos, dispone que estos deberán ser tratados de manera leal, lícita y recogidos para fines

determinados, explícitos y legítimos. Por su parte, el artículo 5 agrega los criterios de licitud del tratamiento y menciona que este únicamente puede llevarse a cabo cuando sea necesario para el cumplimiento de una misión de interés público, sea necesario para el cumplimiento de una obligación jurídica por parte del responsable, sea indispensable para la ejecución de un contrato que el interesado haya dado el consentimiento de forma inequívoca, o bien, que resulte inevitable para proteger los intereses esenciales del interesado.

Entre otras disposiciones, el Reglamento 45/2001 incluye un catálogo de derechos del interesado (derecho de acceso, rectificación, supresión, notificación a terceros y de oposición). Resulta especialmente relevante para este trabajo, el artículo 8 del Reglamento, que establece que las transmisiones de datos personales a destinatarios distintos de las instituciones y organismos comunitarios están sujetos a la Directiva 95/46 y además requiere que el destinatario demuestre la necesidad en la transmisión de los datos y no existan motivos para suponer que ello pueda perjudicar los intereses legítimos del interesado.

4. La tensión entre la transparencia, acceso a los documentos públicos y protección de datos de carácter personal

El análisis separado de los marcos normativos que regulan el acceso a la información pública en la UE resulta pacífico. No obstante, cuando nos encontramos ante el ejercicio del derecho de acceso a documentos que contienen datos de carácter personal, aflora, como lo menciona GUICHOT REINA "la apasionante cuestión de las relaciones entre transparencia y privacidad"[165]. En especial, cuando se pone en contraposición dos derechos que persiguen fines diametralmente opuestos, pero resultan de igual forma tutelados en los ordenamientos jurídicos, en este caso particular, por el Derecho comunitario.

Cómo puede entonces conciliarse el derecho a la intimidad y protección de datos de carácter personal, que por un lado busca garantizar una esfera libre de cualquier tipo de injerencia a las personas, con el principio de transparencia y el derecho de acceso a los documentos, que por su parte pretende dar una máxima divulgación de las actuaciones

[165] Guichot, E. (2011). Transparencia y acceso a la información en el Derecho europeo. Sevilla: Global Law Press. p. 153.

del poder público, que en muchas ocasiones se basan en el tratamiento de datos de carácter personal, es la interrogante que surge.

SOLOVE, citado por PIÑAR MAÑAS[166], plantea la interrogante en los términos de "¿Cómo puede reconciliarse la tensión entre la transparencia y privacidad? ¿Debe sacrificarse le acceso a los documentos en el altar de la privacidad? ¿O debe la privacidad evaporarse para poder desinfectar los gobiernos con la luz del sol?".

En similares términos, la Abogado General Sharpston, en las conclusiones generales del caso Bavarian Lager, plantea la interrogante utilizando la paradoja de Isaac Asimov y pregunta: "¿Qué ocurriría si una fuerza irresistible se enfrentase con un cuerpo inamovible?"[167]. Sugiere la abogado Sharpston que para obtener una imagen de la problemática a la que nos enfrentamos y visualizar la complejidad que entraña, se sustituya "fuerza irresistible" por derecho de acceso a los documentos y "cuerpo inamovible" por derecho a la protección de datos.

Adelanta la señora Sharpston, al igual que Asimov, que no puede existir un universo con tales contradicciones, lo cual lleva a la necesaria precisión y definición de los conceptos jurídicos que supuestamente entrarán en conflicto, para así llegar a la conclusión de que el choque de derechos resulta más aparente que real.[168]

Inicialmente, el WP 29, con ocasión de la consulta pública de la CE sobre el llamado "Libro Verde: La información del sector público: un recurso clave para Europa" COM (1998) 585, emitió el Dictamen 3/99 sobre información del sector público y protección de datos personales, en donde se refirió en forma amplia sobre el debate que ahora nos ocupa. En su dictamen, concluyó que "(…) si bien la protección de los datos personales no debe constituir un obstáculo al derecho de los ciudadanos a tener acceso a los documentos administrativos en las condiciones previstas por cada legislación nacional, la Directiva no pretende sin embargo privar de toda protección a los datos accesibles al público (…) el carácter público de un dato de carácter personal, no priva,

[166] Piñar Mañas, J.L. (2010). Transparencia y protección de datos: las claves de un equilibrio necesario. En García Macho, R. (Coord.), *Derecho administrativo de la información y administración transparente* (p. 81-95). Madrid: Marcial Pons.
[167] Conclusiones del Abogado General Sra. Eleanor Sharpston, de 15 de octubre de 2009, asunto C-28/09 P (caso Comisión/Bavarian Lager), apartado 2.
[168] *Ibíd.* apartados 3-4.

ipso facto y para siempre, a dicha persona de la protección que le garantiza la ley en virtud de los principios fundamentales de defensa de la identidad humana"[169].

Además, sugirió que ambos derechos, acceso a la información y proteger datos, deben ser reconciliados, por medio de una valoración caso por caso, en donde se tengan en cuenta, por ejemplo, los principios de finalidad y legitimidad, la información de la persona, el derecho de oposición de la persona y la utilización de las nuevas tecnologías para contribuir al respeto del derecho a la intimidad.

Por su parte, el Defensor del Pueblo Europeo en su carta *"Openness and data protection"* de 14 de noviembre de 2001, consideró que si bien tanto el derecho de protección de datos como el derecho de acceso a los documentos persiguen fines legítimos, debe encontrarse un balance entre ambos; no obstante lo anterior, a criterio del Defensor del Pueblo ello no implica que la normativa de protección de datos aplique, de forma general como un principio de confidencialidad en la Administración pública, como para requerir que exista dicho balance en cada oportunidad que un documento contenga un nombre; pues esta interpretación excesiva no solo perjudicaría el propósito del derecho de acceso a los documentos, sino también iría en contra de la finalidad genuina del derecho a la protección de datos[170].

Postura similar adoptó el PE en su resolución, de 11 de diciembre 2001, sobre el informe rendido por el Defensor del Pueblo Europeo, en la que enfáticamente señala que "a menudo se producen conflictos entre la demanda de transparencia y la protección de la integridad personal; destaca que el principal objetivo de la protección de los datos es proteger la vida privada y la información; por consiguiente, no debería hacerse referencia a la protección de datos cuando, por ejemplo, las personas están actuando en calidad pública, cuando participan en un proceso de toma de decisiones público por propia iniciativa o cuando intentan influir en dicha toma de decisiones". [171]

Más adelante, por medio de carta de 30 de septiembre de 2002, dirigida al Presidente de la CE, el Defensor del Pueblo enfatiza en su preocupación sobre la indebida

[169] WP 29, *Información del sector público y protección de datos personales,* Dictamen 3/99, 3 de mayo de 1999, p. 5, 12.
[170] *Ibíd.*
[171] Resolución del Parlamento Europeo sobre el Informe Especial al Parlamento Europeo como continuación del proyecto de recomendación remitido a la Comisión Europea en la reclamación 713/98/IJH (redactado de conformidad con el apartado 7 del artículo 3 del Estatuto del Defensor del Pueblo Europeo) (C5-0463/2001 – 2001/2194(COS)), de 11 de diciembre de 2001, apartado 3.

aplicación del derecho a la protección de datos de carácter personal, que conduce a la existencia de un derecho a participar de forma anónima en actividades públicas, lo cual representa un serio riesgo al principio de transparencia y el derecho de acceso a los documentos. Asimismo, en esa nota propone modificaciones a la parte considerativa, tanto de la Directiva 95/46 como del Reglamento 45/2001, para que se interprete que ambos cuerpos normativos no constituyen una limitación al principio de transparencia y el derecho de acceso a los documentos regulado en el Reglamento 1049/2001.

Ese mismo debate fue abordado también por el SEPD en el 2005, en el documento *Public Access to documents and data protection*[172], desde la perspectiva del hecho de que un documento contenga datos personales no implica una vulneración de la privacidad por sí sola; sino dependerá de las circunstancias en que se dé el acceso a los documentos es que se puede vulnerar dicho derecho.

A su criterio, tanto el Reglamento 45/2001 como el 1049/2001 no entran necesariamente en colisión; pues en la mayoría de los casos se puede garantizar el acceso a los documentos públicos sin causar perjuicio o lesión al derecho de proteger datos de carácter personal de cuya persona contenga el documento los datos.

Asimismo, estima que para efectos de determinar la aplicación de la excepción contenida en el artículo 4, apartado 1, letra b) del Reglamento 1049/2001, debe tenerse en cuenta si está en juego el derecho a la intimidad y la protección de datos de una persona; si el acceso afectará a la persona titular de los datos y, por último, si el acceso público a tales datos está permitido por la legislación de protección de datos.[173]

Esta posición fue posteriormente modificada en el 2011[174] en virtud de la STJUE en el caso Bavarian Lager/Comisión, donde se concluye que la colisión entre la transparencia y la protección de datos de carácter personal debe solucionarse a través de una ponderación de los derechos e intereses en juego en cada caso concreto, tal y como lo decidió el TJUE en la sentencia mencionada.

[172] SEPD (2005). Public access to documents and data protection, Background Paper Series, núm. 1, julio 2005. Recuperado de: https://edps.europa.eu/
[173] *Ibíd.*.
[174] SEPD (2011). Public access to documents containing personal data after the Bavarian Lager ruling. Recuperado de: https://edps.europa.eu/

Para autores como GUICHOT REINA[175], la labor de dar una respuesta satisfactoria a la colisión de derechos, encuentra su dificultad ante la ausencia de una norma que encaje entre ambos derechos; pues ni la normativa relativa a la protección de datos de carácter personal ni la del derecho de acceso a los documentos, contienen una disposición lo suficientemente clara a este respecto. Problemática que había sido señalada por el SEPD en su documento de marzo de 2011, en donde tras el fallo del caso Bavarian Lager/Comisión, resaltó que existía una necesidad de contar con un marco normativo general que brindara una guía sobre cómo asegurar el balance adecuado entre la transparencia y la protección de datos[176]. Por su parte, para la Abogado General, por ejemplo, la solución se basa en el justo equilibrio entre ambos derechos y el análisis detallado de la normativa, pues en el Reglamento 1049/2001 existe una remisión al Reglamento 45/2001.

Resolver la cuestión sobre si es posible conciliar el derecho de acceso a los documentos con el derecho a la protección de datos de carácter personal, conlleva necesariamente el análisis de las relaciones existentes entre la normativa que regula cada derecho con el fin de determinar si existen relaciones o remisiones entre ellos o sí por el contrario, resultan excluyentes entre sí. Situados en el primer supuesto, cabe llegar a una solución balanceada que parte de un análisis armónico e integrado, en este caso de los Reglamentos 45/2001 y 1049/2001.

Por el contrario, si se parte de la premisa de que en tanto persiguen fines totalmente contrapuestos son excluyentes entre sí, la solución consiste en decidir cuál derecho tiene una prevalencia sobre el otro. Esta última solución presenta el serio inconveniente de desconocer que ambos derechos se encuentran en un mismo plano y son protegidos por el ordenamiento comunitario. Además, es abundante la jurisprudencia del TJUE que ha dispuesto que en los casos donde existan colisiones de derechos, deben ponderarse los intereses y los derechos fundamentales en juego, cuestión que se analiza a continuación.

[175] Guichot, E. (2011). op. cit., p. 154.
[176] SEPD (2005). Public access to documents… *op. cit.*

Recapitulación

El análisis del marco normativo comunitario que regula el acceso a los documentos en poder de las instituciones comunitarias y el tratamiento de los datos de carácter personal por parte de estas, muestra de entrada la tensión existente entre ambos reglamentos, en tanto persiguen fines que en principio son contrapuestos: mientras uno pretende la publicidad de los documentos públicos, el otro busca asegurar la privacidad y protección de los datos de carácter personal de los ciudadanos.

A nivel comunitario, la aplicación y relación entre ambos reglamentos ha llegado a suscitar polémica, especialmente cuando se ha pretendido el acceso a los documentos que contienen datos de carácter personal y que están en poder de las instituciones comunitarias. Mientras que las instituciones comunitarias aplican la normativa y entienden que el artículo 4 del Reglamento 1049/2001 contiene una excepción al acceso basada en los datos de carácter personal y remite al artículo 45/2001 sobre protección de datos, algunas instituciones comunitarias como el Defensor del Pueblo Europeo y el SEPD, han advertido que la relación existente entre ambos reglamentos y la necesaria aplicación de la normativa de protección de datos, no debe entenderse de forma que se impida el acceso a los mismos o que se pueda entender que existe un derecho al anonimato cuando se actúa en la función pública.

Capítulo IV. La jurisprudencia del Tribunal de Justicia de la Unión Europea en materia de transparencia, acceso a los documentos y protección de datos personales

SUMARIO: 1. Cuestiones preliminares. 2. La jurisprudencia del TJUE en transparencia, acceso a los documentos y protección de datos personales. A. STJUE de 29 de junio de 2010: caso Bavarian Lager/Comisión. a) Hechos. b) La interpretación armónica de ambos reglamentos. B. STGUE de 7 de julio de 2011: caso Valero Jordana/Comisión. a) Hechos. b) La necesaria aplicación de ambos reglamentos. C. STGUE de 23 de noviembre de 2011: caso Dennekamp/Parlamento I. a) Hechos. b) La obligada justificación y demostración de necesidad en el acceso. D. STGUE de 28 de marzo de 2012: caso Egan y Hackett/Parlamento. a) Hechos. b) El riesgo para la intimidad y protección de datos personales debe ser razonablemente previsible. E. STGUE de 11 de junio de 2015: caso McCullough/CEDEFOP. a) Hechos. b) Deber de justificar la negativa del acceso a los documentos que contienen datos de carácter personal. F) STUE de 15 de julio de 2015, caso Dennekamp/Parlamento II. a) Hechos. b) Procedencia de la cesión de datos cuando es el único mecanismo para lograr el objetivo de la transparencia. G. STJUE de 16 de julio de 2015, caso ClientEarth y Pan Europe/EFSA. a) Hechos. b) Procedencia de la cesión de datos cuando es el mecanismo idóneo para la consecución del objetivo que persigue la transparencia. 3. Las claves para la solución del conflicto según la jurisprudencia del TJUE. A. La necesaria justificación del acceso y la ponderación de derechos e intereses. B. La metodología de la ponderación seguida por el TJUE. a) La identificación de los derechos o intereses en conflicto. b. La atribución de un valor o peso a los derechos en conflicto. c) El juicio de prevalencia.

1. Cuestiones preliminares

Encontrar el balance entre transparencia, acceso a los documentos y protección de datos personales no es ni ha sido una tarea fácil y de ello dan cuenta la normativa comunitaria, las opiniones de diferentes organismos comunitarios, sectores académicos y sobre todo, la jurisprudencia del TJUE que se ha encargado de dirimir los conflictos que suscita la aplicación de la legislación vigente, cuando se pretende el acceso a documentos que contienen datos de carácter personal.

A continuación se hará un análisis de la jurisprudencia del TJUE en materia de transparencia, acceso a los documentos y protección de datos, siguiendo un orden cronológico de las sentencias que ha dictado. Esto, no sólo por una cuestión de orden sino porque facilita la comprensión de la evolución de la jurisprudencia, que ha estado marcada desde la primer sentencia que dictó el TJUE en el caso Bavarian Lager/Comisión.

El Capítulo se divide en dos apartados más. En el primero de ellos, haremos un recuento de las sentencias del TJUE en esta materia, dividiendo cada epígrafe en dos sub

epígrafes, uno con los hechos del caso y otro con su principal aporte a la solución del conflicto.

El segundo apartado, por su parte, está dedicado al análisis de las claves de la solución al conflicto que se pueden desprender de la jurisprudencia del TJUE y que a falta de una regulación más detallada en el RGPD, seguirán siendo perfiladas por el TJUE bajo la óptica y nuevo paradigma del RGPD.

2. La jurisprudencia del TJUE en transparencia, acceso a los documentos y protección de datos personales

A. STJUE de 29 de junio de 2010: caso Bavarian Lager/Comisión

En la STJUE de 29 de junio de 2010, caso Bavarian Lager/Comisión, el TJUE tuvo la oportunidad de referirse por primera vez a la relación existente entre la transparencia, el derecho de acceso a los documentos y la protección de datos de carácter personal. Esta sentencia marca un hito importante, además, porque sienta las bases de la línea jurisprudencial que ha seguido el TJUE en esta materia, sea, el de la ponderación caso por caso de los derechos e intereses en juego.

a) Hechos

El caso Bavarian Lager tiene como origen la negativa de la CE de brindar acceso completo al acta de una reunión celebrada dentro del marco de un procedimiento de denuncia por incumplimiento de la normativa comunitaria, interpuesto por Bavarian Lager. En razón de que varios de los participantes en dicha reunión se opusieron a la divulgación de sus nombres, o bien, no pudieron ser localizados, la CE dio acceso a Bavarian Lager al acta eliminando dichos nombres. A criterio de la CE, la empresa no demostró ningún objetivo expreso y legítimo, ni la necesidad de la divulgación de los datos solicitados. Asimismo, consideró que la solicitud de acceso a los documentos formulada por Bavarian Lager no cumplía con los requisitos establecidos en el Reglamento 45/2001, que resulta de aplicación vía excepción contenida en el Reglamento 1049/2001.

Por medio de STGUE de 8 de noviembre de 2007, el TGUE declaró que la CE había incurrido en un error de Derecho al declarar que Bavarian Lager no había demostrado un objetivo expreso y legítimo ni la necesidad de obtener el nombre de las personas que participaron en una reunión y que una vez consultadas, se opusieron a la

divulgación de sus datos. Señaló que el Reglamento 1049/2001, el cual resulta de aplicación prevaleciente en materia de acceso a los documentos, permite la publicación de ciertos datos personales y no requiere, en ese sentido, que se exija al solicitante que demuestre la necesidad e interés en la transmisión de los datos.

b) La interpretación armónica de ambos reglamentos

Contrario a lo que resolvió el STPI, el TJUE parte de la consideración de que si bien ambos reglamentos persiguen fines diferentes, al encontrarse el derecho a la protección de datos y el derecho de acceso a los documentos en un mismo plano, no existe una primacía de uno de ellos sobre el otro; por lo tanto, resulta necesario que se garantice la plena aplicación de ambos.

Haciendo una conciliación de normativa que parecía casi imposible por perseguir ambos reglamentos fines opuestos, el TJUE menciona que ambas normas no son excluyentes entre sí y su vínculo expreso se encuentra en la excepción al acceso a los documentos que establece el artículo 4.1.b) del Reglamento 1049/2001, en aquellos casos donde la divulgación de los datos suponga un perjuicio para la intimidad de la persona, según la normativa de protección de datos comunitaria. Esta excepción constituye a criterio del TJUE un régimen específico y reforzado de la persona frente a la eventual divulgación de sus datos de carácter personal[177].

Continúa el Tribunal, explicando que el TPI incurrió en un error de interpretación del Derecho comunitario, pues limitó la aplicación de dicha excepción solo a las situaciones que supusieran una vulneración a la intimidad o la integridad de la persona, según el artículo 8 de la CEDH y la jurisprudencia del TEDH, dejando de lado la consideración de la normativa de protección de datos, como así lo exige la correcta aplicación del Reglamento 1049/2001[178].

De acuerdo con lo anterior y la plena vigencia del Reglamento 45/2001, en casos en los que el tratamiento se efectúa en el ejercicio de actividades pertenecientes al ámbito comunitario, resulta evidente la aplicación en su totalidad de la normativa comunitaria en materia de protección de datos, incluidos los artículos 8 y 18, los cuales se demuestre la necesidad e interés público en la divulgación de los datos, así como la facultad del

[177] STJUE de 29 de junio de 2010, asunto C-28/08 P… apartado 56-57, 60.
[178] *Ibíd.* apartado 58.

interesado de ejercer su derecho de oposición a la divulgación de sus datos[179]. De ahí, que al no haber acreditado la Bavarian Lager la necesidad en conocer los datos a los que pretendía el acceso, corresponde como lo hizo la CE denegar el acceso a los mismos, más aún, cuando habiendo sido consultados los interesados, se negaron expresamente a que sus datos fuesen suministrados, o bien, no pudieron ser localizados.

Concluye el Tribunal que excluir de entrada la remisión a la normativa comunitaria en materia de protección de datos, a través de una interpretación particular y limitativa de la excepción contenida en el artículo 4.1.b) del Reglamento 1049/2001, considera el TJUE no responde al equilibrio que el legislador de la UE quiso establecer entre ambos reglamentos[180].

B. STGUE de 7 de julio de 2011: caso Valero Jordana/Comisión

a) Hechos

En Sentencia, de 7 de julio de 2011, asunto T-161/04 de 7 de julio de 2011 (caso Valero Jordana/Comisión), el TGUE conoció de un recurso de anulación de la decisión de la CE de 10 de febrero de 2004, donde denegó al demandante el acceso a la lista de reserva del concurso general A 7/A 6 COM/A/37 y a las decisiones individuales de nombramiento de funcionarios en el grado A 6 a partir de octubre de 1995. La CE denegó el acceso a dichas decisiones por considerar que estaban incluidas en la excepción relativa a la protección de la intimidad y la integridad de la persona que prevé el artículo 4.1.b) del Reglamento 1049/2001.

b) La necesaria aplicación de ambos reglamentos

En su Sentencia, el TGUE señala que los nombres y los apellidos de las personas que figuran en una lista de reserva de un concurso o de los funcionarios mencionados en las decisiones individuales de nombramiento, son datos de carácter personal y su comunicación constituye un tratamiento de datos, según lo dispuesto en el artículo 2.a) y b), del Reglamento 45/2001, respectivamente. [181]

En segundo lugar, apunta que las solicitudes de acceso presentadas por el demandante, tienen como base el Reglamento 1049/2001, de modo que el litigio versa

[179] *Ibíd.* apartado 62-63.
[180] *Ibíd.* apartado 65.
[181] STGUE (Sala Octava) de 7 de julio de 2011, asunto T-161/04 (caso Valero Jornada/Comisión), apartado 91.

sobre la validez de la respuesta negativa que proporcionó la CE sobre esa misma base jurídica, especialmente, con fundamento en el artículo 4.1.b) del Reglamento 1049/2001, donde prevé una excepción al acceso a un documento cuando su divulgación suponga un perjuicio para la protección de datos de carácter personal.

Al instar la CE al demandante a presentar una nueva solicitud de acceso, con base en el Reglamento 45/2001 ante otro órgano de la institución, no solo obvió el artículo 4.1.b) del Reglamento 1049/2001 que establece el vínculo entre ambos reglamentos, sino que vulneró también las exigencias de una buena administración. En virtud de lo anterior, el TGUE considera que la decisión impugnada es ilegal por cuanto resulta contraria a lo dispuesto en el artículo 4.1.b) del Reglamento 1049/2001.[182]

C. STGUE de 23 de noviembre de 2011: caso Dennekamp/Parlamento I

a) Hechos

Por medio de la Sentencia, de 23 de noviembre 2011, asunto T-82/09 (caso Dennekamp/Parlamento), el TJCE conoció de un recurso de anulación presentado contra una decisión del PE que denegó la solicitud del demandante de acceso a ciertos documentos relacionados con la afiliación a un plan de pensiones por parte de ciertos miembros del PE. El demandante basó el acceso a los documentos en el Reglamento 1049/2001; no obstante, el PE denegó la solicitud de acceso por estimarla incompatible con el Reglamento 45/2001.

b) La obligada justificación y demostración de necesidad en el acceso

EL TJCE indica que ni el Reglamento 1049/2001 ni el 45/2001 contienen disposiciones que otorguen primacía de una norma sobre la otra; por tanto, debe garantizarse la plena aplicación de ambos cuerpos dispositivos. Indica que cuando una solicitud de acceso a documentos que incluyan datos de carácter personal se formula basada en el Reglamento 1049/2001, corresponde también la aplicación del Reglamento 45/2001. En ese sentido, remarca que los nombres de los diputados del PE que tiene por objeto la solicitud de acceso, constituyen un dato personal y su comunicación constituye un tratamiento de datos en el sentido del artículo 2 del Reglamento 45/2001. En razón de

[182] *Ibíd.* Apartados 99-103

lo anterior, resulta aplicable el artículo 8.b) del Reglamento 45/2001 relativa a las solicitudes de acceso a documentos que contienen datos de carácter personal.[183]

Añade el TJUE con respecto a la divulgación de datos personales contenidos en los documentos que solicitó el demandante, que este debió justificar la necesidad de conocer dichos datos, de modo que el PE pudiera haber contado con los elementos necesarios para sopesar los intereses, por un lado, de acceso a los documentos y, por otro, de protección a los datos de carácter personal. En el caso concreto, el demandante no cumplió con esa exigencia de demostrar la necesidad.[184]

D. STGUE de 28 de marzo de 2012: caso Egan y Hackett/Parlamento

a) Hechos

En Sentencia, de 28 de marzo de 2012, asunto T-190/10 (caso Egan y Hackett/Parlamento), el TGUE conoció de un recurso de anulación de la decisión del Parlamento Europeo de negar a los demandantes el acceso a los registros públicos de asistentes de antiguos miembros del PE.

b) El riesgo para la intimidad y protección de datos personales debe ser razonablemente previsible

En primer lugar, en la STGUE el Tribunal señala que ni el Reglamento 1049/2001 ni el Reglamento 45/2001, contienen una excepción o exclusión respecto de los documentos que fueron puestos al público, pero ya no están disponibles; por lo tanto, ambos reglamentos resultan aplicables en el caso concreto.

Por otra parte, el TGUE considera que la justificación de la negativa del Parlamento de conceder el acceso a los documentos que contengan los nombres de las personas que fueron asistentes de miembros del Parlamento Europeo, se expresa en términos generales y no explica por qué la divulgación atentaría contra los intereses de los particulares en materia de privacidad, o por qué la divulgación afectaría los intereses financieros de los asistentes.

Es decir, el PE no realizó el examen debido para demostrar que el acceso a los documentos solicitados causaría un perjuicio específico y efectivo al derecho a la

[183] STGUE de 23 de noviembre de 2011, asunto T-82/09.
[184] *Ibíd.* 44

intimidad y la protección de datos de carácter personal de los posibles afectados. Tampoco verificó si el riesgo del interés protegido era razonablemente previsible o se trataba de un riesgo tan solo hipotético. En virtud de lo anterior, acepta la demanda por cuanto la decisión impugnada vulnera lo dispuesto en el artículo 4, apartado 1, letra b) del Reglamento 1049/2001.

E. STGUE de 11 de junio de 2015: caso McCullough/CEDEFOP

a) Hechos

En Sentencia, de 11 de junio de 2015, asunto T-496/13 (caso McCullough/CEDEFOP), el TGUE conoció de un recurso de anulación contra la decisión del Centro Europeo para el Desarrollo de la Formación Profesional (CEDEFOP) que denegó el acceso a un ex funcionario del CEDEFOP a una serie de minutas del Consejo de Administración y otros órganos, bajo el argumento de que los requería para su defensa en un proceso contra el CEDEFOP, pendiente resolución por los tribunales de justicia griegos. El CEDEFOP negó el acceso a los documentos con base en el artículo 4.1.b) del Reglamento 1049/2001, por considerar que los nombres de las personas que aparecen en la minuta, constituyen datos de carácter personal protegidos por las disposiciones contenidas en el Reglamento 45/2001.

b) Deber de justificar la negativa del acceso a los documentos que contienen datos de carácter personal

En su Sentencia, el TGUE comienza por precisar que de acuerdo con su jurisprudencia, el nombre y apellido de una persona se encuentran cubiertos por el concepto de dato de carácter personal y, por ende, están cubiertos por las disposiciones del Reglamento 45/2001. Señala que dichos datos no pierden su calidad de carácter personal, por ejemplo, por haber participado en los órganos de toma de decisión del CEDEFOP o sus actividades no hayan sido desarrolladas en la esfera privada, sino que sean como resultado de su actividad pública.[185]

Asimismo, el TGUE estima que la necesidad de la comunicación de la información no queda acreditada únicamente por el dicho del demandante, quien justifica la solicitud argumentando que requiere de la información para su defensa en el proceso instaurado ante los tribunales de justicia. El demandante no aportó información ni

[185] STGUE de 11 de junio de 2015, asunto T-496/13, apartado 66.

justificación ante el CEDEFOP ni ante el Tribunal sobre cómo el acceso a los documentos solicitados que contienen datos de carácter personal, puede incidir en el proceso al que se refiere, los riesgos derivados de la revelación de dicha información en un proceso, ni cómo se verían afectados sus argumentos y defensa en caso de no tener acceso a ellos.[186]

Por otra parte, el TGUE señala que las excepciones contenidas en el artículo 4 del Reglamento 1049/2001, en el tanto limitan el principio de máximo acceso a los documentos públicos, deben ser interpretadas de forma restrictiva. Solo procede aplicar las excepciones, cuando se tenga previamente comprobado que el acceso a los documentos sería contrario a los intereses y los derechos que protegen dichas excepciones. Asimismo, el riesgo aducido debe ser razonable y no tan solo hipotético.

Lo anterior implica que la institución que deniegue el acceso a los documentos, debe justificar las razones que le hacen suponer que permitir el acceso a los documentos iría en contra de otros derechos e intereses también salvaguardados por la normativa comunitaria, en especial, cuando se trata de la aplicación del artículo 4.1.b) del Reglamento 1049/2001.[187]

Determina el TGUE que el CEDEFOP no cumplió con las exigencias anteriormente expuestas, pues tan solo señala que el acceso a los documentos que solicita el demandante conllevaría a una violación al derecho a la intimidad y la protección de datos de carácter personal de las personas cuyos nombres figuran en las minutas solicitadas, ya que dichos documentos demuestran los puntos de vista y opiniones de todos los miembros participantes. A criterio del TGUE, no se demuestra cómo dichas opiniones y puntos de vista expresados por los participantes en las reuniones de los órganos de decisión del CEDEFOP pueden ser comprendidas dentro del ámbito de actividad privada de las personas, ni cómo su revelación afectaría la intimidad de los participantes. Tampoco demostró, si bien la solicitud se refiere a una cantidad numerosa de documentos, cómo dichos accesos, en razón de su cantidad, puede vulnerar la intimidad de otras personas.

El TGUE anula la decisión del CEDEFOP de negar el acceso a los documentos solicitados, salvo lo relativo a la revelación de los nombres de los miembros del Consejo de Administración.

---

[186] *Ibíd.* Apartados 69-70.
[187] *Ibíd.* Apartados 82-85

F. STGUE de 15 de julio de 2015, caso Dennekamp/Parlamento II

a) Hechos

Por Sentencia, de 15 de julio de 2015, asunto T-115/13 (caso Dennekamp/Parlamento), el TGUE conoció de un recurso de anulación de la decisión del Parlamento Europeo, que denegó al demandante el acceso a determinados documentos relativos a la afiliación de algunos diputados del Parlamento a un régimen de pensión complementaria. Después de la Sentencia del TGUE de 23 de noviembre de 2011, el demandante presentó una nueva solicitud de acceso a cuatro categorías de documentos referentes al tema del régimen de pensión complementaria de algunos diputados del Parlamento. El demandante basó su solicitud en el interés público por la transparencia y un necesario debate sobre los procesos de toma de decisiones, en especial, conocer quiénes eran los diputados que tenían un interés personal en el régimen de pensiones complementarias.

Asimismo, argumentó la inexistencia de un perjuicio de los derechos e intereses legítimos de los diputados. El Parlamento negó el acceso a tres de las cuatro categorías de documentos, basado en que no se demostró la necesidad de la transmisión de los datos solicitados.

b) Procedencia de la cesión de datos cuando es el único mecanismo para lograr el objetivo de la transparencia

En su Sentencia, TGUE señala que el requisito de necesidad establecido en el artículo 8.b) del Reglamento 45/2001 no puede considerarse una interpretación extensiva de una excepción a derecho fundamental de acceso a los documentos. Es decir, que dicha excepción no crea una excepción de categoría al principio de acceso a los documentos en favor de los datos personales, sino que obliga a una conciliación de ambos derechos, en especial cuando una solicitud de acceso a los documentos versa sobre datos personales. Agrega, además, que la interpretación restrictiva del requisito de necesidad que establece el artículo 8.b) del Reglamento 45/2001, no impide que pueda tomarse como justificación de la transmisión de los datos de carácter personal, el derecho a la información del público en cuanto al comportamiento de los diputados en el ejercicio de sus funciones.[188]

[188] STGUE (Sala Quinta) de 15 de julio de 2015, asunto T-115/13 (caso Dennekamp/Parlamento), apartados 60-61.

Ahora bien, el TGUE estima que la solicitud del demandante de acceso a los documentos, que basa su justificación de la necesidad de la transmisión en el derecho a la información y el derecho a la libertad de expresión, no basta para demostrar que es la medida más adecuada entre otras medidas más factibles, así como que es proporcionada con el objetivo perseguido. El demandante se limitó a indicar que la transmisión de los datos permitirá un control del público sobre los gastos públicos realizados en el marco del régimen de pensiones, mas no señala elementos que permitan determinar de qué modo la transmisión de los nombres de los diputados que están afiliados al régimen complementario de pensiones, es la medida más adecuada y proporcionada para alcanzar el objetivo perseguido. Según lo anterior, el TGUE desestima el argumento del demandante en cuanto a la necesidad de la transmisión de los nombres de los diputados afiliados al régimen con el objetivo de informar al público y generar el debate sobre la legitimidad del régimen.[189]

No obstante lo anterior, el TGUE considera que la necesidad de sacar a la luz los posibles conflictos de intereses de los diputados cuando se pronuncian sobre el régimen, justifica la transmisión de los nombres de los diputados afiliados a él. A juicio del TGUE, la transmisión de los datos constituye la única medida que permite alcanzar el objetivo de determinar la existencia o no de posibles conflictos de intereses, tal y como lo persigue el demandante. Ninguna otra medida distinta a la transmisión de los nombres de los diputados, puede garantizar la identificación de los miembros del Parlamento que se encuentren en una situación potencial de conflicto de interés.[190]

Partiendo de lo anterior, el TGUE anula la decisión del Parlamento en la medida en que deniega el acceso a los nombres de los diputados afiliados al régimen de pensión complementaria que participaron en las votaciones sobre dicho régimen de pensión

G. STJUE de 16 de julio de 2015, caso ClientEarth y PAN Europe/EFSA

a) Hechos

En Sentencia, de 16 de julio de 2015, el TJUE conoció del asunto C-615/13 P (caso ClientEarth y PAN Europe/EFSA), en el cual se solicita la anulación de la Sentencia del TJUE que desestimó un recurso que pretendía la anulación de la decisión del 10 de

[189] *Ibíd.* Apartados 81-83, 87.
[190] *Ibíd.* Apartado 94.

febrero de 2011, por medio de la cual EFSA denegó una solicitud de acceso a ciertos documentos relacionados con una opinión preparada, destinada a los solicitantes de una autorización de comercialización de un producto fitosanitario, así como una pretensión para anular la decisión de EFSA de 12 de diciembre de 2011, que revocó esa decisión y autorizó a ClientEarth y PAN Europe a acceder a todas las informaciones solicitadas, excepto las relativas al nombre de los expertos externos que habían presentado ciertas observaciones al proyecto de opinión.

b) Procedencia de la cesión de datos cuando es el mecanismo idóneo para la consecución del objetivo que persigue la transparencia

EL TJUE considera que de conformidad con lo dispuesto en el artículo 2.a) del Reglamento 45/2001, el concepto de dato personal comprende toda información sobre una persona física identificada o identificable. En este caso, los recurrentes ClientEarth y PAN Europe pretenden conocer quién es, dentro de los expertos externos, el autor de cada observación formulada. A criterio del TJUE, en el tanto dicha información permite atribuir a un determinado experto una observación específica, constituye un conjunto de datos personales que afecta a personas físicas identificadas. Siguiendo su jurisprudencia en los casos Österreichischer Rundfunk y otros, Comisión/Bavarian Lager y Worten, resalta que el hecho de que dicha información se produzca en el contexto de una actividad profesional, no puede privarse del carácter y la calificación de datos personales.

Asimismo, en línea similar a la que se pronunció en el caso Satakunnan Markkinapörssi y Satamedia, estima que tampoco afecta, en el caso concreto, el hecho de que la identidad de los expertos interesados como las observaciones presentadas sobre el proyecto de opinión, se hayan hecho públicas en el sitio de Internet de la EFSA, pues ello no implica que la información relativa al nombre de los expertos haya perdido su condición de dato personal. A criterio del TJUE, tampoco cobra relevancia la falta de oposición a divulgar la información por parte de los interesados, pues esa oposición no es un elemento constitutivo del concepto de datos personales.[191]

De conformidad con el artículo 8.b) del Reglamento 45/2001, los datos personales, en casos de acceso a la documentación al amparo de dicha normativa, solo se transmitirán si el destinatario demuestra la necesidad de que sean transmitidos los datos

[191] STJUE de 16 de julio de 2015, asunto C-615/13 P, apartados 27-33.

y no existen motivos para suponer que dicha transmisión pueda perjudicar los intereses de la persona interesada.

En ese sentido, el TJUE procede a examinar la procedencia de la necesidad argumentada por los recurrentes, por ser este el primer elemento que debe valorar la autoridad a efectos de divulgar los datos personales. Recuerda, al igual que en la sentencia del caso Volker und Markus Schecke y Eifert, que no existe una preminencia automática de la transparencia frente al derecho a la protección de datos de carácter personal; por lo tanto, un argumento en ese sentido para justificar la necesidad de la divulgación de los datos de carácter personal no procede.[192]

Como segundo motivo, los recurrentes aducen la necesidad de conocer los nombres de los expertos, ya que dicha información es necesaria en el contexto para garantizar la transparencia en el proceso de adopción de un acto que iba a repercutir en las actividades de ciertos operadores económicos. En ese sentido, a criterio de los recurrentes resulta necesario conocer en qué grado cada uno de los expertos pudo influir en el contenido del acto a través de su opinión científica. Esto, en un ambiente de desconfianza hacia la EFSA, que a menudo se le acusa de parcialidad por la contratación de expertos con intereses personales derivados de vínculos con medios empresariales, hecho que fue acreditado mediante un estudio que ponía de manifiesto la situación.

El TJUE considera que si bien los recurrentes fueron informados del nombre, la biografía y las declaraciones de intereses de expertos que formularon las observaciones sobre el proyecto de opinión, la obtención de los datos resultaba necesaria para comprobar, en concreto, la imparcialidad de cada uno de los expertos en el cumplimiento de sus funciones al servicio de la EFSA.[193]

Por último, en relación con la posición de la EFSA de no transmitir los datos porque puede perjudicar el interés protegido, el TJUE considera que aducir que la divulgación de la información habría podido perjudicar la intimidad e integridad de los expertos, sin mayor sustento y pruebas, constituye una alegación de carácter general que no procede. En todo caso, considera que dadas las circunstancias, haber facilitado la información habría permitido comprobar o no las sospechas de parcialidad, o habría ofrecido a los expertos potencialmente afectados la ocasión para contestar las alegaciones

[192] *Ibíd.* Apartados 44-45, 51.
[193] *Ibíd.* Apartados 53-58.

de parcialidad. Aceptar alegaciones abstractas sobre la posible existencia de un perjuicio a la intimidad e integridad de las personas interesadas, puede permitir que sea aplicada de manera general, lo cual contravendría la exigencia de interpretación estricta de las excepciones del derecho de acceso a los documentos en poder de las instituciones europeas, que exige sea comprobado la existencia del riesgo y el prejuicio del interés protegido.[194]

3. Las claves para la solución del conflicto según la jurisprudencia del TJUE

El TJUE ha tenido un papel importante en la delimitación de las relaciones existente entre la transparencia y la protección de los datos personales en el marco normativo comunitario a través de su jurisprudencia, la cual ha partido de la premisa de que ninguno de los dos derechos es absoluto y su interacción y relación depende, en cada caso concreto, de una ponderación entre los derechos e intereses en juego. Esta posición está en consonancia con la de las demás instituciones comunitarias que han señalado la ponderación como mecanismo de solución, sin posturas radicalizadas que sacrifiquen uno u otro derecho.[195]

Al igual que con el desarrollo del derecho a la protección de datos personales a la luz de la Directiva 95/46, el TJUE ha tenido un papel preponderante en la delimitación de las relaciones existente entre la transparencia y la protección de los datos personales en el marco normativo comunitario. Es importante tener en consideración en todo

[194] *Ibíd.* Apartados 69-70.

[195]Para algunos autores como GUICHOT REINA, las tensiones de esta relación no se generan por el hecho de tener que ponderar derechos e intereses en juego, sino por la aplicación del concepto de dato de carácter personal por parte del TJUE. En ese sentido, apunta que: "hemos podido comprobar cómo todas las instituciones consideran que se trata de una cuestión de enfrentamiento entre derechos fundamentales que debe resolverse en clave de ponderación, sin posiciones maximalistas que sacrifiquen por completo el derecho de acceso y la transparencia (de modo que ningún documento en el que figure el nombre de una persona pueda ser conocido por el resto de los ciudadanos) ni el derecho a la intimidada y a la protección de datos (de manera que los ciudadanos puedan conocer cualquier información de terceros, del tipo que sea). Todas entienden que la solicitud de información por un tercero debe resolverse mediante el procedimiento establecido en la normativa sobre acceso. Los principios establecidos en la normativa sobre protección de datos, coinciden, debe no obstante ser respetados en interpretación de la normativa sobre acceso. Al respecto, todos consideran que la información que afecta datos sensibles debe ser la más reacia a la publicidad, mientras que la comercial o profesional (incluida la relativa a empleados públicos), debe ser pública, salvo que haya causas excepcionales que lo justifiquen. Y, por último, si bien la normativa no lo prevé, todos consideran –salvo, al menos de forma expresa, el TPI- que para una correcta ponderación debe darse entrada a las consideraciones que pueda efectuar el solicitante de información y el afectado, sin que no obstante exista un derecho de veto por parte del afectado, esto es, se exija su consentimiento. Si hay ese acuerdo, en el fondo, ¿cuál es el origen de la discrepancia de razonamientos? Un elemento clave de distancia es el propio concepto de "dato personal y su integración o no en el concepto de "intimidad". Ver en: Guichot Reina, E. (2011). Las relaciones entre transparencia y privacidad en el Derecho comunitario ante la reforma de la normativa sobre acceso a los documentos públicos. *Revista Española de Derecho Europeo*, núm. 37, enero-marzo, 2011, pp. 37-69.

momento que el derecho a la protección de datos, al igual que cualquier otro derecho del ordenamiento jurídico no es absoluto, por lo que se ha hecho necesaria su precisión en relación con los otros intereses que tutelados en la normativa comunitaria, con el fin de llegar a una solución adecuada sin sacrificio o desconocimiento de ningún derecho.

A. La necesaria justificación del acceso y la ponderación de derechos e intereses

El TJUE ha fijado desde sus primeras sentencias la ponderación como parámetro para la solución de los conflictos[196] que se presentan entre transparencia, acceso a la información y protección de datos personales, partiendo de la idea de que "la limitación de los derechos fundamentales sólo podrá llevarse a cabo de acuerdo con el principio de proporcionalidad, pues se hace necesario proceder a una ponderación[197] de los respectivos intereses que permita alcanzar la compatibilidad, el equilibrio y la coordinación adecuada de varios e, incluso, de contradictorios, principios normativos".[198]

Es a través de esta ponderación, "como discurso jurídico a través de cual se resuelven las colisiones entre principios"[199] que el TJUE entiende se cumple la máxima de que no existe una primacía absoluta de la transparencia y el derecho de acceso a los documentos sobre el derecho a la protección de datos personales o viceversa, y que corresponde, caso por caso un análisis detenido para determinar cuál priva sobre el otro cuando entre en conflicto. Lo anterior, bajo la premisa de que atribuir primacías

[196] VILLAVERDE MENÉNDEZ considera, que más que conflictos o colisiones de derechos se trata de una colisión entre el derecho y sus respectivos límites. Inclusive, apunta que es erróneo hacer alusión a conflictos o colisiones, puesto que los "límites de un derecho fundamental no colisionan con él, sino que justamente sirven para solventar sus posibles colisiones con otros derechos, bienes e intereses". En ese sentido, se puede apreciar que la labor del TJUE prácticamente consiste en la aplicación de los límites al derecho de acceso a los documentos en razón de la protección de la intimidad y datos de carácter personal, como mecanismo de solución del –mal llamado a criterio de Villaverde- conflicto entre ambos derechos. Villaverde Menéndez, I. (2004). La resolución de conflictos entre derechos fundamentales. El principio de proporcionalidad. En F. Bastida Frejiedo (Ed.) Teoría general de los derechos fundamentales en la Constitución española de 1978. Madrid: Tecnos. pp. 175-187. En un sentido similar RODRÍGUEZ BOENTE menciona que la ponderación coadyuva a conocer los límites de los derechos. En: Rodríguez Boente, S.E. (2003). Ponderación y "reglas" de derechos fundamentales: dos enemigos conciliables. *Dereito*, Vol. 12, núm. 2, pp. 137-160.

[197] Para ATIENZA RODRÍGUEZ, la ponderación opera cuando concurran en alguno de los tres escenarios: cuando no hay una regla que regule el caso (existe una laguna normativa en el nivel de las reglas), existe una regla pero, por alguna razón, la misma resulta inadecuada, o bien, es dudoso si existe o no una regla que regule el caso. El caso del derecho comunitario y la solución del conflicto de transparencia, acceso a los documentos y protección de datos, parece que se ubica en el primer escenario, pues hay un vacío o laguna normativa que hace necesario recurrir a la ponderación para resolver cada caso concreto. Ver: Atienza Rodríguez, M. (2010). A vueltas con la ponderación. *Anales de la Cátedra Francisco Suárez*, núm. 44. (2010). pp. 43-59.

[198] Del Castillo Vásquez, I. (2007). Transparencia, acceso a la documentación administrativa y protección de datos de carácter personal. *Foro, Nueva Época*, núm. 6/2007. pp. 231-254,

[199] Arroyo Jiménez, L. (2009). Ponderación, proporcionalidad y Derecho administrativo. *Indret: Revista para el Análisis del Derecho*, núm. 2/2009. Recuperado de: www.indret.com

automáticas, únicamente conlleva a lesiones automáticas de los derechos fundamentales en juego.

Asimismo, refuerza su postura frente a las innecesarias posiciones poco matizadas que, en un caso de primar el derecho a la protección de datos de forma absoluta, conducen al secretismo, o que por conceder el acceso a los documentos sin mayor reparo de la afectación de otros derechos o intereses, como la protección de datos, conducen a prácticamente la desaparición del derecho a la privacidad y la intimidad de los ciudadanos en su relación con la Administración Pública, en este caso, con las instituciones comunitarias.

La ponderación, como forma de decidir[200] que utiliza el TJUE en su jurisprudencia busca ser a la vez garante de la institucionalidad democrática de los organismos comunitarios, a través de la transparencia y el ejercicio del derecho de acceso a los documentos, pero también persigue la garantía y vigencia de otros derechos fundamentales como lo es también la protección de datos personales, ponderación que se ha encargado de señalar debe realizarse a todo nivel, desde el ejercicio del derecho de acceso por medio de una solicitud, hasta la aprobación de reglamentos o directrices que pretendan imponer limitaciones a los derechos fundamentales.

De la jurisprudencia del TJUE, podemos observar como en su primer sentencia dictada en la materia, la STJUE del caso Bavarian Lager/Comisión[201], el Tribunal marcó su línea jurisprudencial del Tribunal y condicionó la resolución de los demás casos[202] presentados a la doctrina sentada en esa ocasión: la obligatoriedad de demostrar la necesidad del acceso a documentos que contienen datos de carácter personal, así como la

[200] Rodríguez de Santiago, J.M. (2000). La ponderación de bienes e intereses en el derecho administrativo. Madrid: Marcial Pons. p. 10.
[201] STJUE de 29 de junio de 2010, asunto C-28/08 P…
[202] Es importante apuntar que la línea jurisprudencial mencionada, como bien lo HIJMANS, ha sido mantenida no únicamente en relación con el derecho de acceso a los documentos públicos sino también en casos en que la normativa comunitaria pretendía garantizar la transparencia mediante la adopción de obligaciones de publicidad activa. Así por ejemplo, en el caso Volker Markus und Shecke & Eifert, el TJUE –en aplicación directa de la CDFUE- resolvió que previó al establecimiento de obligaciones que requieran a los Estados miembros el establecimiento de exigencias que impliquen la publicación periódica en Internet de ciertos datos de carácter personal de ciudadanos que reciben ayudas de un fondo agrícola de la UE, debe ponderarse si existen medidas menos gravosas que permitan garantizar el mismo fin sin que el ciudadano pierda el control de sus datos personales Ver en: Hijmans, H. (2016). The European Union as guardian of internet privacy: the story of art 16 TFUE. Law, Governance and Technology Series (Vol. 31). Springer: Bruselas. pp. 238-239.

obligatoria ponderación de dicha necesidad, caso por caso, previo a conceder el acceso al documento que los contenga, patrón que ha sido recurrente en todos los casos.

En dicha STJUE, el Tribunal se encargó de conciliar aspectos del Reglamento 45/2001 sobre protección de datos y el Reglamento 1049/2001 sobre acceso a la información pública que parecían de primera entrada irreconciliables y dispuso que si bien se permite el acceso a los documentos que estén en poder de las instituciones europeas, cuando el documento contenga datos de carácter personal, debe demostrarse la necesidad de que los datos sean transferidos con el fin de conceder el acceso a dicha información.

En esta primer sentencia, el TJUE llama a una ponderación caso por caso y estima que en la aplicación de ambos reglamentos, necesario que se deba justificar la solicitud de acceso con el fin de que, en ese caso, la CE, dispusiera de todos los elementos necesarios con el fin de poder decidir –ejercicio de ponderación-, si existían o no motivos para suponer que conceder el acceso a la información podía causar un perjuicio objetivo al derecho a la intimidad y la protección de datos de los interesados, y resalta, como lo haría después en otros casos, que la simple invocación del principio de transparencia no resulta suficiente para justificar el acceso a la información que contiene datos personales.

En consecuencia, el TJUE fija como parámetro en esta sentencia que se debe establecer por parte del solicitante, la necesidad de que el acceso a los documentos o la información sea concedido, mientras que quien tiene en su poder la información, debe valorar, en cada caso, sin con el acceso a los documentos causa un perjuicio objetivo a la intimidad y los datos personales de los interesados, o si por el contrario, cede este derecho ante el interés público o la inexistencia de la lesión que revista el acceso. Y lo anterior, a juicio del TJUE sólo puede lograrse, cuando quien solicita el acceso a la información ha justificado su solicitud.

Para la resolución de este caso fueron clave las conclusiones emitidas por la Abogado General Sharpston, quien de forma enfática manifestó en todo momento que le derecho de acceso a la información así como el derecho a la intimidad y a la protección de datos se encuentran en un mismo rango, por lo que la solución a la que se llegue en estos casos no puede ignorar la existencia de ninguno de os dos derechos ni mucho menos, dar prioridad absoluta a alguno, sino que por el contrario, corresponde en estos casos

ponderar los intereses en juego y buscar un equilibrio que no conduzca, a lo que considera, una solución con una elección injusta.

Para algunos autores como GARCÍA MACHO, de la STJUE caso Bavarian Lager/Comisión "se puede concluir que se trata, en principio, de una sentencia ponderada, puesto que se respeta el derecho de información de la empresa demandada, al no ser relevantes los datos personales que se solicita, pero también se salvaguarda el derecho a la protección de datos personales de las personas concernidas, que no quieren que esos datos se hagan públicos".[203]

No obstante lo anterior, la doctrina fijada en esta primera sentencia del TJUE no ha sido del todo pacífica y ha levantado críticas entre diferentes autores quienes estiman que en el fondo debe prevalecer el derecho de acceso a los documentos y que exigir que se demuestre la necesidad en la cesión de los mismos puede llegar a constituir un lastre en la consecución del fin de la transparencia que se persigue con el ejercicio del derecho de acceso a la información. Asimismo, hay quienes estiman que desde esta sentencia queda en evidencia que la ponderación a la que llama el TJUE, sobre una base de igualdad de los derechos en la realidad es distinta, pues en la práctica ha quedado demostrado que generalmente prevalece el derecho a la protección de los datos personales sobre el derecho de acceso a la información pública.[204]

---

[203] García Macho, R. (2012). La transparencia en el sector público. En A. B lasco Esteve, *El Derecho público de la crisis económica. Transparencia y sector público. Hacia un nuevo derecho administrativo. Actas del VI Congreso de la Asociación Española de Derecho Administrativo*. Madrid: INAP. Recuperado de: http://www.marcialpons.es/libros/el-derecho-publico-de-la-crisis-economica-transparencia-y-sector-publico-hacia-un-nuevo-derecho-administrativo/9788473514194/.

[204] A este respecto, autores como HIJMANS advierten que desde este momento se pone de manifiesto que no siempre la ponderación entre transparencia y protección de datos se hace en condiciones de igualdad, haciendo alusión a la aparente primacía que da el TJUE al derecho a la protección de datos de carácter personal sobre el derecho de acceso a los documentos. Ver en: Hijmans, H. (2016). The European Union as guardian of internet privacy: the story of art 16 TFUE. Law, Governance and Technology Series (Vol. 31). Springer: Bruselas. pp. 238-239. También RAMS RAMOS indica que es innegable que el TJUE ha sido "más proclive a la defensa de los datos de carácter personal que al recnocimiento del derecho de acceso a los datos que lo contienen". Se puede consultar en Rams Ramos, L. (2016). Tratamiento y acceso público a documentos oficiales... op. cit. *pp. 601-619.* Resulta también especialmente crítica BALLESTER MARTÍNEZ, quien menciona en relación con la sentencia del caso Bavarian Lager que las consecuencias que produzca pueden ser catalogadas como "desastrosas para el principio de transparencia. Esto, por cuanto a su criterio, así como el TJUE estimó que la compañía no demostró la necesidad en el acceso, pudo haber decidido que la CE tampoco tuvo los elementos necesarios para favorecer o inclinar la balanza hacia el derecho a la protección de datos personales, más aún, teniendo en consideración que a su juicio Bavarian Lager no estaba en la obligación de demostrar la necesidad. : "Las consecuencias de esta sentencia pueden ser desastrosas para el principio de transparencia. Concluye que "a la luz de este análisis, parece que el principio de transparencia y apertura que el Reglamento 1049/2001 pretende consagrar y defender puede verse seriamente limitado por la interpretación jurisprudencial que de las excepciones se haga. De hecho, la sentencia Bavarian Lager nos muestra a un Tribunal de Justicia condescendiente con la Comisión y reticente a ampliar la aplicación del principio de transparencia, favoreciendo el otro interés jurídico en juego

En la sentencia seguida a la del caso Bavarian Lager/Comisión, la STGUE del caso Valero Jordana/Comisión[205], en un sentido similar a uno de los extremos reconocidos en la sentencia del caso Bavarian Lager/Comisión, recuerda que no se puede obviar el vínculo que existe entre ambos reglamentos comunitarios –el de acceso a los documentos y el de protección de datos- siendo que se deben aplicar de forma conjunta, lo que como ya vimos en el caso Bavarian Lager, conduce a que cuando se esté ante el acceso a documentos que contienen datos de carácter personal, se requiera al solicitante que acredite la necesidad del acceso, con el fin que la institución u organismo comunitario pueda llevar a cabo la ponderación de bienes e intereses, y pueda decidir, si en el caso concreto, procede el acceso a la información o por el contrario, la denegación con el fin de tutelar el derecho a la protección de datos personales.

Posición que se ve reforzada en el caso Dennekamp/Parlamento I, en el que el TJUE precisa que las disposiciones contenidas en ambos reglamentos deben garantizarse la aplicación de ambos cuerpos normativos, pues no existen disposiciones que otorguen una primacía a uno de ellos sobre el otro. Ello, conlleva al GJUE a desestimar el recurso de anulación bajo el argumento de que no se justificó por parte del solicitante la necesidad del acceso, de forma que se hubiera permitido al Parlamento valorar o sopesar los intereses por un lado, de acceso a la información, y por otro, el derecho a la protección

(en consonancia con las reticencias que la revisión del Reglamento 1049/2001 suscita a día de hoy en las instituciones. En segundo lugar, es también reseñable el hecho de que el Tribunal General haya intentado por todos los medios a su alcance primar la transparencia y que el Tribunal de Justicia haya anulado dichos intentos". Ver en: Ballester Martínez, B. (2011). La forja jurisprudencial del principio de transparencia. *Teoría y Realidad Constitucional, núm. 28, 2011*. pp. 383-406. Sobre este particular, ADAMSKI coincide con las dos posiciones anteriores y considera que la posición del TJUE da mucho margen a las instituciones para que se inclinen a favor de la protección de datos personales, especialmente en las negociaciones con quienes realizan algún tipo de lobby ante las instituciones comunitarias. Es interesante la posición de este autor, quien considera que el TJUE debió precisar que no se requiere exigir que se compruebe la demostración de la necesidad del acceso a los datos cuando del contexto se pueda desprender la misma. Ver en: Adamski, D. (2014). Access to documents, accountability and the rule of law – do private watchdogs matter? *European Law Journal.* Vol. 20, No. 4, July 2014. pp. 520-543. Posición similar manifiestan LEPPÄRVIRTA Y DARBISHIRE, quienes señalan su preocupación en torno a la exigencia de la obligatoria acreditación de la necesidad en el acceso como requisito indispensable para la entrega de la información. Se pude consultar en: Leppärvita, L.; Darbshire, H. (2017). The right to ask… the right to know – the successes and failures in Access to documents rules and practices from an NGO perspective. En C. Harlow et al (Eds.) Research Handbook on EU Administrative Law. Massachusetts: Elgar pp.400-423. BOEHM, apunta que el uso inadecuado que se pueda dar a los argumentos de protección de datos para limitar el acceso a documentos públicos, en el sentido de supremacía que le da la STJUE del caso Bavarian Lager/Comisión, es un riesgo potencial y va en detrimento de la transparencia. En: Boehm, F. (2012). Information Sharing and Data Protection in the Area of Freedom, Security and Justice. Towards Harmonized Data Protection Principles for Information Exchange at EU-level. Brusleas: Springer. p. 168.

[205] STGUE de 7 de julio de 2011, asunto T-161/04.

de datos personales, incumpliéndose así la normativa comunitaria y además, la línea jurisprudencial forjada en relación con la ponderación y la demostración de la necesidad.

Posteriormente, el TGUE reflejó dicha doctrina en la STGUE del caso Dennekamp/Parlamento Europeo I[206], en el que indicó que la simple invocación de la transparencia y el derecho de toda persona de conocer la información que está en poder de las instituciones europeas no justifica por sí sola el acceso a documentos que contengan datos de carácter personal, sino que debe además debe demostrarse la necesidad en que se revelen datos de carácter personal, haciendo así una vez más énfasis en la inevitable demostración de la necesidad en el acceso como único mecanismo para poder llevar a cabo la ponderación a la que ya había hecho referencia en la STJUE del caso Bavarian Lager.

Siempre en esa línea, ya centrado en lo que se refiere al ejercicio de ponderación, después de dejado claro el mandatorio parámetro de acreditación de la necesidad en el acceso, el TJUE ha estimado que las denegaciones de acceso a la información que se fundamenten en el límite del acceso por motivos de protección de la intimidad y datos personales, no pueden ser peligros hipotéticos, sino que debe existir un peligro razonable o concreto a dichos derechos de los supuestos afectados. No procede, como lo hizo el Parlamento en el caso Egan Hackett/Parlamento[207], hacer alusión de forma hipotética a un supuesto perjuicio a los derechos de los posibles afectados. Debe, *contrario sensu*, demostrarse que existe un daño razonablemente previsible si se concede el acceso.

Del otro lado, ha estimado también que la acreditación de la necesidad del acceso debe sostenerse en pruebas y argumentos sólidos que permitan ponderar a la institución y organismos comunitarios si procede conceder el acceso a la información. En ese sentido, son claras dos sentencias. En la STGUE del caso McCullough/CEDEFOP[208], pese a que el solicitante de la información acusa que el acceso a la misma es necesario para ser aportada en un proceso pendiente de resolución ante los Tribunales de Justicia, el TGUE estimó que l la necesidad del acceso no quedaba lo suficientemente acreditada, en el tanto el solicitante no aportó información o justificación alguna, ante el CEDEFOP ni ante el TJUE, de cómo el acceso a los documentos solicitados podían incidir en el proceso pendiente de resolución ni cuáles serían las consecuencias de no aportarlos al mismo. Esta

[206] STGUE de 23 de noviembre de 2011, asunto T-82/09.
[207] STGUE de 28 de marzo de 2012, asunto T-190/10.
[208] STGUE de 11 de junio de 2015, asunto T-496/13.

falta de información, impedía al CEDEFOP poder llevar a cabo el ejercicio de ponderación necesario con el fin de determinar si se concedía o no el acceso a la información.

En ese sentido, similar es la posición del TGUE en el caso Dennekamp/Parlamento II[209], en el que consideró que la simple invocación del interés público por la transparencia y la libertad de expresión no permiten acreditar por sí solos la necesidad del acceso a la información solicitada. Tampoco aportó el demandante, a criterio del TJUE, los elementos necesarios que permitieran ponderar a la institución comunitaria que el fin perseguido sólo era factible de conseguirse mediante el acceso a la información solicitada, o siquiera, que esta era la medida más proporcionada respecto del fin perseguido. No obstante lo anterior, y de la justificación dada ante el TGUE, el Tribunal considera que la necesidad de sacar a la luz pública determinados conflictos de intereses que puedan existir entre algunos diputados del Europarlamento sobre la adopción de posiciones en determinados casos que deben decidir, justifica que se conceda el acceso solicitado sobre la información de la participación en votaciones y el voto de cada uno de ellos. Es decir, que en casos en que la única manera de alcanzar el objetivo de la transparencia sea la transmisión de datos de carácter personal, como en este caso, previa ponderación, cede dicho derecho frente a la transparencia y el acceso a la información.

En otro caso similar, relacionado con el control de la ciudadanía de los procesos de toma de decisiones[210] (STJUE del caso ClientEarth y PAN Europe/EFSA[211]), el TJUE determinó una vez más que la alegación de la protección de datos como límite al acceso a la información debe hacerse ante la existencia de un daño y perjuicio concreto a este derecho y no con base en una suposición. Además, previo ejercicio de ponderación, determinó que procedía el acceso por parte del solicitante a los nombres de expertos de la EFSA, pues el ambiente de desconfianza, en varias veces cuestionado, en el que se encuentra sumergido dicha agencia comunitaria, justifica la necesidad de la transmisión de los datos, pues es la única forma en que se puede controlar la acusada parcialidad de los expertos debido a su vínculo con medios empresariales, hecho que se acreditó

[209] STGUE de 15 de julio de 2015, asunto T-115/13.
[210] Pecsteen, E. (2015). Public Access to documents: effective rear guard to a transparent EU?. Recuperado de: https://europeanlawblog.eu/2015/12/30/public-access-to-documents-effective-rear-guard-to-a-transparent-eu/
[211] STGUE de 16 de julio de 2015, asunto C-615/13 P.

mediante un estudio que aportó el solicitante y en el que se dejaba constancia de esta situación.

Más adelante, en la sentencia del caso ClientEarth y PAN Europe/EFSA, en el que se solicitaba el acceso a nombres de expertos de la EFSA decidió que cuando se alegue la protección de datos como límite al acceso a la información, debe hacerse ante la existencia de un daño y perjuicio concreto a este derecho y no con base en una suposición o hipótesis.

Ambos casos, Dennekamp I y EFSA están ampliamente ligados con el control de la ciudadanía de los procesos de toma de decisiones, ya sea mediante el conocimiento del nombre de expertos de un agencia comunitaria, a efectos de conocer si ha habido presiones que influyeran en la opinión técnica o bien, mediante el conocimiento de parlamentarios que participaron en la votación de temas en los que tienen interés directo.

Resulta entonces claro, de la jurisprudencia mencionada, que la clave de solución a la colisión entre transparencia, acceso a los documentos y protección de datos personales, se encuentra en la siempre necesaria ponderación de derechos e intereses en juego. Para poder sopesar estos derechos e intereses, debe indagar "qué valor o interés último persiguen y dando valor preferente en el caso concreto a aquella expectativa que persigue el valor o interés más cualificado o importante (…) Para esta técnica no es necesario jerarquizar los derechos según el caso concreto y conforme un orden de valores o interés preferente en cada situación, sino examinar sus recíprocos límites y constatar cuál de las expectativas de conducta solapadas no está privada de protección".[212]

B. La metodología de la ponderación seguida por el TJUE

En la práctica y según se desprende de las sentencias explicadas, el TJUE sigue un modelo de ponderación similar al que explica el profesor RODRÍGUEZ DE SANTIAGO[213], y que consiste en prácticamente tres fases: la primera de ellas, la identificación de los principios en conflicto, la segunda, correspondiente a la atribución de peso a cada uno de los principios en conflicto, en atención a las particularidades de cada caso en concreto, y por último, la tercera, que se corresponde con el juicio de prevalencia de uno sobre el otro.

[212] Villaverde Menéndez, I. (2004). La resolución de conflictos entre derechos fundamentales... *op.cit.* pp. 175-187.
[213] Rodríguez de Santiago, J.M. (2000). La ponderación de bienes e intereses… *op. cit.* p. 121-141.

a) La identificación de los derechos o intereses en conflicto

La primera fase, que es una de las más importantes según la metodología del profesor RODRÍGUEZ DE SANTIAGO[214], resulta claramente identificable en todos los casos, en los que el TJUE hace la relación entre la normativa existente y la subsunción de los derechos o interese en conflicto dentro de esta.

Esta delimitación, en primer lugar se debe hacer, como lo hace el TJUE delimitando si existe un dato de carácter personal comprendido dentro del ámbito de aplicación del Reglamento 45/2001, y seguidamente, si existe un documento al que se solicita acceso, bajo el entendido del Reglamento 1049/2001. Nótese que la importancia de identificación de los derechos o intereses en conflicto dentro de una norma viene dada por sí sola, pues la incorrecta categorización de un derecho dentro de una norma, puede llevar a que finalmente sopese el otro derecho.

b) La atribución de un valor o peso a los derechos en conflicto

Seguidamente, identificados los derechos e intereses que están sobre la mesa, corresponde según la metodología mencionada, y que también sigue en la práctica el TJUE, atribuirle a cada uno de ellos el peso que corresponde en función con el contexto concreto. En la jurisprudencia del TJUE esto se ve traducido en el reconocimiento que hace en sus casos de la necesaria protección del derecho a la intimidad y a la protección de datos de carácter personal, como derecho fundamental –especialmente después del Tratado de Lisboa- dentro de una sociedad democrática y libre, pero también en el reconocimiento del valor e interés que tiene para la institucionalidad democrática la plena vigencia del principio de transparencia y la concreción del derecho de acceso a los documentos como mecanismo para perseguir dicho fin.

Esto conecta a su vez con la posición del TJUE que requiere justificar el acceso a los documentos cuando los mismos contengan datos de carácter personal, porque a su juicio, sino se acredita el interés de la persona en el acceso, es imposible que se pueda atribuir un peso al derecho de acceso y por ende resulta inviable la ponderación que sugiere en la mayoría de sus casos. Esto, no obstante, genera conflictos, pues las teorías vigentes de derecho de acceso a la información sostienen que no resulta necesario por parte del solicitante acreditar el interés en el acceso, pero al menos en la práctica del

[214] *Ibíd.* p. 127.

TJUE, la necesidad de la justificación viene dada por la normativa vigente en la materia (artículo 4.1.b) del Reglamento 1049/2001 y artículo 8.c) Reglamento 45/2001) pero también como requisito indispensable para la ponderación.

Es decir, que al menos bajo la normativa comunitaria y la jurisprudencia del TJUE, si no se acredita el interés en el acceso por parte del solicitante, resulta imposible poder llevar a cabo la ponderación. Inclusive, si se observa con detenimiento la jurisprudencia del Tribunal en esta materia, la mayoría de recursos han tenido como objeto el análisis de la falta de acreditación de la necesidad en la transmisión de los datos personales y sólo en aquellos casos en que ha sido evidente la necesidad, porque así ha sido demostrado por medio de pruebas fehacientes ante el TJUE, se ha concedido el acceso a los datos personales que constan en los documentos públicos.

Para Rodríguez de Santiago, en esta fase "se trata de formular argumentos sobre el grado de incumplimiento del principio que en la tercera fase se hará retroceder y sobre la importancia del cumplimiento del principio al que se le otorgará la prevalencia, para lo que hay que introducir datos fácticos y jurídicos relevantes que fundamenten la corrección argumentativa".[215]

c) El juicio de prevalencia

Definido el peso que le corresponde a cada derecho, corresponde hacer el juicio de prevalencia de un derecho sobre el otro, que consiste básicamente en determinar cuál de los derechos debe ceder ante la mayor importancia del otro derecho. En la jurisprudencia analizada, el TJUE se ha encargado de dar una prevalencia en la mayoría de los casos al derecho a la protección de datos de carácter personal, ante la ausencia de una justificación que permitiese al órgano decisor determinar si en el caso concreto, el derecho a la protección de los datos personales cedía ante el derecho de acceso a los documentos.

No obstante, en razón de algunas de las críticas a la jurisprudencia, que están más relacionadas con una disconformidad con la normativa comunitaria vigente que exige la demostración de la necesidad en el acceso cuando el documento contenga datos personales, debe aclararse que el TJUE ha sido enfático, a la hora de ponderar, en reconocer que no procede la alegación en abstracto del perjuicio a la intimidad o la

[215] *Ibíd.* p. 134.

protección de datos personales, y que en aquellos casos en que se acredite la necesidad en el acceso como medio para la consecución del fin que persigue la transparencia, procede la cesión de los datos frente a la protección de los mismos, lo que parece una situación bastante equilibrada en la tutela de ambos derechos.

Recapitulación

Desde su primer sentencia en el caso Bavarian/Lager, el TJUE ha mantenido una línea clara constatable en sus sentencias en lo que se refiere a la solución del conflicto que suscita la relación entre la transparencia, el acceso a los documentos y la protección de datos de carácter personal.

Partiendo de que ambos derechos están en un plano de igualdad y la inviabilidad de atribuir una primacía automática de uno sobre el otro, porque ello conlleva a lesiones injustificadas de cualquiera de los dos derechos, ha encontrado como solución la ponderación caso por caso de los derechos e intereses en juego: en el particular, la ponderación entre el derecho a la protección de datos personales y el derecho al acceso a los documentos, ambos plena y ampliamente tutelados en el ordenamiento comunitario.

Con el fin de poder llevar a cabo la ponderación sobre una base de igualdad, que algunos autores cuestionan porque en la práctica generalmente priva el derecho a la protección de datos, el TJUE entiende que se deben buscar las relaciones entre ambos derechos en la normativa vigente, llegando así a la conclusión de que el Reglamento 1049/2001, contiene una excepción en relación con los datos de carácter personal que remite a la aplicación del Reglamento 45/2001, que una vez analizado, requiere que se acredite y justifique la necesidad en la transmisión de los datos a lo que se solicita el acceso. Y con el fin de garantizar una igualdad entre ambos derechos para poder llevar a cabo la ponderación, en todos los casos se debe garantizar la plena vigencia de ambas normas, sin que exista la posibilidad de inaplicar alguna de las dos en claro detrimento del derecho que tutelan.

Ello nos lleva a un segundo factor al que el TJUE le atribuye plena importancia para poder llevar a cabo la ponderación por medio de la cual se

puede resolver el conflicto de ambos derechos y es la demostración de la necesidad en el acceso a los datos personales. Esto, por cuanto la normativa lo exige y además, porque a su criterio, sino se motiva o se explica la necesidad de la transmisión de los datos personales, no resulta factible poder atribuir un peso en la ponderación al acceso a los documentos para sopesarlo frente al derecho a la protección de datos de carácter personal.

En la búsqueda de ese equilibrio, ha precisado que no procede la invocación hipotética de un daño al derecho a la intimidad y a la protección de datos personales, así como que la simple y genérica invocación del principio de transparencia y la libertad de expresión no resulta suficiente para justificar y demostrar la necesidad en el acceso a los datos.

Por el contrario, ha entendido que cuando se acredita la necesidad de la transmisión de los datos personales, mediante informes o pruebas que demuestren, que la única forma de conseguir el objetivo que persigue la transparencia es el acceso a los datos personales –como por ejemplo, acceder a los nombres de expertos con el fin de conocer las opiniones que han emitido en una agencia comunitaria que constantemente es cuestionada por su parcialidad y ello se acredita con un informe-, procede conceder el derecho de acceso a los documentos y cede el derecho a la protección de los datos personales.

La ponderación como solución al conflicto entre transparencia y protección de datos personales parece ser una de las más adecuadas, aún y cuando ello pueda conllevar críticas según del lado en el que se incline la balanza en cada caso concreto. Hay otras formas de solucionar el conflicto, como lo es el caso español, en el que la LTAIBG, si bien termina declinándose por una ponderación entre derecho –cuando no se trate de datos especialmente protegidos según la LOPD o datos meramente identificativos que puedan suponer un perjuicio para la intimidad y los datos personales-, expresamente menciona una serie de criterios objetivos de ponderación que el aplicador de la norma puede tener en consideración a la hora en que deba llevarla cabo.

Tercera parte

Transparencia, acceso a la información y protección de datos en España

Capítulo V. El derecho a la protección de datos en España

SUMARIO: 1. Cuestiones preliminares. 2. El derecho a la protección de datos en España. 3. La creación jurisprudencial del derecho a la protección de datos de carácter personal. 4. El objeto del derecho fundamental a la protección de datos personales.

1. Cuestiones preliminares

El análisis al derecho a la protección de datos personales que pretende hacer esta capítulo, más que un estudio exhaustivo de este derecho desde la óptica de la LOPD es una aproximación a la naturaleza jurídica de este derecho en el ordenamiento jurídico español y a algunas de las disposiciones de la LOPD que como se analizará en un capítulo más adelante, tienen una plena incidencia cuando entramos en la relación de transparencia, acceso a la información y protección de los datos personales.

La creación del derecho a la protección de datos de carácter personal en España deriva de la interpretación jurisprudencial del artículo 18.4 Constitución española que contiene una limitación a los usos de la informática en función del respeto a la intimidad, pero del cual el Tribunal Constitucional (TC) ha entendido que se desprenden una garantía a favor de la tutela de los datos personales. En ese sentido, se hará un análisis de la jurisprudencia más relevante del TC hasta llegar a la sentencia del Tribunal Constitucional (STC) 292/2000, de 30 de noviembre, en la que termina de reconocer plenamente como derecho autónomo el derecho a la protección de datos de carácter personal y además define en su sentencia, una serie de derechos y principios integradores de este derecho.

Posteriormente, se hará un breve análisis de algunas de las disposiciones contenidas en la LOPD así como sus derechos y principios integradores, para concluir con una recapitulación en la que se dará cuenta de la incidencia que tiene la LOPD en la interpretación armónica que se debe hacer entre las leyes que regulan la transparencia y el derecho de acceso a la información junto con las normativa reguladora de la protección de datos personales.

2. El derecho a la protección de datos en España

El derecho a la protección de datos personales ha nacido como un mecanismo de tutela de los derechos y libertades de las personas físicas, en cuanto a los riesgos y las amenazas que derivan del constante uso de las nuevas tecnologías en la sociedad[216]. Con el inicio de los procesos de constitucionalización en Europa, generados después de la segunda mitad del siglo XX es que puede observarse este desarrollo del derecho a la protección de datos de carácter personal[217] pues es a partir de este momento que el desarrollo de las tecnologías y la incidencia en la vida privada y familiar de las personas comienza a ser inminente. Las formas de configuración de este derecho han variado según la realidad jurídica de cada país, así por ejemplo, menciona ORDOÑEZ SOLÍS que en Alemania se dedujo vía jurisprudencia del Tribunal Constitucional alemán, en los países anglosajones se deriva del "*rigth to privacy*"; mientras que en países latinoamericanos ha nacido como *habeas data*[218].

Previo a la inclusión del derecho a la protección de datos personales como parte del catálogo de derechos fundamentales, existieron algunas normas que lo regulaban como por ejemplo la *Datenschutz,* de 7 de octubre de 1970, publicada por el Länder Hesse (Alemania) y la *Data Lag* de Suecia en 1973[219]. Estas normas nacen como parte del resultado del trabajo del Consejo de Europa en la materia. En especial, de la Recomendación 509/1968 de la Asamblea del Consejo de Europa sobre "Los derechos humanos y los nuevos logros científicos y técnicos", en la que se recomendó estudiar y reportar sobre sí la legislación de los Estados Miembros del Consejo era adecuada para garantizar la protección del derecho a la privacidad contenido en el artículo 8 del CEDH frente al uso de las nuevas tecnologías, así como dar las recomendaciones necesarias en caso de que no fuera así[220].

Esta Recomendación dio cabida a las resoluciones (73) 22, de 26 de septiembre de 1973 y (74) 29, de 20 de septiembre de 1974, ambas aprobadas por el Comité de

[216] Prieto Gutiérrez, J. M. (2004). Objeto y naturaleza jurídica del derecho fundamental a la protección de datos personales. *Boletín del Ministerio de Justicia.* Año 58, núm. 1973, 2004. pp. 3317-3337.
[217] Ordóñez Solís, D. (2011). Privacidad y protección judicial de los datos personales. Barcelona: Bosch. p. 108.
[218] *Ibíd.*
[219] Rebollo Delgado, L. (2008). Vida privada y protección de datos en la Unión Europea. Madrid: Dykinson. p. 86.
[220] Recomendación 509/1968 de 31 de enero, de la Asamblea del Consejo de Europa, apartado 8.

Ministros del Consejo de Europa y relativas a la protección de la privacidad de los individuos frente al uso de bancos de datos en el sector público y privado respectivamente, que recogen la esencia de los derechos y principios que integran hoy en día el derecho a la protección de datos personales. [221]

Seguidamente, en el ámbito doméstico existieron otros desarrollos normativos tempranos, como por ejemplo, la promulgación de la *Bundesdatenschutzgesetz*, ley alemana de protección de datos de enero de 1977 y la *Loi 78-17 relative a l'informatique, aux fichiers et aux libertés*, ley francesa de informática, ficheros y libertades de 6 de enero. En paralelo, el trabajo de las instituciones europeas continuaba y dio lugar a la resolución del Parlamento Europeo, de 8 de mayo de 1979 "sobre la tutela de los derechos del individuo frente al creciente progreso técnico en el sector de la informática".[222]

Ahora bien, es en la Constitución Política portuguesa de 1976[223] donde se reconoce por primera vez en un texto fundamental, la necesidad de tutelar las libertades y los derechos de los ciudadanos frente al uso de las nuevas tecnologías. Posteriormente, la segunda Constitución Política en recoger en 1978 una disposición dirigida a garantizar los derechos y libertades de los ciudadanos en este ámbito es la española, que en su artículo 18.4 dispone que "la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

Para AGUADO RENEDO, la inclusión de esta disposición en el texto constitucional español obedece a que se trata de una norma fundamental promulgada en un contexto moderno y "una de las manifestaciones más evidentes de ello lo constituye la alusión a la

[221] Ambas resoluciones tutelan el derecho de toda persona de que la información registrada en los bancos de datos sea exacta y mantenida de forma actualizada, sea apropiada y relevante para el fin perseguido, no haya sido obtenida por medios fraudulentos o ilegales, con especificación temporal sobre el período en el que serán resguardados ciertas categorías de datos, la prohibición de comunicar a terceros sin autorización, el derecho de toda persona a conocer la información almacenada relativa a su persona, derecho a solicitar la corrección y eliminación de información incorrecta u obtenida de forma ilegítima, el derecho a que se tomen las medidas necesarias para evitar el uso ilegítimo de la información, incluyendo la seguridad de los sistemas, el derecho de acceso a la información y derecho de disociación cuando la información sea utilizada para fines estadísticos.

[222] Albuquerque, L. (2007). Los ficheros de solvencia patrimonial y crédito: breves comentarios a su régimen jurídico. *Anuario de la Facultad de Derecho,* Vol. XXV, 2007. pp. 179-194.

[223] El artículo 35 de la Constitución Política portuguesa disponía en su versión original: "Artículo 35. Utilización de la informática. 1. Todos los ciudadanos tendrán derecho a tomar conocimiento de lo que conste en forma de registros mecanográficos acerca de ellos y de la finalidad a que se destinan las informaciones y podrán exigir la rectificación de los datos, así como su actualización. 2. No se podrá utilizar la informática para el tratamiento de datos referentes a convicciones políticas, fe religiosa o vida privada, salvo cuando se trate de la elaboración de datos no identificables para fines estadísticos. 3. Se prohíbe atribuir un número nacional único a los ciudadano*s".*

informática que se hace en la misma, en concordancia, por lo demás, con las diversas normas que en los Estados europeos se estaban dictando por aquellas mismas fechas en relación con la materia".[224]

Estas dos Constituciones son los primeros textos que elevan a rango constitucional ese derecho de los ciudadanos frente al uso de las nuevas tecnologías, aunque si bien como menciona SERRANO PÉREZ[225], existen matices, siendo la disposición portuguesa más concreta y comprehensiva de la incidencia de las nuevas tecnologías en los derechos y libertades de las personas.

A diferencia del precepto constitucional portugués que regula tanto el aspecto negativo –limitación del uso de la informática para tratar determinados datos–, como el aspecto positivo –el derecho de los ciudadanos a conocer la información personal que poseen terceros–, el legislador español optó por regular únicamente el aspecto negativo de la informática y su incidencia en la esfera jurídica al disponer que la ley limitará su uso con el fin de garantizar la intimidad personal y familiar de los ciudadanos, así como el pleno ejercicio de sus derechos. En palabras de SUBIZA PÉREZ, el constituyente español "más que recoger un derecho lo que hace es advertir de un peligro".[226]

Asimismo, no puede dejarse de lado que pese al temprano acogimiento en el texto constitucional de una disposición de este tipo, es hasta 1992 cuando España se aprueba su primera ley de protección de datos, la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD), esta normativa llega muy por detrás respecto de otros países europeos. En todo caso, como menciona PEREZ LUÑO, citado por SERRANO PÉREZ, ha de reconocerse que esta disposición ha venido a mejorar el panorama existente y supone un avance frente a la situación anterior de inexistencia de una legislación, que poco tiempo después fue reemplazada por la LOPD[227].

---

[224] Aguado Renedo, C. (2010). La protección de los datos personales ante el Tribunal Constitucional español. *Revista Mexicana de Derecho Constitucional*, Núm 23, julio-diciembre 2010. pp. 3-25.

[225] Serrano Pérez, M.M. (2003). El derecho fundamental a la protección de datos. Derecho español y comparado. Madrid: Thomson Civitas. P.123-124.

[226] Subiza Pérez, I.; Arias Pou, M. (2009). La protección de datos y sus mundos. Pamplona: DAPP Publicaciones Jurídicas. p. 33.

[227] Pérez Luño, citado por Serrano Pérez, M.M. (2003). El derecho fundamental a la protección de datos… *op. cit.* p. 127. DE LA QUADRA-SALCEDO Y FERNÁNDEZ DEL CASTILLO lleva a cabo un análisis interesante en relación a las causas por las cuales existió el retraso en la aprobación de una legislación en materia de protección de datos y las razones por las cuáles se aprueba la LORTAD ya cuando habían iniciado las

3. La creación jurisprudencial del derecho a la protección de datos de carácter personal

No abordar el tema de forma directa partiendo de la experiencia del legislador portugués costó un debate sobre su naturaleza jurídica como un derecho autónomo, labor de la cual se tuvo que encargar el TC. VILLAVERDE MENÉNDEZ anota que lo que el precepto constitucional español hace es únicamente apuntar una reserva de ley que ofrece varias interpretaciones, una de ellas entender el artículo 18.4 de la Constitución española como una garantía adicional a los derechos contenidos en el artículo 18.1 de la misma Constitución, o bien, la interpretación de un derecho fundamental implícito, aunque ello conllevara a forzar la literalidad de lo dispuesto en el 18.4 de la Constitución española.[228]

Ante la indefinición conceptual del bien jurídico que tutela el artículo 18.4 constitucional, el TC tuvo que construir desde su jurisprudencia el alance y contenido de este derecho. Así por ejemplo, en la STC 254/1993, de 18 de agosto, consideró que el mandato contenido en el artículo 18.4 de la Constitución española constituía una garantía de los derechos fundamentales, especialmente los relativos al honor y la intimidad, pero que a su vez constituía un derecho a la libertad frente a las agresiones potenciales contra la dignidad y la libertad de la persona que provienen de un uso ilegítimo del tratamiento mecanizado de datos. Al mismo tiempo, se ocupó de interpretar el artículo 18.4 de la Constitución Española en relación con el Convenio 108 y las facultades y derechos derivados de los efectos que este texto jurídico internacional despliega en el ordenamiento español[229]. Por último, reconoció que:

---

negociaciones de la Directiva 95/46, lo que iba a venir a suponer de entrada un cambio o al menos adaptación en cualquier legislación que fuese aprobada en cualquier legislación doméstica de los Estados Miembro. Ver en: De la Quadra-Salccedo y Fernández del Castillo, T. (2015). La primera ley española de protección de datos (LORTAD) y el proceso de su elaboración. En AEPD, 20 años de protección de datos en España. Madrid: Agencia Española de Protección de Datos. pp. 27-39. En ese mismo sentido y en relación con los retos que supone la aprobación de un marco normativo en materia de protección de datos personales, PRADO FALCÓN apunta que "al amparo de las regulaciones internacionales y sobre todo comunitarias, se va a producir también el desarrollo legislativo en nuestro país del derecho a la protección de datos personales, que a diferencia de lo que sucede con el resto de los derechos fundamentales y como expresión de su singularidad complejidad, va a precisar de una pluralidad de leyes y otras normas de rango inferior para su adecuada regulación". En: Prado Falcón, J. (2008). La protección de datos personales. En M.E. Casas Baamonde y M. Rodríguez-Piñero y Bravo-Ferrer (Dir.) Comentarios a la Constitución Española. Madrid: Fundación Wolters Kluwer. pp. 456-459.

[228] Villaverde Menéndez, I. (2006). La jurisprudencia del Tribunal Constitucional sobre el derecho fundamental a la protección de datos de carácter personal. En A. Farriols i Solá (Coord.). *La protección de datos de carácter personal en los centros de trabajo*. Madrid: Cinca: Fundación Francisco Largo Caballero. Pp. 48-63.

[229] En ese sentido, el FJ 7 de la STC 254/1993, de 18 de agosto, dispone: "En este sentido, las pautas interpretativas que nacen del Convenio de protección de datos personales de 1981 conducen a una respuesta

> "Esta constatación elemental de que los datos personales que almacena la Administración son utilizados por sus autoridades y sus servicios, impide aceptar la tesis de que el derecho fundamental a la intimidad agota su contenido en facultades puramente negativas, de exclusión. Las facultades precisas para conocer la existencia, los fines y los responsables de los ficheros automatizados dependientes de una Administración pública donde obran datos personales de un ciudadano son absolutamente necesarias para que los intereses protegidos por el art. 18 C.E., y que dan vida al derecho a la intimidad, resulten real y efectivamente protegidos. Por ende, dichas facultades de información forman parte del contenido del derecho a la intimidad, que vincula directamente a todos los poderes públicos, y ha de ser salvaguardado por este Tribunal, haya sido o no desarrollado legislativamente (STC 11/1981, fundamento jurídico 8° y 101/1991, fundamento jurídico 2°)".[230]

Como se puede observar, si bien trasciende la posición del legislador de únicamente contemplar un ámbito negativo frente a las libertades informáticas, el TC reconoce otra dimensión positiva –el derecho de acceso a los datos–, pero ligada al derecho a la intimidad y no como un parte esencial de un derecho autónomo a la protección de datos personales.

Por su parte, en la STC 143/1994, de 9 de mayo, señaló que "un sistema normativo que, autorizando la recogida de datos incluso con fines legítimos, y de contenido aparentemente neutro, no incluyese garantías adecuadas frente a su uso potencialmente inversor de la vida privada del ciudadano a través de su tratamiento técnico, vulneraría el derecho a la intimidad de la misma manera en que lo harían las intromisiones directas en el contenido nuclear de ésta".[231]

Posteriormente, en la STC 11/1998, de 13 de enero, también reconoció que el artículo 18.4 de la Constitución española "no sólo entraña un específico instrumento de protección de los derechos del ciudadano frente al uso torticero de la tecnología informática, como ha quedado dicho sino que además, consagra un derecho fundamental autónomo a controlar el flujo de informaciones que conciernen a cada persona –a la privacidad según la expresión utilizada en la Exposición de Motivos de la Ley Orgánica Reguladora del Tratamiento Automatizado de Datos de Carácter Personal, pertenezcan o

---

inequívocamente favorable a la tesis del demandante de amparo. La realidad de los problemas a los que se enfrentó la elaboración y la ratificación de dicho tratado internacional, así como la experiencia de los países del Consejo de Europa que ha sido condensada en su articulado, llevan a la conclusión de que la protección de la intimidad de los ciudadanos requiere que éstos puedan conocer la existencia y los rasgos de aquellos ficheros automatizados donde las Administraciones públicas conservan datos de carácter personal que les conciernen, así como cuáles son estos datos personales en poder de las autoridades*"*.

[230] STC 254/1993, de 18 de agosto, FJ 6.

[231] STC 143/1994, de 9 de mayo, FJ 7.

no al ámbito más estricto de la intimidad, para así preservar el pleno ejercicio de sus derechos. Trata de evitar que la informatización de los datos personales propicie comportamientos discriminatorios".

En la STC 144/1999, de 22 de julio, en un sentido similar a las anteriores, dispuso el TC que "el art. 18.1 CE no garantiza sin más la 'intimidad', son el derecho a poseerla, a tener vida privada disponiendo de un poder de control sobre la publicidad de la información relativa a nuestra persona y familia, sea cual sea el contenido de aquello que se desea mantener al abrigo del conocimiento público. Esta garantía impone a los poderes públicos la prohibición de que se conviertan en fuentes de esa información sin las debidas garantías, y también el deber de prevenir los riesgos que puedan derivarse del acceso o divulgación indebidas de dicha información. (…) De otro lado, el derecho a la intimidad impone a los poderes públicos la obligación de adoptar cuantas medidas fuesen necesarias para hacer efectivo aquel poder de disposición, y preservar de potenciales agresiones ese ámbito reservado de la vida personal y familiar, no accesible a los demás; en especial, cuando la protección de otros derechos fundamentales o bienes constitucionalmente protegidos pueden justificar que ciertas informaciones relativas a una persona o su familia sean registradas y archivadas por un poder público, como es el caso del Registro Central de Penados y Rebeldes (…)[232]".

Aún y cuando en estas y otras sentencias[233] ya se vislumbraba el alcance, contenido y naturaleza jurídica del derecho incluido en el artículo 18.4 de la Constitución española, son las SSTC 290/2000 y 292/2000, de 30 de noviembre, las que terminan de precisar vía jurisprudencial esa preocupación que externaba el legislador sobre el poco alcance que tendrían los derechos fundamentales frente al uso de la informática y reconoció el carácter de derecho autónomo de la protección de datos de carácter personal. El momento en que el TC dicta esta sentencia, existía una fuerte corriente y desarrollo tanto doctrinario como normativo a nivel internacional que optaba e impulsaba al reconocimiento del derecho a la protección de datos personales como un derecho autónomo, como por ejemplo, la CDFUE que había sido aprobada unos meses antes e incluía ya en su artículo 8 el derecho fundamental a la protección de datos.

[232] STC 144/1999 de 22 de julio, FJ 8.
[233] Ver STC 202/1999, de 8 de noviembre.

Específicamente, en la STC 292/2000, de 30 de noviembre, sentencia que a criterio de CASAS BAAMONDE "con mayor carga doctrinal y as incisiva (…) efectuó el control de constitucionalidad en nombre de los derechos"[234], el TC resolvió el recurso de inconstitucionalidad interpuesto por el Defensor del Pueblo[235], D. Antonio Rovira, e incorporó de forma inequívoca al catálogo de derechos fundamentales contenidos en la Constitución española, el derecho a la protección de datos de carácter personal como un derecho fundamental de carácter autónomo:

> "Este derecho fundamental a la protección de datos, a diferencia del derecho a la intimidad del art. 18.1. CE, con quien comparte el objetivo de ofrecer una eficaz protección constitucional de la vida privada y familiar, atribuye a su titular un haz de facultades que consisten 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). La peculiaridad de este derecho fundamental a la protección de datos respecto de aquel derecho fundamental tan afín como es el de la intimidad radica, pues, en su distinta función, lo que apareja, por consiguiente, que también su objeto y contenido difieran".[236]

[234] Casas Baamonde, M. E. (2015). El derecho a la protección de datos de carácter personal en la jurisprudencia del Tribunal Constitucional. En AEPD, 20 años de protección de datos en España. Madrid: Agencia Española de Protección de Datos. pp. 91-126.

[235] En su recurso de inconstitucionalidad, recibido el 14 de marzo de 2000 en el Registro General del TC, el Defensor del Pueblo, realiza una exposición clara y extensiva del reconocimiento del derecho a la protección de datos de carácter personal en el ordenamiento jurídico internacional y comunitario, e invoca a favor de su reconocimiento a partir del artículo 18.4 de la Constitución española lo siguiente: "nuestra Constitución, en el artículo 18.4 y de manera coherente con los requerimientos actuales de protección de los derechos y libertades fundamentales frente a los nuevos tipos de agresiones que estos pueden sufrir, ordena al legislador a limitar el uso de la informática no sólo para garantizar el honor y la intimidad de los ciudadanos, sino también para asegurar que cada uno de ellos pueda libremente y en todo momento ejercitar los derechos que legítimamente le corresponden. Porque, como acertadamente afirma el Tribunal alemán, "quien se siente inseguro de si en todo momento se registran cualesquiera comportamientos divergentes y se catalogan, utilizan o transmiten permanentemente a título de información procurará no llamar la atención con esa clase de comportamiento. Quien sepa de antemano que su participación, por ejemplo, en una reunión o en una iniciativa cívica va a ser registrada por las autoridades y que podrían derivarse riesgos para él por este motivo renunciará presumiblemente a lo que supone un ejercicio de los correspondientes derechos fundamentales. Esto no sólo menoscabaría las oportunidades de desarrollo de la personalidad individual, sino también el bien público, porque la autodeterminación constituye una condición elemental de funcionamiento de toda comunidad fundada en la capacidad de obrar y de cooperación de sus ciudadanos". Pues bien, si para la intimidad y el ejercicio de los derechos por parte de los ciudadanos uno de los mayores riesgos del uso de la informática es el derivado de las casi infinitas posibilidades que esta técnica ofrece para almacenar datos, obtener de ellos informaciones precisas y completar o contrastar sin límites espaciales o temporales esa información con la obrante en otras bases de datos o con los datos procedentes de otros ficheros, parece de todo punto evidente que la garantía elemental del derecho exige que el ciudadano pueda controlar el flujo de información que sobre él circule, decidiendo básicamente por sí mismo sobre la difusión y la utilización de sus datos personales y para ello resulta esencial que conozca y en general consienta el almacenamiento y uso de dicha información".

[236] FJ 6.

Asimismo, amparada en el reconocimiento internacional del derecho a través de diferentes medios, como la Resolución 45/95 de la Asamblea General de las Naciones Unidas, el Convenio 108, la Directiva 95/46 y la CDFUE[237], el TC señala una serie de matices propios del derecho a la protección de datos de carácter personal, entre ellos:

- El objetivo de garantizar a la persona un poder de control sobre sus datos personales, uso y destino, con el propósito de impedir un tráfico ilícito y lesivo para la dignidad y el derecho del afectado.
- Garantiza a las personas un poder de disposición de sus datos, lo cual a su vez conlleva la prohibición de que los poderes públicos se conviertan en fuentes de la información sin las garantías debidas, así como el deber de prevenir los riesgos que puedan derivarse del acceso o divulgación indebida de los datos personales.
- El poder de disposición de los datos lleva consigo aparejado el derecho de conocer cuáles datos son los que poseen terceros, quiénes los poseen y con qué fin.
- El derecho a la protección de datos se extiende a los datos íntimos de la persona, pero también a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar tanto derechos fundamentales como derechos ordinarios.
- El objeto del derecho es la tutela de los datos y no solo de los datos íntimos de la persona. Los datos amparados son todos los que identifiquen o permitan la identificación de la persona, incluso pueden servir para la

[237] Sobre los antecedentes normativos y jurisprudenciales usados por el TC en esa sentencia, LUCAS MURILLO DE LA CUEVA, hace un recuento especialmente ilustrativo y señala: "desde la Ley Orgánica 5/1992, hasta la Sentencia del Tribunal Constitucional 292/2000 que reconoce el derecho fundamental, se han sumado los siguientes elementos, cuya concurrencia explica el sentido de este pronunciamiento: 1.°) El debate de intensidad creciente promovido desde ámbitos académicos y sociales sobre el bien jurídico que protegía esa legislación y, en particular, sobre la diferencia existente entre intimidad y autodeterminación informativa. 2. °) La progresiva elaboración en el espacio europeo, a partir del Convenio del Consejo de Europa n.° 108, de una disciplina orientada a proteger los datos personales, que acabará plasmada en la Directiva 95/46. 3. °) El paso dado por la Unión Europea en el 2000 con la Carta de los Derechos Fundamentales al reconocer la autonomía del derecho a la protección de datos de carácter personal. 4°-) La jurisprudencia del Tribunal Europeo de Derechos Humanos, que, a partir del derecho a la vida privada reconocido por el artículo 8 de la Convención, dotó de autonomía a la protección de datos de carácter personal (casos Amann contra Suiza y Rotaru contra Rumania, ambos del 2000. 5.°) La dinámica generada por la aplicación de una Ley –la LORTAD- que expresamente hablaba de un nuevo derecho fundamental, y por la jurisprudencia constitucional que, en sintonía con posiciones doctrinales, iba acentuando la autonomía de la técnica jurídica de la protección de datos personales respecto del derecho a la intimidad". En: Lucas Murillo de la Cueva, P. (2007). Perspectivas del derecho a la autodeterminación informativa. *Monográfico "III Congreso Internet, Derecho y Política (IDP). Nuevas Perspectivas"*, *IDP*, núm. 5 (2007). pp. 18-32.

confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo.

- Atribuye al titular de los datos un haz de facultades consistente en diversos poderes jurídicos, cuyo ejercicio impone a terceros deberes jurídicos. Garantizar a la persona un poder de control sobre sus datos personales solo es posible y efectivo si se imponen a los terceros deberes de hacer, como por ejemplo, que se requiera el consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho de acceder, rectificar y cancelar dichos datos.
- El derecho a la protección de datos consiste en un poder de disposición y de control de los datos personales, el cual faculta a la persona a decidir cuáles datos proporciona a un tercero, sea el Estado o un particular, o cuáles datos puede el tercero recabar, y también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posición o uso.

En palabras de VILLAVERDE MENÉNDEZ, en estos pronunciamientos el TC termina por concretar lo que ya venía anunciado en sus sentencias citadas, sea que el artículo 18.4 de la Constitución contiene un derecho fundamental implícito[238]. Basta recordar que en la STC 254/1993, de 18 de agosto, había anunciado que dicho precepto constitucional contenía una garantía de otros derechos, pero constituía en sí mismo un derecho frente a los abusos de la informática.

4. El objeto del derecho fundamental a la protección de datos personales

Según la STC 292/2002, de 30 de noviembre[239], el derecho a la protección de datos de carácter personal refiere a un derecho de poder de disposición y control sobre los datos personales, entendidos estos no sólo como los datos íntimos sino como cualesquiera datos que permitan la identificación de una persona. Esta disposición y control sólo puede verse concretada a través de la facultad de consentir la recogida, obtención y acceso a los datos

[238] Villaverde Menéndez, I. (2006). La jurisprudencia del Tribunal Constitucional sobre el derecho fundamental a la protección de datos… *op. cit.* pp. 48-63.
[239] En especial, el FJ 7.

personales, así como su posterior tratamiento y usos ya sea por parte del Estado o de un tercero particular. Igualmente, el ejercicio efectivo de esta facultad requiere que el titular o afectado tenga en todo momento la facultad de conocer quién dispone de sus datos personales, el uso al que los somete y el poder de oponerse tanto a la posesión de los datos como a los usos de los mismos.

En palabras de LUCAS MURILLO DE LA CUEVA, "la previsión constitucional de la tutela de los derechos frente al uso de la informática se proyecta sobre los datos personales e implica, por un lado, derechos y garantías para los titulares de esos datos de carácter personal. Por el otro, supone para quienes los recogen, tratan, transmite, ceden o conservan, una serie de obligaciones en lo que se refiere a la calidad y a la seguridad de la información de esa naturaleza que manejan y a las condiciones en que pueden utilizarla, almacenarla, facilitarla o cederla. Además, implica restricciones a la posibilidad de acceder a ella por parte de terceros, así como límites respecto de los datos personales que pueden ser tenidos en consideración y, posteriormente incorporados a los ficheros automatizados"[240].

De conformidad con lo anterior, según la doctrina constitucional y la doctrina académica, el objeto de tutela del derecho a la protección de datos contenido en el artículo 18.4 de la Constitución española es la libre disposición y control de los datos de carácter personal, lo cual impone a los poderes públicos y terceros no solo limitaciones respecto del tratamiento, sino también obligaciones para garantizar la plena vigencia de este derecho. Dentro de estas facultades oponibles a terceros, destaca la exigencia del consentimiento informado como requisito inexorable para el tratamiento de los datos, salvo en los casos en que la ley en forma expresa indique que no se requieren. Adicionalmente a esta facultad, está el reconocimiento de otras prerrogativas como por ejemplo, el derecho de acceso, rectificación, cancelación y oposición.[241]

---

[240] Lucas Murillo de la Cueva, P. (1999). La construcción del derecho a la autodeterminación informativa. *Revista de Estudios Políticos (Nueva época)*. Núm. 104. Abril-Junio 1999. pp. 35-60.

[241] Lucas Murillo de la Cueva, P. (2008). El derecho a la autodeterminación informativa y la protección de datos personales. *Azpilcueta*. Núm. 20, 2008. pp. 43-58. Menciona además, Serrano Pérez, que la LORTAD tenía como referente inmediato el Convenio 108 del Consejo de Europa, mientras que la LOPD, que respondía a la adaptación de la Directiva 95/46, que a su vez ampliaba los derechos y contenidos del Convenio 108. En: Serrano Pérez, M.M. (2005). El derecho fundamental a la protección de datos. Su contenido esencial. *Nuevas Políticas Públicas: Anuario multidisciplinar para la modernización de las Administraciones Púbicas,* núm. 1, 2005. pp. 245-265. También, sobre este particular puede verse: Ruiz Miguel, C. (1994). En torno a la protección de los datos personales automatizados. *Revista de estudios políticos,* núm. 84, pp. 273-264.

La LOPD –que sustituyó la LORTAD de 1992 y que se circunscribe en el proceso por parte de los Estados de trasposición de la Directiva 95/46[242]- delimita claramente el objeto del derecho a la protección de datos personales en el artículo 1 de la LOPD, donde se señala que la ley tiene "por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar", dando así al derecho un enfoque de garantía más allá del de límite previsto en el artículo 18.4 de la Constitución española[243].

En relación con el objeto de aplicación de la LOPD, inmediatamente debe remitirse al artículo 3 de la LOPD que define, de forma precisa, que dato personal es cualquier información concerniente a personas físicas identificadas e identificables y define como tratamiento de datos aquellas "operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias".

La precisión terminológica de los conceptos de *"dato personal"* y *"tratamiento de datos"* para MARTÍNEZ MARTÍNEZ ofrecen una ventaja en la aplicación de la norma; pues aseguran la prevalencia de lo dispuesto en la LOPD de forma automática. En cualquier caso en que se haya identificado un dato personal objeto de tratamiento, aplica de forma directa la LOPD[244], sin perjuicio de la aplicación y relevancia que tienen los demás principios que contiene la LOPD.

Asimismo, más adelante define el ámbito de aplicación y las exclusiones, siendo que la LOPD aplica para todo tratamiento de datos de carácter personal salvo que se trate de ficheros utilizados para actividades exclusivas personales o domésticas, los relativos a

[242] Ordóñez Solís D. (2011). Privacidad y protección judicial de los datos personales… *op. cit.* p.118. Sobre este proceso, puede consultarse también: De la Quadra-Salccedo y Fernández del Castillo, T. (2015). La primera ley española de protección de datos (LORTAD) y el proceso de su elaboración. En AEPD, 20 años de protección de datos en España. Madrid: Agencia Española de Protección de Datos. pp. 27-39.

[243] Lucas Murillo de la Cueva. P. (2010). El objeto de la Ley Orgánica de Protección de Datos de Carácter Personal. En A. Troncoso Reigada (Dir.) Comentario a la Ley Orgánica de Protección de Datos de Carácter personal. Pamplona: Aranzadi. pp. 75-96. Puede consultarse en esa misma línea: Lucas Murillo de la Cueva, P. (1999). La construcción del derecho a la autodeterminación informativa… *op. cit.* pp. 35-60.

[244] Martínez Martínez, R. (2007). El derecho fundamental a la protección de datos: perspectivas. *Monográfico "III Congreso Internet, Derecho y Política (IDP). Nuevas perspectivas". Revista de Internet Derecho y Política.* Núm. 5 (2007). pp. 47-61.

materias clasificadas; así como los que se establezcan para la investigación de terrorismo y otras formas graves de delincuencia organizada.

En su artículo 4, la LOPD refiere a los principios integradores del derecho a la protección de datos, que se agrupan bajo la denominación de calidad de datos y que incluyen a su vez el principio de adecuación de los datos, el principio de finalidad, la licitud del tratamiento, así como la necesaria exactitud y veracidad de los datos[245]. Estos principios, como menciona TRONCOSO REIGADA "recogen por una parte, las obligaciones que incumben a los responsables de tratamiento y que deben estructurar todos los tratamientos de datos personales. Por otra parte, estos principios también pueden ser comprendidos como derechos de las personas cuyos datos sean objeto de tratamiento".[246]

Importante, es la referencia que hace la LOPD al consentimiento informado, que se encuentra plenamente apegado a lo dispuesto en la STC 292/2000, de 30 de noviembre, que reconoce esta facultad como uno de los elementos esenciales del derecho a la protección de datos personales[247]. De conformidad con el artículo 6 de la LOPD, se requiere para cualquier tipo de tratamiento de datos personales, el consentimiento inequívoco –toda manifestación de voluntad, libre, inequívoca, específica e informada,

[245] APARICIO SALOM recoge bien la esencia de este derecho y menciona que: "en definitiva, conforme al régimen establecido en este artículo, la información sometida a tratamiento está directamente vinculada a la finalidad a que se destina y, por ello, la legitimidad del tratamiento está condicionada a su adecuación. Así, cabe afirmar que no bastará simplemente con obtener el consentimiento del interesado para someter la información a tratamiento, sino que, además, el tratamiento sólo será legítimo si los datos que se procesan son adecuados para atender o conseguir dicha finalidad. En definitiva, la LOPD prohíbe el tratamiento de datos que no sean necesarios para atender a la finalidad que se autoriza, aunque el interesado haya prestado su consentimiento informado. Esta regla constituye, en definitiva, un límite adicional al alcance que el responsable del tratamiento puede atribuir al consentimiento del interesado, ya que la LOPD exige, para calificar la legitimidad del tratamiento, que la información se adecue a las finalidades que lo motivan.". En: Aparicio Salom, J. (2010). La calidad de los datos. En A. Troncoso Reigada (Dir.) Comentario a la Ley Orgánica de Protección de Datos de Carácter personal. Pamplona: Aranzadi. pp. 323-340.

[246] Troncoso, Reigada. A. (2010). El principio de calidad de los datos. En A. Troncoso Reigada (Dir.) Comentario a la Ley Orgánica de Protección de Datos de Carácter personal. Pamplona: Aranzadi. pp. 340-394.

[247] En este sentido, la STC 292/2000 indica en el FJ 7: "7. De todo lo dicho resulta que el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué so los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos".

mediante la que el interesado consienta el tratamiento de datos personales que le conciernen (artículo 3.h de la LOPD) salvo las excepciones previstas por la ley.

La LOPD exige un deber de secreto en su artículo 10 así como los supuestos bajo los cuales los datos pueden ser comunicados. En relación con el deber de secreto, la LOPD es clara en señalar que el responsable o encargado de tratar los datos, está obligado a guardar secreto profesional respecto de los mismos. Esta disposición conecta de forma directa con el artículo 11 de la LOPD, que establece bajo que supuestos se pueden comunicar los datos a un tercero, dentro de los cuales se encuentran y son de especial relevancia para el análisis que se efectuará en otros apartados de esta tesis, cuando exista el consentimiento informado o bien, cuando concurra alguna de las excepciones previstas en dicho artículo, como por ejemplo, que exista una ley que habilite la transmisión de los datos a dicho tercero (como lo es, para nuestros efectos, la LTAIBG[248]).

Por último, y entre otras disposiciones que escapan al alcance de este trabajo, la LOPD recoge un catálogo de derechos que resulta acorde con la Directiva 95/46 que incluyen el derecho a solicitar y obtener información de los datos que le conciernan y estén siendo objeto de tratamiento (derecho de acceso, artículo 15 de la LOPD), el derecho a rectificar o cancelar los datos personales cuyo tratamiento no se ajuste a lo dispuesto en la ley, o bien, resultasen los datos inexactos e incompletos (artículo 16 de la LOPD), así como el derecho a un procedimiento que le faculte el ejercicio de estos derechos (artículo 17 de la LOPD).

Recapitulación

La relación entre transparencia, acceso a la información y protección de datos personales depende en todo caso de la interpretación armónica que se lleve a cabo de la legislación vigente tanto en materia de acceso a la información como en materia de protección de datos personales.

[248] En relación con este tema, resulta interesante ver los comentarios que hace el profesor Guichot Reina en los casos en que la cesión o comunicación de datos opere por parte de una Administración Pública hacia terceros o sujetos privados desde antes de la aprobación de la LTAIBG. Ver en: Guichot Reina, E. (2010). Comunicación de datos por las Administraciones Públicas a Sujetos Privados. En A. Troncoso Reigada (Dir.) Comentario a la Ley Orgánica de Protección de Datos de Carácter personal. Pamplona: Aranzadi. pp. 1024-1056

Especial referencia e incidencia tiene en esa relación, la naturaleza jurídica de ambos derechos y su reconocimiento o no como derecho fundamental dentro del catálogo de derechos y libertades que confiere la Constitución española. Como hemos visto, en el caso del derecho de acceso a la información, el TC se ha amparado en que su regulación deriva del mandado del artículo 105.b) de la Constitución y que por ende merece un tratamiento como derecho de configuración legal y la doctrina que así lo considera, parte de la imposibilidad del TC de crear derecho vía jurisprudencia, razón por la cual no podría declararse su naturaleza iusfundamental en relación con el artículo 20 de la Constitución española. Paradójicamente, el derecho a la protección de datos personales ha nacido a partir de la jurisprudencia del TC en relación con el artículo 18.4, especialmente a partir de su STC 292/2000. Con este comentario no se pretende suponer una crítica al reconocimiento jurisprudencial del derecho a la protección de datos personales, sino que existe la posibilidad para el TC de reconocer constitucionalmente el derecho de acceso a la información como derecho fundamental, vía jurisprudencia, con el fin de solventar así la disparidad que supone en la relación entre transparencia, acceso a la información y protección de datos, ponderar entre un derecho fundamental y un derecho de configuración legal.

Dicho lo anterior, la mención a la legislación vigente en materia de protección de datos personales, centrada para este estudio en la LOPD, su objeto así como principios y derechos, demuestran la directa incidencia que tiene la misma cuando nos movemos al campo de la interrelación entre transparencia, acceso a la información y protección de datos personales. No sólo porque la LTAIBG, contiene una excepción con el fin de salvaguardar los datos personales de terceros y necesariamente su correcta interpretación depende de las definiciones y normas contenidas en la LOPD, sino porque además, la LTAIBG, es una ley que habilita la cesión de datos a terceros sin que para ello sea necesario contar con el consentimiento informado del interesado.

Capítulo VI. El derecho de acceso a la información en España desde la óptica de la Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno

SUMARIO: 1. Cuestiones preliminares. 2. La naturaleza jurídica del derecho de acceso a la información pública. A. El derecho de acceso a la información pública como derecho fundamental y su interpretación por parte de los tribunales internacionales. a) La jurisprudencia de la Corte IDH. b) La jurisprudencia del TEDH. B. La naturaleza jurídica del derecho de acceso a la información pública en España. 3. Las implicaciones de la consideración del derecho de acceso a la información pública como derecho de configuración legal frente a la protección de datos personales. 4. El objeto del derecho de acceso a la información pública en la LTAIBG.

1. Cuestiones preliminares

Este Capítulo se centrará en el análisis del derecho de acceso a la información en España según su regulación más reciente en la LTAIBG.

Para estos efectos, un primer acercamiento a la regulación del derecho de acceso a la información se hará desde la naturaleza jurídica que le ha atribuido el ordenamiento jurídico español, sea la de derecho de configuración legal según el mandado expreso del artículo 105.b) de la Constitución española, en comparación con el reconocimiento iusfundamental de este derecho que ha sido efectuado por parte de tribunales internacionales como la Corte IDH y la más reciente doctrina del TEDH.

Ello permitirá avanzar posteriormente en el análisis de los serios inconvenientes que representa que la LTAIBG no haya optado por al menos hacer referencia a la evidente conexión que tiene este derecho con el derecho a la libertad de recibir y difundir informaciones contenido dentro del derecho fundamental a la libertad de expresión, uno de los aspectos más criticados de la LTAIBG.

La falta de reconocimiento expreso no es nimia y como se expondrá, tiene serias repercusiones cuando se trata la relación que existe entre la transparencia, el derecho de acceso a la información y la protección de datos personales, y así ha quedado plasmado, por ejemplo, en los informes tanto de la AEPD como del Consejo de Estado en relación con el anteproyecto de ley de la LTAIBG, en la que constantemente recordaban al legislador el carácter de configuración legal del derecho de acceso a la información frente al carácter de derecho fundamental de la protección de datos personales.

Abordados estas cuestiones, haremos una referencia al objeto de tutela de la LTAIBG, lo que permitirá posteriormente y el mecanismo de ejercicio del derecho de acceso a la información, lo que pone de relieve la difícil situación de su conciliación con el derecho a la protección de datos personales, en el tanto persiguen fines distintos y permitirá una mejor comprensión en un posterior Capítulo tanto de los criterios como de las resoluciones emitidas por el CTBG.

2. La naturaleza jurídica del derecho de acceso a la información pública

A. El derecho de acceso a la información pública como derecho fundamental y su interpretación por parte de los tribunales internacionales

A nivel global existen, según GUICHOT REINA[249], dos tendencias en torno a la naturaleza jurídica del derecho de acceso a la información pública. La primera de ellas, es la que tiende a considerar el derecho de acceso a la información pública como parte del derecho a la libertad de expresión. Por su parte, la segunda tendencia, propia de Constituciones Políticas más recientes, parte de la consideración del derecho de acceso a la información pública como un derecho fundamental autónomo.

En este apartado nos encargaremos de reflexionar sobre la tesis que considera el derecho de acceso a la información como parte del derecho a la libertad de expresión, que es la que en todo caso, parece más cercana a la realidad jurídica española. Más específicamente en este punto, nos ocuparemos de la doctrina de los tribunales internacionales (TEDH y Corte IDH) que han jugado un papel determinante en el reconocimiento del carácter fundamental del derecho de acceso a través de la interpretación de los instrumentos jurídicos internacionales en materia de derechos humanos, especialmente, el Convenio Europeo de Derechos Humanos (CEDH) y la Convención Americana de Derechos Humanos (CADH).

Cabe recordar que el artículo 19 de la Declaración Universal de Derechos Humanos (DUDH), el artículo 19 del Pacto de Derechos Civiles y Políticos (PDCP), el artículo 10 CEDH y el artículo 13 de la CADH reconocen el derecho fundamental de toda persona a la libertad de pensamiento y expresión, lo cual comprende a su vez la libertad de buscar, recibir y difundir informaciones de toda índole. No obstante, dentro de ellas

[249] Guichot Reina, E. (2011). Transparencia versus protección de datos. Ponencia impartida en el VI Congreso Anual de la Asociación Española de Profesores de Derecho Administrativo. Palma de Mallorca, 12 de febrero 2011. p. 6

no se incluye de forma inequívoca, al menos en atención a su literalidad, un derecho de acceso a la información pública. Esta falta de concretar en forma expresa el derecho de acceso a la información dentro de los textos jurídicos internacionales provocó, en un primer momento, en el TEDH una resistencia al reconocimiento de su carácter fundamental, mientras que en la Corte IDH, la oportunidad de pronunciarse por primera vez a favor del reconocimiento del derecho de acceso como elemento esencial del derecho a recibir informaciones que, a su vez, está contenido en el derecho fundamental a libertad de expresión.

Ahora bien, es con la Declaración conjunta del Relator Especial de las Naciones Unidas (ONU) para la libertad de opinión y expresión, el Representante de la Organización para la Seguridad y Cooperación en Europa (OECE) para la libertad de los medios de comunicación y el Relator especial de la Organización de Estados Americanos (OEA), de 6 de diciembre de 2004 que se reconoce que "el derecho de acceso a la información es un derecho humano fundamental que debería aplicarse a nivel nacional a través de legislación global (por ejemplo, las Leyes de Libertad de Acceso a Información) basada en el principio de máxima divulgación, el cual establece la presunción de que toda la información es accesible, sujeto solamente a un sistema restringido de excepciones".

a) La jurisprudencia de la Corte IDH

Esta posición sobre el carácter *iusfundamental* del derecho de acceso a la información o "*right to know*", pasó posteriormente a ser reconocida por un tribunal internacional. El primero en hacerlo fue la Corte IDH en la sentencia por el fondo del caso Claude Reyes y otros vs. Chile, de 19 de septiembre de 2006 en el que conoció sobre la negativa del Estado chileno de permitir el acceso a determinada información relacionada con asuntos públicos. Sobre el derecho de acceso a la información como parte del derecho a la libertad de expresión contenido en el artículo 13 de la CADH, la Corte IDH pronunció:

> "75. La jurisprudencia del Tribunal ha dado un amplio contenido al derecho a la libertad de pensamiento y de expresión consagrado en el artículo 13 de la Convención, a través de la descripción de sus dimensiones individual y social, de las cuales ha desprendido una serie de derechos que se encuentran protegidos en dicho artículo.
>
> 76. En este sentido la Corte ha establecido que, de acuerdo a la protección que otorga la Convención Americana, el derecho a la libertad de pensamiento y de expresión comprende 'no sólo el derecho y la libertad de expresar su propio pensamiento, sino también el derecho y la libertad de buscar, recibir y difundir

> informaciones e ideas de toda índole'. Al igual que la Convención Americana otros instrumentos internacionales de derechos humanos tales como la Declaración Universal de Derechos Humanos y el Pacto Internacional de Derechos Civiles y Políticos, establecen un derecho positivo a buscar y recibir información.
>
> 77. En lo que respecta a los hechos del presente caso, la Corte estima que el artículo 13 de la Convención, al estipular expresamente los derechos a 'buscar' y a 'recibir' 'informaciones', protege el derecho que tiene toda persona a solicitar el acceso a la información bajo el control del Estado, con las salvedades permitidas bajo el régimen de restricciones de la Convención. Consecuentemente, dicho artículo ampara el derecho de las personas a recibir dicha información y la obligación positiva del Estado de suministrarla, de forma tal que la persona pueda tener acceso a conocer esa información o reciba una respuesta fundamentada cuando por algún motivo permitido por la Convención el Estado pueda limitar el acceso a la misma para el caso concreto. Dicha información debe ser entregada sin necesidad de acreditar un interés directo para su obtención o una afectación personal, salvo en los casos en que se aplique una legítima restricción. Su entrega a una persona puede permitir a su vez que ésta circule de manera que pueda conocerla, acceder a ella y valorarla. De esta forma, el derecho a la libertad de pensamiento y de expresión contempla la protección del de acceso a la información bajo el control del Estado, el cual también contiene de manera clara las dos dimensiones, la individual y la social, del derecho a la libertad de pensamiento y de expresión, las cuales deben ser garantizadas por el Estado de forma simultánea.
>
> (…)
>
> 92. la Corte observa que en una sociedad democrática es indispensable que las autoridades estatales se rijan por el principio de máxima divulgación, el cual establece la presunción de que toda información es accesible, sujeto a un sistema restringido de excepciones.
>
> 93. Corresponde al Estado demostrar que al establecer restricciones al acceso a la información bajo su control ha cumplido con los anteriores requisitos".

De esta sentencia de la Corte IDH no solo se rescata ser el primer reconocimiento jurisprudencial del derecho fundamental de acceso a la información, sino que además existen una serie de matices y precisiones que bien valen un análisis detenido y pormenorizado del cual no nos podemos ocupar en esta investigación.

No obstante, cabe destacar el reconocimiento de al menos tres aspectos puntuales de suma importancia que hace la Corte IDH en su sentencia. El primero de ellos, es la referencia expresa a la aplicación restrictiva del sistema de excepciones y limitaciones que es capaz de soportar el derecho de acceso a la información. El segundo punto relevante para la configuración del derecho fundamental de acceso a la información, es la facultad del solicitante del acceso de no tener que acreditar un interés legítimo ni motivar la solicitud de acceso, aunque esto como podremos apreciar más adelante, pueda llegar a suponer una dificultad cuando el acceso a la información afecte otros derechos

constitucionalmente protegidos y se deba aplicar un juicio de ponderación. Un último punto que puede merecer especial referencia es la incorporación del principio de máxima divulgación dentro del derecho de acceso a la información, por medio del cual se fija una presunción de que toda información que esté en manos de la Administración Pública, es en principio accesible por cualquier ciudadano. A su vez, esto conecta con la aplicación restrictiva y estricta de excepciones a este derecho y la no necesidad de acreditar un interés legítimo en el acceso.

b) La jurisprudencia del TEDH

Influenciado por la tendencia internacional, el TEDH reconoció por primera vez el carácter de derecho fundamental del acceso a la información pública en la Sentencia del TEDH (STEDH) del caso Táraság a Szabadságjogokért c. Hungría, de 14 de abril de 2009. Esta sentencia dio al traste con su línea jurisprudencial que negaba el carácter fundamental del derecho de acceso a la información pública y en la que había entendido, por ejemplo, que el artículo 10 del CEDH no garantizaba al individuo el derecho de acceso a los registros que contienen su información relativa a su situación personal, así como tampoco imponía una obligación al gobierno de suministrar dicha información a los individuos[250].

En la STEDH del caso Táraság a Szabadságjogokért c. Hungría, el TEDH comienza haciendo mención al sistemático reconocimiento del derecho de las personas a recibir información que sea de interés general, así como su vínculo con la libertad de prensa, especialmente cuando los Estados o autoridades nacionales adopten medidas que sean capaces de desincentivar el papel de "*watchdogs*" que le ha sido confiado a la prensa y que contribuye al debate público de temas de interés general[251].

Asimismo, reconoce que en virtud del artículo 10 de la CEDH no pueden permitirse restricciones que se constituyan en una forma de censura indirecta e impidan la recopilación de información que está en poder de las autoridades[252]. De igual forma, reconoce que la labor de informar sobre asuntos públicos no está limitada a los medios de

[250] "74. The Court observes that the right to freedom to receive information basically prohibits a Government from restricting a person from receiving information that others wish or may be willing to impart him. Article 10 (art. 10) does not, in circumstances such as those of the present case, confer on the individual a right of access to a register containing information on his personal position, nor does it embody an obligation on the Government to impart such information to the individual. 75. There has thus been no interference with Mr. Leander's freedom to receive information, as protected by Article 10 (art. 10)."
[251] STEDH de 14 de abril de 2009, caso Táraság a Szabadságjogokért c. Hungría, apartado 26.
[252] *Ibíd.* Apartado 27.

comunicación o periodistas profesionales, sino que también se reconoce a otros sujetos que contribuyan al debate público, como puede ser una organización no gubernamental[253].

Más adelante en la sentencia, el TEDH menciona que, si bien existe jurisprudencia en donde había reconocido la dificultad de derivar del CEDH un derecho general de acceso a los datos y los documentos administrativos, el Tribunal ha avanzado hacia una interpretación más amplia del concepto de *"libertad de recibir información"* y hacia el reconocimiento de un derecho de acceso a la información[254]. Con base en esta consideración es que el TEDH efectúa su primer acercamiento al reconocimiento de un derecho fundamental de acceso a la información.

En ese mismo año, por STEDH del caso Kenedi c. Hungría, de 26 de mayo de 2009, el TEDH señala que el acceso a fuentes documentales originales para la investigación histórica es un elemento esencial del ejercicio del derecho del demandante a la libertad de expresión, tal y como fue reconocido en la STEDH Táraság a Szabadságjogokért v. Hungría[255], reafirmando así el carácter de derechos fundamental del acceso a la información pública y su vínculo directo con el artículo 10 del CEDH.

Más recientemente, en la STEDH, de 25 de junio de 2013, caso Youth Initiative for Human Rights c. Serbia afina esta línea jurisprudencial. Frente a la solicitud del Estado serbio de inadmitir la demanda por *ratione materia* al no existir un derecho al acceso a la información contenido en el artículo 10 del CEDH, el TEDH, haciendo alusión a la sentencia del caso Táraság a Szabadságjogokért c. Hungría, recuerda que el derecho de recibir información trae aparejado consigo el derecho de acceso a la información[256]. Asimismo, resalta nuevamente que el papel de "*watchdog*" que puede llegar a tener una organización no gubernamental en temas de interés general es tan importante como el que le es conferido a la prensa[257]. Concluye el TEDH que la negativa del Serbia de dar información a la ONG demandante violenta el artículo 10 del CEDH, en el tanto impide que la organización pueda tener acceso a la información y contribuya al debate público[258].

[253] *Ibíd.*
[254] *Ibíd.* Apartados 35-39.
[255] STEDH de 26 de mayo de 2009, caso Kenedi c. Hungría, apartados 40-45.
[256] STEDH de 25 de junio de 20143, caso Youth Initiative for Human Rights c. Serbia, apartado 20.
[257] *Ibíd.*
[258] *Ibíd.* Apartado 24.

Para ROLLNERT LIERN, la sentencia del caso Youth Initiative for Human Rights c. Serbia es la derivación de las consecuencias del reconocimiento hecho por el TEDH en sus sentencias de 2009 y es la primera que puede ser equiparada por su rotundidad a la sentencia de la Corte IDH dictada en el caso Claude Reyes y otros c. Chile[259].

Para otros autores como FERNÁNDEZ VIVAS[260], al TEDH le sigue faltando mayor claridad y contundencia en el reconocimiento del derecho de acceso a la información y sus efectos. En ese sentido, se coincide con la posición de FERNÁNDEZ VIVAS en el tanto se considera que al TEDH le ha faltado, a diferencia de la Corte IDH, un análisis más profundo sobre alcances, contenido y límites aplicables en el ámbito europeo al derecho fundamental del acceso a la información. Sin perjuicio de ello, es destacable el cambio de jurisprudencia por parte del TEDH y su progresión y respaldo hacia el reconocimiento del derecho fundamental de acceso a la información como parte integral del derecho a la libertad de expresión y el derecho a recibir y difundir comunicaciones.

A criterio de esta investigación, la sentencia más explicativa y comprehensiva del TEDH en esta materia es la reciente STEDH, de 8 de noviembre de 2016, caso Magyan Helsinki Bizottság c. Hungría, en el Tribunal nuevamente aborda y reitera su posición de considerar el derecho de acceso a la información como un derecho fundamental esencial dentro del contenido del artículo 10 del CEDH. En esta ocasión, el TEDH comienza por señalar que, según los antecedentes desarrollados en la misma sentencia, que incluye el abordaje del tema desde el contexto internacional y los trabajos preparatorios del CEDH, no existen elementos que impidan al Tribunal interpretar que el artículo 10 incluye el derecho de acceso a la información.

Asimismo, recuerda que si bien el TEDH es conocedor de la seguridad jurídica internacional y que no cabría esperar que los Estados deban aplicar obligaciones internacionales no acordadas inicialmente, ya existían precedentes que permitían la previsibilidad de esta obligación. También menciona que la CEDH es un sistema de protección de derechos humanos, en el que debe tenerse en cuenta la evolución y el cambio de las circunstancias y las condiciones de los Estados contratantes.

[259] Rollnert Liern, G. (2014). El derecho de acceso a la información pública como derecho fundamental: una valoración del debate doctrinal a propósito de la Ley de transparencia. *Teoría y Realidad Constitucional.* UNED, núm. 34, 2014. pp. 349-368.
[260] Fernández Vivas, Y. (2016). Debatiendo: La influencia de la Sentencia de la Corte Interamericana de Derechos Humanos "Claude Reyes contra Chile" en la jurisprudencia del Tribunal Europeo de Derechos Humanos. *Eunomía. Revista en Cultura de la Legalidad,* núm. 9, octubre 2015-marzo 2016. pp. 321-333.

Además, en esa sentencia señala que del examen de la jurisprudencia del TEDH en la materia, se desprende la una evolución perceptible a favor del reconocimiento, en determinadas condiciones, del derecho a la libertad de información como un elemento esencial de la libertad de recibir y difundir informaciones consagrada en el artículo 10 del CEDH. Esta evolución, indica el Tribunal, es también constatable y se refleja en la postura que han adoptado otros órganos internacionales de los derechos humanos, los cuales vinculan el derecho de los "*watchdogs*" de recibir información, con el derecho del público en general a recibirla. Asimismo, se suman a esta consideración que, a la fecha, casi todos los 31 Estados miembros del Consejo de Europa han promovido leyes de acceso a la información, así como que ya en el marco normativo europeo existe el Convenio del Consejo de Europa sobre el Acceso a los Documentos Públicos (CEADP). Sobre la interpretación del artículo 10 del CEDH, el TEDH textualmente señala:

> "155. El objeto y fin de la Convención, como instrumento de protección de los derechos humanos, exige que sus disposiciones sean interpretadas u aplicadas de manera que sus derechos sean prácticos y efectivos y no teóricos e ilusorios (véase la sentencia Soering, antes citada, § 87). Como se desprende claramente de la reciente jurisprudencia del Tribunal y de sentencias de otros órganos de derechos humanos, sostener que el derecho de acceso a la información no puede en ningún caso entrar en el ámbito de aplicación del artículo 10 de la Convención conduciría a situaciones en que la libertad de "recibir y comunicar" información se vería perjudicado de tal forma que se afectaría la esencia misma de la libertad de expresión. Para el Tribunal, en circunstancias en que el acceso a la información es fundamental para el ejercicio del derecho del aplicante de recibir y comunicar información, denegar su acceso puede constituir una injerencia en ese derecho. El principio de asegurar los derechos de la Convención de manera práctica y efectiva requiere que un solicitante en dicha situación pueda confiar en la protección del artículo 10 de la Convención.
>
> 156. En resumen, ha llegado el momento de aclarar los principios clásicos. El Tribunal sigue considerando que "el derecho a la libertad de recibir información básicamente prohíbe a un gobierno restringir el derecho de una persona de recibir información que otros deseen o puedan estar dispuestos a darle." Además, "el derecho a recibir información no puede ser interpretado de forma que se imponga a un Estado obligaciones positivas de recopilar y difundir información de oficio." El Tribunal considera además que el artículo 10 no confiere al individuo un derecho de acceso a la información en poder de una autoridad pública ni obliga al gobierno a impartir dicha información al individuo. Sin embargo, tal y como se desprende del análisis anterior, dicho derecho u obligación puede surgir, en primer lugar, cuando la divulgación de la información ha sido impuesta por una orden judicial que ha adquirido fuerza jurídica (lo que no es un problema en el presente asunto). En segundo lugar, en circunstancias en que el acceso a la información es fundamental para el ejercicio de su derecho a la libertad de expresión, en particular "la libertad de recibir y difundir información" y cuando su denegación constituye una injerencia en ese derecho.
>
> (…)

> 180. En suma, la información requerida por la ONG solicitante a los departamentos de policía pertinentes, era necesaria para completar una encuesta sobre el funcionamiento del plan de defensores públicos que estaba llevando a cabo en su condición de organización no gubernamental de derechos humanos, con el fin de contribuir a la discusión sobre una cuestión de evidente interés público. Al negar el acceso a la información solicitada, que estaba lista y disponible, las autoridades nacionales impidieron que la ONG solicitante ejerciera su libertad de recibir e impartir información, de manera que se afecta el contenido de los derechos del artículo 10. Por lo tanto, ha habido una injerencia en un derecho protegido por esa disposición, que es aplicable a este caso. Procede desestimar la objeción del Gobierno de que la queja de la demandante es incompatible *ratione materiae*."

Para el caso español, la relevancia de las posiciones hasta ahora expuestas, no solo vienen dadas por el reconocimiento del derecho fundamental de acceso a la información pública por parte del TEDH, sino que el cambio de jurisprudencia efectuado por el TEDH podría justificar la especial trascendencia constitucional de un recurso de amparo ante el Tribunal Constitucional (TC), por medio del cual se pretenda el reconocimiento del derecho fundamental de acceso a la información como parte intrínseca del derecho a recibir información contenido en el artículo 20.d) de la Constitución española[261].

B. La naturaleza jurídica del derecho de acceso a la información pública en España

El artículo 105.b) de la Constitución española, confiere el derecho a los ciudadanos de acceder a los archivos y registros administrativos, salvo cuando el acceso suponga una afectación a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas. A diferencia de los derechos fundamentales que aparecen contenidos en el Título I de la Constitución que especialmente se refiere a los derechos y deberes fundamentales, el derecho de acceso mencionado en el artículo 105.b), se ubica en el Título IV que por su parte contiene disposiciones relativas al Gobierno y la Administración.

Esto ha dado origen a diferentes debates sobre si se trata de un derecho fundamental, un derecho de configuración legal o un principio de actuación de las Administraciones Públicas[262]; mientras que en la actualidad las teorías más modernas del

[261] Rollnert Liern, G. (2014). El derecho de acceso a la información pública como derecho fundamental… *op. cit.* pp. 349-368. En similar sentido, desde mismo autor puede verse: Rollnert Liern, G. (2014). La justiciabilidad del derecho de acceso a la información pública ante el Tribunal Constitucional. XII Congreso de la Asociación de Constitucionalistas de España, "Participación, representación y democracia", Salamanca, 3 y4 de abril de 2014.

[262] Piñar Mañas, J.L. (2014). Transparencia y protección de datos. Una referencia a la Ley 19/2013… *op. cit.* pp. 45-57.

derecho de acceso a la información plantean el debate en torno a la consideración del derecho de acceso a la información como un derecho fundamental con carácter autónomo o, si por el contrario, se encuentra contenido dentro de otros derechos fundamentales, como por ejemplo el derecho a la libertad de expresión[263].

El debate no es en vano y trasciende el plano meramente de la discusión académica, pues la ubicación de un derecho dentro de la Constitución Española condiciona su tratamiento jurídico. En el caso concreto, que el derecho de acceso a los documentos esté regulado en el Título IV y no en el Título I que contiene el catálogo de derechos fundamentales tiene, como bien lo menciona GUICHOT REINA[264], "implicaciones jurídicas de gran trascendencia para determinar el alcance y la garantía del derecho, como la necesidad o no de la ley orgánica para desarrollarlo y la posibilidad del Estado de regularlo respecto de todos los poderes públicos de cualquier nivel político, su mayor o menor grado de 'configuración' legal, o su posibilidad de tutela a través del recurso de amparo".

En el ordenamiento jurídico español –sin pretender simplificar ni abarcar de forma extensa este debate jurídico–, la cuestión ha quedado zanjada con la aprobación de la LTAIBG. El legislador finalmente se ha inclinado por reconocer el derecho de acceso a la información como un derecho de configuración legal derivado del artículo 105.b) de la Constitución española y no como parte esencial del derecho fundamental a comunicar y recibir libremente información tutelado en el artículo 20.d) de la Constitución.

Constancia de ello es la equiparación que hace el Preámbulo II de la LTAIBG del derecho de acceso a la información con otras disposiciones contenidas previamente en el ordenamiento jurídico que tienen como punto de partida la previsión contenida en el artículo 105.b) de la Constitución Española. Especialmente, menciona la disposición del artículo 37 de la –ya derogada- Ley 30/1992, de 26 de noviembre, del Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, así como otra normativa sectorial adoptada con el fin de trasponer directivas comunitarias[265] y en la cual se reconocía el carácter de derecho de configuración legal del acceso a la

[263] Guichot Reina, E. (2011). Transparencia versus protección de datos… p. 13.
[264] *Ibíd.*
[265] Entre ellas, la Ley 27/2006, de 18 de julio, por la que se regula el derecho de acceso a la información, de participación pública y de acceso a la justicia en materia de medio ambiente y la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector púbico.

información pública[266]. También, se deja patente el carácter de derecho de configuración legal en su artículo 8, cuando expresamente dispone que "todas las personas tienen derecho a acceder a la información pública en los términos previstos en el artículo 105.B) de la Constitución Española y en esta Ley".

En todo caso, esta posición coincide con la interpretación que hasta ahora han hecho tanto el Tribunal Supremo (TS) como el TC sobre la naturaleza jurídica del derecho de acceso a la información pública[267]. Así, por ejemplo, ya desde la STC 161/1988, de 20 de septiembre, el TC señaló que las reglas y principios contenidos, entre otros, en el artículo 105.b) de la Constitución española son inadecuadas para fundamentar una petición de amparo, pues no reconocen un derecho fundamental o libertad civil incluidos como amparables en el artículo 52.2 de la Constitución[268].

También, puede apreciarse la STS 4291/2012, de 19 de junio, en la que el TS reconoció la imposibilidad de interponer un recurso contencioso especial para la protección de los derechos fundamentales contra una denegación de acceso a la información, pues a criterio del Tribunal el derecho de acceso a los archivos y registros contenidos en el artículo 105.b) de la Constitución española y artículo 37 de la derogada Ley 30/1992 no son en sí mismo un derecho fundamental. No obstante lo anterior, no deja de ser interesante tener en consideración que en la STS 3886/2012, de 29 de mayo, en la que también se reclama el derecho de acceso a documentos en poder de la Administración, el TS indicó que aún y cuando se hubiera admitido "a efectos puramente argumentativos que los artículos 20.1.d) y 23.1 CE engloban el derecho a obtener información de los poderes públicos –algo que dista de ser evidente– la sentencia impugnada no los ha infringido, ya que lo solicitado por la recurrente no era información." Para algunos autores

[266] La Ley 37/2007 expresamente reconocía en su Preámbulo el carácter de derecho de configuración legal del acceso a la información al indicar que "la ley posee unos contornos específicos que la delimitan del régimen general de acceso previsto en el artículo 105 b) de la Constitución Española y en su desarrollo legislativo, en esencia representado por la Ley 30/1992, de 26 de noviembre, del Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común".

[267] En palabras de RAZQUIN LIZARRAGA, "el Tribunal Supremo ha establecido que el derecho de acceso no es un derecho fundamental y por tanto los recursos contra su denegación no se pueden articular por el procedimiento especial de defensa de los derechos fundamentales (Sentencia de 19 de junio de 2012), aunque sea un derecho conocido constitucionalmente (STS de 6 de junio de 2005) que exige una interpretación favorable al derecho de acceso (STS de 16 de diciembre de 2011)". Razquin Lizarraga, M.M. (2015). El derecho de acceso a la información pública. Teoría y práctica, en especial, para las entidades locales. Oñati: Instituto Vasco de Administración Pública. p .20

[268] Para autores como ROLLNERT LIERN esto no debía invitar a confusión, pues el pronunciamiento del TC guardaba relación con si el artículo 105.b) era susceptible de ser base para la interposición de un recurso de amparo pero no así respecto de si el artículo 20.d), que sí es tutelable por medio de un recurso de amparo, engloba un derecho fundamental de acceso a la información pública.

como GUICHOT REINA, esto debe ser entendido no como una denegación expresa del TS al reconocimiento del derecho de acceso a la información como parte de algún otro derecho fundamental, sino como que ha preferido "mantener la cuestión imprejuzgada".[269]

A pesar de esto, cabe resaltar que *Access Info Europe*, actora del proceso judicial en el que se dictó la STS 3386/2012 interpuso un recurso de amparo ante el TC, el cual fue rechazado por medio de una providencia de 9 de octubre de 2013 *"dada la manifiesta inexistencia de violación a un derecho fundamental tutelable en amparo"*[270]. Ante esta decisión, la organización ha optado por interponer una demanda ante el TEDH para reclamar el reconocimiento del derecho de acceso a la información como derecho fundamental que también ha sido inadmitida[271].

Ahora bien, este reconocimiento del derecho de acceso a la información como un derecho de configuración legal y no como un derecho fundamental –quizá no autónomo pero si contenido dentro de la previsión constitucional del artículo 20.d) –, ha valido una parte de las críticas más importantes a la LTAIBG y su tramitación como ley ordinaria y no como ley orgánica. Si bien constituye un avance significativo, no puede obviarse que teniendo la oportunidad el legislador de adoptar una legislación moderna y acorde a las tendencias de la mayoría de los países democráticos de occidente, aprobó la LTAIBG que reconoce un derecho de acceso a la información muy inferior a cualquier otro derecho fundamental contenido en la Constitución Española.

No es de extrañar, como lo menciona DE LA NUEZ SÁNCHEZ CASCADO[272], que la LTAIBG parezca antigua pues lo cierto es que nace bajo una concepción que no es acorde con el paradigma actual de gobierno abierto, sino que por el contrario, nace desde una óptica de Derecho administrativo tradicional; desde un paradigma cada vez más superado que es el de la Administración Napoleónica. Se suma a esta crítica de la visión meramente

[269] Guichot Reina, E. (2012). El proyecto de Ley de Transparencia y acceso a la información pública y el margen de actuación de las Comunidades Autónomas. *Revista Andaluza de Administración Pública*. Núm. 84, Sevilla, septiembre-diciembre (2012). pp. 89-134.
[270] Así consta en el formulario de demanda interpuesto ante el TEDH consultable en el siguiente enlace: https://www.access-info.org/wp-content/uploads/Formulario_Demanda_TEDH_final.pdf
[271] Ver nota de prensa publicada por *Access Info Europe* en el siguiente enlace: https://www.access-info.org/es/sin-categorizar/13804
[272] De la Nuez Sánchez Cascado, E. (2012). El proyecto de Ley de Transparencia, Acceso a la Información Pública y Buen Gobierno ¿Una ley gatopardesca?. Recuperado de: http://hayderecho.com/2012/09/24/el-proyecto-de-ley-de-transparencia-acceso-a-la-informacion-publica-y-buen-gobierno-una-ley-gatopardesca/

administrativista de la LTAIBG MORETÓN TOQUERO[273], quien lamenta que, pese a la relevancia política de la transparencia, el legislador no haya optado por un abordaje desde el Derecho constitucional, con las graves consecuencias que deriva del abordaje solo desde el Derecho administrativo.

SÁNCHEZ DE DIEGO[274] también se une a esta posición y enfatiza en el anclaje constitucional de la LTAIBG únicamente al artículo 105.b) de la Constitución y la continua referencia en la Ley a su aplicación en forma exclusiva a actividades sujetas a Derecho administrativo, lo cual supone que existan áreas fuera de la aplicación de la LTAIBG. En sentido similar, RAMS RAMOS[275] ha criticado que pese al reconocimiento internacional del derecho de acceso a la información como un derecho fundamental, el legislador español se muestra "ajeno" a dicha realidad y vincula el acceso a la información únicamente al artículo ya mencionado de la Constitución Española y lo regula como un derecho ordinario.

En su comparecencia ante la Comisión Constitucional de Congreso en la tramitación del proyecto de LTAIBG, GUICHOT REINA fue igualmente enfático en la crítica a la consideración del derecho de acceso a la información como un derecho de configuración legal y no como un derecho de carácter fundamental y expuso ante el Congreso que:

> "[le] parece difícil cuestionar a día de hoy que el acceso a información sobre la gestión pública, que solo está en poder de la Administración pública y que, por tanto, contribuye de forma esencial a la formación de una opinión pública informada, no está dentro del derecho fundamental a la libertad de información, y que este es sólo un derecho de abstención de la censura. Como nota política les diré que desde un punto de vista sociológico, desde el que también hay que interpretar adicionalmente los derechos, difícilmente a los ciudadanos se les puede explicar en 2013 que el derecho de acceso a la información y la transparencia no son un derecho fundamental".

Incluso, con ocasión del segundo aniversario de la entrada en vigor de la LTAIBG en diciembre de 2016, un grupo de cincuenta académicos españoles, entre los que se encuentran destacados profesores que se han encargado de estudiar la materia, como por ejemplo: GUICHOT REINA, PIÑAR MAÑAS, SÁNCHEZ DE DIEGO, DE LA NUEZ, VILLORIA

[273] Arancha Moretón Toquero, citada por Manuel Sánchez de Diego, en: Sánchez de Diego Fernández de la Riva, M. (2014) Transparencia y acceso a la información desde una perspectiva constitucional. *Iurisprudentia Elegans: Revista de Derecho Político e Historia Constitucional*, núm. 1, 2014. pp. 30-55
[274] Sánchez de Diego Fernández de la Riva, M. (2014) Transparencia y acceso a la información desde una perspectiva constitucional. *Iurisprudentia Elegans: Revista de Derecho Político e Historia Constitucional.* Núm. 1, 2014. pp. 30-55
[275] Rams Ramos, L. (2016). Tratamiento y acceso público a documentos oficiales… *op. cit.* pp. 601-619.

entre otros destacados, firmaron una declaración por medio de la cual hacían un llamado a las autoridades públicas sobre la necesidad de reconocer el derecho de acceso a la información pública como un derecho fundamental, pues es parte esencial del derecho a comunicar o recibir información que tutela el artículo 20.1.d) de la Constitución española[276].

Asimismo, para finalizar la aproximación crítica a la naturaleza de configuración legal del derecho, debe recordarse que el catálogo de derechos no es cerrado y no es la primera vez que se recurre a la creación de un derecho aún y cuando no se encuentre previsto de forma expresa. La mayoría de la doctrina que se ha encargado de promover la naturaleza de derecho fundamental del acceso a la información pública como parte del derecho fundamental a la libertad de expresión o cualquier otro que se encuentre íntimamente relacionado e incorporado dentro del catálogo de derechos fundamentales, recuerda que tanto el legislador como el TC, reconocieron un derecho fundamental a la protección de datos que no se encuentra contenido de forma expresa en el artículo 18.4 del texto constitucional.

3. Las implicaciones de la consideración del derecho al acceso a la información pública como derecho de configuración legal frente a la protección de datos personales

La consideración del derecho de acceso a la información como un derecho de configuración legal, en relación con el artículo 105.b) de la CE y no en relación con un derecho fundamental de asidero constitucional como el derecho a la libertad de expresión, como ya se ha insistido, no resulta una cuestión nimia. En la práctica, la configuración legal del acceso a la información conlleva inconvenientes que van desde el ámbito de aplicación –todos los poderes públicos o solo una parte de ellos–, hasta la relación y los límites que se deriven del vínculo con otros derechos.

La desventaja en la que se encuentra el derecho de acceso a la información respecto de los derechos fundamentales contenidos en el catálogo de la CE es a todas luces evidente. Al tener el derecho de acceso a la información contenido en el artículo 105.b) de la CE un carácter ordinario frente a cualquier otro derecho fundamental tutelado

[276] La declaración suscrita por los cincuenta académicos titulada "*Por el reconocimiento del derecho de acceso a la información como un derecho fundamental"* puede ser consultada en el siguiente enlace: https://www.access-info.org/es/frontpage-es/27052

por el ordenamiento jurídico, se le coloca de forma inmediata en una posición de inferioridad que, como explica ROLLNERT LIERN[277], trae consigo una prevalencia casi que automática de cualquier derecho fundamental, especialmente cuando se está en la aplicación del juicio de ponderación que exige el artículo 14 y, en particular, el artículo 15.3 de la LTAIBG. Coincide con este planteamiento OLMEDO PALACIOS[278], quien considera que la regulación de este derecho como un derecho meramente administrativo y no ligado a un derecho fundamental, no sólo lo deja desprovisto de la protección y garantías propias de un derecho fundamental, sino que de antemano define y prejuzga la ponderación de los intereses que debe llevarse a cabo para conciliar los conflictos que surjan con otros derechos e intereses protegidos por el ordenamiento jurídico.

MORETÓN TOQUERO[279] llama también la atención sobre este punto en particular. La vinculación del derecho de acceso a la información a otros derechos fundamentales le hubiera colocado en una mejor situación frente a cualquier conflicto de derechos que surja, particularmente frente a la configuración del derecho–fundamental– a la protección de datos de carácter personal y la intimidad de la persona como límite al derecho de acceso a la información. El hecho de que este derecho de acceso tenga atribuida una condición de derecho de configuración legal lo sitúa en forma automática en una posición de desventaja y debilidad a la hora de resolver los conflictos que puedan surgir con el derecho a la protección de datos que sí tiene consideración de derecho fundamental y, por ende, un rango superior.

El más claro ejemplo de esta problemática se evidenció en los informes tanto de la AEPD como del Consejo de Estado sobre el Anteproyecto a la LTAIBG, que de manera reiterada le recordaron al legislador que en la ponderación inicial que debía llevar a cabo entre el derecho de acceso a la información y el derecho a la protección de datos a la hora de redactar la norma, no podía obviarse esta distinción así como el carácter de ley orgánica

[277] Rollnert Liern, G. (2014). El derecho de acceso a la información pública como derecho fundamental… *op. cit.* pp. 349-368.
[278] Olmedo Palacios, M. (2014). La Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información y buen gobierno. *Diario La Ley*, (8327).
[279] Moretón Toquero, A. (2014). Los límites del derecho de acceso a la información pública. *Revista jurídica de Castilla y León.* Núm. 33, mayo 2014. Recuperado de: http://www.jcyl.es/web/jcyl/AdministracionPublica/es/Plantilla100Detalle/1215245063566/_/1284319275652/Redaccion

de la LOPD frente al carácter de ley ordinaria de la actual LTAIBG. Así, por ejemplo, la AEPD apuntó que:

> "No debe olvidarse en este punto que el derecho fundamental a la protección de datos aparece reconocido expresamente por la Sección segunda del Capítulo I del Título I de la Constitución, mientras que el derecho de acceso a la información pública, aun siendo una garantía esencial de funcionamiento de un Estado democrático, no aparece incluido en el catálogo de derechos fundamentales y libertades públicas reconocido por la Constitución".

En igual sentido, el Consejo de Estado, que en su mayoría adoptó la posición de la AEPD, indicó en su dictamen:

> "Como es obvio, este inciso inicial no puede ser entendido como una excepción a la aplicación preferente del régimen contenido en la LOPD en materia de garantía y protección de las 'las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar' (artículo 1 de la LOPD) en lo que concierne al tratamiento de los datos personales. El anteproyecto, en cuanto ley ordinaria no puede condicionar ni alterar el régimen de aplicación de la citada Ley Orgánica, ni mucho menos alterar su ámbito de aplicación o desplazarla".

4. El objeto del derecho de acceso a la información en la LTAIBG

La LTAIBG ha venido a suponer uno de los hitos más importantes[280] en la consecución del principio de transparencia en España, por cuanto viene a facilitar, con

[280] Meseguer Yebra señala a este respecto que: " a estas alturas a nadie se le oculta la trascendencia del derecho que regula la LTAIPBG, dada la relevancia que adquiere en nuestros tiempos y su trascendencia en el entendimiento de las relaciones Administración Pública-ciudadano. Como sabemos, la ley supone no solo un paso de gigante en el desarrollo de este derecho de configuración legal [art. 105.b) de la CE], sino que comporta un giro copernicano con respecto a la regulación insuficiente, parcial y dispersa que hasta ahora existía de este derecho en nuestro ordenamiento. El salto de la opacidad y secretismo administrativos a un nuevo concepto de información pública como patrimonio ciudadano es un largo y arduo proceso en el que la LTAIPBG es, sin duda, uno de sus pasos más decisivos. La normativa sobre reutilización de la información pública y el impulso del gobierno abierto (*open government*) son otros dos hitos que marcan el itinerario a seguir para que los poderes públicos recuperen su legitimidad y credibilidad. La única regulación general de este derecho, aparte del referente de la CE, se encontraba en los arts. 35.h) y 37 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (LRJPAC). Además, el art. 3.5 de la LRJPAC dispone que en sus relaciones con los ciudadanos las Administraciones Públicas actúan de conformidad con los principios de transparencia y participación, principios que han obtenido respaldo judicial (SSTS de 31 de julio de 2007 y 3 de junio de 2008). Sin embargo, todos los operadores jurídicos y la jurisprudencia han coincidido en reconocer las insuficiencias y lagunas de esta normativa, que difícilmente podía dar satisfacción a las

luces y sombras, el derecho de acceso a la información pública contenido en el artículo 105.b) de la Constitución española, que dispone que "la ley regulará (….) b) el acceso de los ciudadanos a los archivos y registros administrativos, salvo en lo que afecte a la seguridad y la defensa del Estado, la averiguación de los delitos y la intimidad de las personas".

Y es que la aprobación de la LTAIBG resulta un paso importante en la garantía del ejercicio de este derecho de configuración legal, aspecto sobre el cual ahondaremos más adelante, en el tanto viene a dotar al ordenamiento jurídico de un marco normativo de derecho de acceso a la información pública más estructurado frente al existente, que básicamente consistía en el artículo 37 de la LRJPAC, norma que a criterio de la doctrina, poseía deficiencias notables como la falta de un procedimiento y un órgano de control independiente. Todo ello, condujo a que la norma pasara prácticamente desapercibida y fuera incapaz de generar una cultura de transparencia, ni en los ciudadanos ni en la Administración"[281], situación que ahora ha venido a remediar la LTAIBG.

Enmarcada en un contexto de crisis económica y profunda desconfianza hacia los partidos políticos y la buena gestión por parte de las Administraciones Públicas en 2011 se inició la tramitación de la que dos años después, se convertiría en la actual LTAIBG[282]

---

expectativas generadas por el reconocimiento constitucional del derecho de acceso: se limitaba a documentos relacionados con procedimientos terminados y archivados, establecía restricciones adicionales a las previstas en la CE, inclusivas de una cláusula abierta (podía ser denegado el acceso cuando prevalecieran razones de interés público, intereses de terceros más dignos de protección o cuando así lo dispusiera una ley), lo que hacía depender la efectividad del derecho, *de facto*, de una decisión discrecional de la Administración, máxime cuando el acceso se condicionaba, además, a que no obstaculizara el funcionamiento de los servicios públicos".En: Meseguer Yebra, J. (2014). El procedimiento administrativo para el ejercicio del derecho al acceso a la información pública. *Revista Jurídica de Castilla y León. Revista jurídica de Castilla y León.* núm. 33, mayo 2014. Recuperado de: http://www.jcyl.es/web/jcyl/AdministracionPublica/es/Plantilla100Detalle/1215245063566/_/1284319275652/Redaccion

[281] Guichot Reina, E. (2014). La nueva Ley de Transparencia… *op. cit.* pp. 94-107.

[282] Sobre este particular, se pude ver un análisis detallado y pormenorizado de la tramitación parlamentaria y su contexto en: Guichot Reina, E. (2014). La nueva Ley de Transparencia… *op. cit.* pp. 94-107. Este mismo autor, en otro trabajo en relación con la legislación española en materia de acceso a la información indica que el artículo 37 de la LRJPAC: "se limita a documentos relacionados con procedimientos terminados y archivados, se establece restricciones adicionales a las previstas en la Constitución, inclusivas de una cláusula abierta (según la cual el ejercicio de los derechos que establecen podrá ser denegado cuando prevalezcan razones de interés público, por intereses de terceros más dignos de protección o cuando así lo disponga una ley) que hace depender la efectividad del derecho, de facto, de una decisión discrecional de la Administración, máxime cuando el mismo se condiciona, además, a que su ejercicio no merme la eficacia en el funcionamiento de los servicios públicos. A todo esto hay que sumar la falta de regulación del procedimiento o de creación de instituciones de tutela que libren al demandante de información de tener que acudir a un costoso y lento proceso judicial con efectos disuasorios. Todas estas trabas y condicionantes sitúan a la regulación española en la retaguardia de las modernas regulaciones de acceso". Guichot Reina, E. (2011). Transparencia y acceso a la información pública en España: análisis y propuestas legislativas. Documento de trabajo 170/2011. Recuperado de: http://www.fundacionalternativas.org/.

y solución a la legislación mencionada que era insuficiente y no respondía a las exigencias sociales ni políticas.[283] Esto a través de la consecución de tres objetivos que aparecen mencionados en el artículo 1, que indica que la LTAIBG "tiene por objeto garantizar y reforzar la transparencia de la actividad pública, reconocer y garantizar el derecho de acceso a la información relativa a aquella actividad y establecer las obligaciones de buen gobierno que deben cumplir los responsables públicos así como las consecuencias derivadas de su incumplimiento".

Como se desprende de lo anterior, la LTAIBG tiene como fin regular las dos manifestaciones de la transparencia en la actividad pública: por un lado, la transparencia activa (Capítulo II de la LTAIBG) y, por otro, el derecho de acceso a la información pública (Capítulo III de la LTAIBG). Si bien son manifestaciones del mismo enunciado , cabe destacar que entre ellas existen convergencias, por ejemplo respecto del fin perseguido y los límites que la LTAIBG impone (artículo 5.3 de la LTAIBG), pero también existen elementos característicos que diferencian a uno del otro: mientras que la transparencia activa pretende que los ciudadanos obtengan información sin tener que solicitarla a la Administración, el derecho de acceso persigue que los ciudadanos, a instancia propia, puedan solicitar información pública a las Administraciones.

No obstante sus diferencias, es innegable la correlación entre ambos, ya que a mayor información publicada y disponible por las Administraciones, menor será la necesidad de las personas de reclamarla mediante los procedimientos de solicitud de acceso a la información pública[284]. Sobre este último particular, se observará más adelante algunas resoluciones del CTBG en donde los ciudadanos han ejercido el derecho de acceso ante la escasa o poco pertinente información publicada en los portales de transparencia, lo cual permite sostener la afirmación anterior. Ejemplo de ello es la información que algunas Administraciones publican en sus portales como "agenda" que en realidad no responde a una publicación de la información integral sobre la verdadera agenda del organismo o ente.

En esta ocasión, nos ocuparemos del derecho de acceso a la información previsto en la LTAIBG. Este derecho, según se expresa la ley tiene por objeto garantizar a las personas el derecho de acceder a la información pública en los términos previstos por la

[283] Goig Martínez, J.M. (2015). Transparencia y corrupción. La percepción social ante comportamientos corruptos. *Revista de Derecho UNED*, núm. 17, 2015. pp. 73-107.
[284] Razquin Lizarraga, M.M. (2015). El derecho de acceso a la información pública… *op. cit.* p. 31.

misma LTAIBG, entendiéndose información pública "los contenidos o documentos, cualquiera que sea su formato o soporte, que obren en poder de alguno de los sujetos incluidos en el ámbito de aplicación de este título y que hayan sido elaborados o adquiridos en el ejercicio de sus funciones" (artículo 13 LTAIBG) ajustándose al CEADP[285].

Para MORETÓN TOQUERO, "una interpretación conforme al principio de accesibilidad máxima, acorde con una configuración amplia del derecho de acceso (a la que se refiere la Exposición de Motivos) requiere que la posibilidad de acceso sea efectivamente la regla general, permitiendo que el ejercicio de este derecho recaiga sobre todas las informaciones de las que disponen los poderes públicos, en la línea de lo que dispone el Convenio del Consejo de Europa, cuando en su preámbulo manifiesta que "todos los documentos públicos son en principio públicos y sólo pueden ser retenidos para proteger otros derechos e intereses legítimos", y remarcando también con ello el carácter instrumental de la publicidad."[286]

A los límites a los que se hace referencia y que constituyen una excepción a la regla generalizada de la transparencia[287], han quedado plasmados en el artículo 14 y 15 de la LTAIBG[288]. El artículo 15 contempla una excepción en relación con la protección

[285] GUICHOT REINA alude que la utilización del concepto de información pública es más ventajoso que la mayoría del derecho comparado e incluso, el CEADP que refiere el acceso únicamente a los documentos públcicos. Ver en Guichot Reina, E. (2014). La nueva Ley de Transparencia… *op. cit.* p. 104. Por su parte, el CEADP en su artículo 1.2.b) define documento público como "toda la información registrada [archivada] de cualquier forma, elaborada o recibida, y en posesión de las autoridades públicas". No obstante lo anterior, KOMANOVCS no reconoce dicha distinción y refiere a un concepto tan amplio como el de la LTAIBG cuando indica que "the definition of "official document" is very progressive in the Convention: it includes all information recorded in any form, drawn up or received and held by public authorities to provide access to existing documents as wee as to search for documents if the applicant cannot actually identify the document he wishes to receive or if it is not easily accessible and, if necessary, to extract and compile information from various documents if the requested information has not already been compiled. Regrettably, para. 14 of the Explanatory Report stipulates that the conventions does not oblige Parties to create new documents upon requests for information. This interpretation, is however clearly inconsistent with the wording of the Convention. The notion of "official documents" convers any information that is recorded on any sort of physical medium such as written texts, information recorded on a sound or audiovisual tape, photographs, e-mails, information stored in electronic format such as electronic databases, etc.)". Ver en: Komanovics, A. (2010). Transparent Europe? The Council of Europe Convention on Access to Official Documents. *Boletín JADO,* Bilbao, año VIII, núm. 19, mayo, 2010. pp. 141-170.

[286] Moretón Toquero, A. (2014). Los límites del derecho de acceso a la información pública… *op. cit.*

[287] Razquin Lizarraga, M.M. (2015). El derecho de acceso a la información pública… *op. cit. p. 43.*

[288] Sobre estas disposiciones, la exposición de motivos de la LTAIBG señala: "el Capítulo III configura de forma amplia el derecho de acceso a la información pública, del que son titulares todas las personas y que podrá ejercerse sin necesidad de motivar la solicitud. Este derecho solamente se verá limitado en aquellos casos en que así sea necesario por la propia naturaleza de la información –derivado de lo dispuesto en la Constitución Española- o por su entrada en conflicto con otros intereses protegidos. En todo caso, los límites previstos se aplicaran atendiendo a un test de daño (del interés que se salvaguarda con el límite) y de interés público en la divulgación (que en el caso concreto no prevalezca el interés público en la divulgación de la

de datos personales de la que nos ocuparemos de manera amplia más adelante, mientras que el artículo 14 contiene una lista importante de limitaciones al derecho, entre las cuales destacan la seguridad nacional, la defensa, las relaciones exteriores, la seguridad pública, la prevención, investigación y sanción de ilícitos penales, administrativos o disciplinarios, la igualdad de las partes en procesos judiciales, las funciones administrativas de vigilancia, inspección y control, los intereses económicos y comerciales, la política económica y monetaria, el secreto profesional y la propiedad intelectual, confidencialidad en los procesos de toma de decisión y la protección del medio ambiente. Límites que han sido calificados por parte de la doctrina, como amplios desde un punto de vista objetivo, así como indeterminados en su redacción[289].

En cuanto al procedimiento para el ejercicio del derecho de acceso a la información, este aparece regulado en el artículo 17 de la LTAIBG, que dispone que el mismo da inicio con la presentación de la solicitud correspondiente ante el órgano administrativo o entidad que posea la información. Una vez presentada la solicitud, el órgano correspondiente decidirá sobre la admisión de la misma, siendo que puede inadmitirla por ser información que está curso de elaboración o publicación general, tiene carácter auxiliar o de apoyo, requiere una acción previa de reelaboración, o no sea el órgano competente para poseer la información. No se requiere que se justifique la solicitud, pero se permite que se motive ante el órgano correspondiente. Sin perjuicio de ello, la LTAIBG es clara en indicar que la ausencia o falta de motivación, no es por sí sola una causa de rechazo de la solicitud.

La resolución que emita el órgano correspondiente debe indicar si se concede o no el acceso a la información y deberá notificarse en el plazo máximo de un mes desde que el órgano competente recibió la solicitud para resolver, plazo que puede ampliarse ante el volumen y complejidad de la información a la que se solicita el acceso. Si se

información) y de forma proporcionada y limitada por su objeto y finalidad. Asimismo, dado que el acceso a la información puede afectar de forma directa a la protección de los datos personales, la Ley aclara la relación entre ambos derechos estableciendo los mecanismos de equilibrio necesarios. 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.

[289] Moretón Toquero, A. (2014). Los límites del derecho de acceso a la información pública… *op. cit.* GUICHOT REINA también apunta que durante la tramitación parlamentaria, se generó un intenso debate en cuanto a si "todos los bienes que pueden suponer un límite al acceso están justificados y si su enunciado es o no demasiado genérico o inconcreto." Ver en: Guichot Reina, E. (2014). Límites a la transparencia y el acceso a la información. En E. Guichot Reina (Coord.). Transparencia, Acceso a la Información Pública y Buen Gobierno. Estudio de la Ley 19/2013, de 9 de diciembre. Madrid: Technos. pp. 97-142

deniega el acceso a la información, lo que resulta de interés para el análisis que se efectuará más adelante, deben indicarse las razones por las cuales se ha denegado la solicitud.

Recapitulación

Pese a que a nivel global la tendencia a reconocer el derecho de acceso a la información como un derecho de carácter fundamental es creciente, llama poderosamente la atención a posición del legislador español y de los tribunales de justicia que se niegan a reconocer, a contracorriente, su carácter iusfundamental. Se insiste únicamente en el reconocimiento del derecho a partir de la premisa de que está contenido en el artículo 105.b) que se encuentra fuera del catálogo de derechos de la Constitución española y se obvia por completo la posibilidad de reconocer su carácter de derecho fundamental esencial comprendido dentro del derecho a la libertad de expresión y el derecho a recibir y difundir informaciones.

Lo anterior resulta más que un absurdo en una obstinación al reconocimiento de un derecho fundamental, que no sólo está ampliamente reconocido con ese carácter en el derecho comparado, sino que ha sido avalado ampliamente por los tribunales internacionales como la Corte IDH y el TEDH. Sobre la sentencia del caso Claude Reyes, poco queda más que decir que desarrolla ampliamente el contenido y alcance del derecho fundamental al acceso a la información, y de la jurisprudencia del TEDH, vale agregar que si bien no llega a la profundidad que llegó la sentencia del a Corte IDH, sí que tiene al día de hoy una sólida línea jurisprudencial que reconoce el derecho de acceso a la información como un derecho fundamental.

No es por ello gratuito que las principales críticas a la LTAIBG hayan nacido con ocasión de este reconocimiento puramente administrativista del derecho al acceso a los documentos, con todos los inconvenientes que ello significa, en especial, cuando entra en interacción con otros derechos que sí tienen reconocido un carácter de derecho fundamental, como la protección de datos personales –de paradójica creación jurisprudencial-. En este sentido y en coincidencia con algunos autores ya citados, la LTAIBG nace desfasada y

responde a un paradigma que ya se encuentra ampliamente superado, en contraposición con las tendencias más modernas que promueven el derecho de acceso a la información como mecanismo de control de la buena gestión de la Administración.

Es a todas luces evidente que la relación que existe entre transparencia, derecho –de configuración legal- al accesos a los documentos y derecho –fundamental- a la protección de datos de carácter personal, se encuentra claramente determinada por el rango normativo de cada uno de ellos. La transparencia como principio rector de las actuaciones de la Administración Pública y el derecho de acceso a los documentos como derecho de configuración legal, se encuentran en una clara desventaja frente al derecho a la protección de datos personales, que tiene reconocido su carácter iusfundamental.

Así ha quedado plasmado por ejemplo en los informes que oportunamente rindió la AEPD y el Consejo de Estado en relación con el anteproyecto de ley de la LTAIBG, en que en el que abiertamente expresaron la improcedencia de pretender introducir limitaciones al derecho a la protección de datos personales –regulado en una ley orgánica- por medio de una ley ordinaria como lo es la LTAIBG.

De ahí que como se verá más adelante, aún y cuando la propia LTAIBG trata de acortar esta brecha entre derechos mediante la creación de criterios objetivos de conciliación que llevan a la ponderación en determinados supuestos, es naturalmente más factible que la balanza se incline hacia el derecho a la protección de datos personales en algunos casos. Para algunos autores, esta ponderación no es más que un intento de elevar a rango cuasi-constitucional el derecho de acceso a la información porque de lo contrario, sería evidente que en el tanto el derecho a la protección de datos personales es un derecho fundamental, necesariamente prevalecerá sobre cualquier otro derecho de configuración legal.

Queda aún camino por recorrer en el reconocimiento del derecho al acceso a la información pública como un derecho iusfundamental, cuando no autónomo, por lo menos ligado y como derecho esencial a la libertad de expresión y de recibir y difundir comunicaciones. Hasta que ello no suceda, no podremos

hablar de una verdadera ponderación "on an equal footing" como lo ha reconocido la jurisprudencia del TJUE en los casos resueltos en los que ha aplicado la ponderación como solución al conflicto entre transparencia, acceso a la información y protección de datos personales.

Cuarta parte

El necesario equilibrio entre transparencia, acceso a la información y protección de datos y su regulación en la Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno

Capítulo VII. La excepción de protección de datos contenida en la Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno

SUMARIO: 1. Cuestiones preliminares. 2. La relación entre transparencia, acceso a la información y protección de datos personales en la LTAIBG: la solución normativa al conflicto mediante una excepción relativa a la protección de datos personales. 3. El régimen de excepciones contenido en el Anteproyecto de LTAIBG. A. Informe preceptivo de la AEPD sobre el Anteproyecto de la LTAIBG. B. Dictamen 707/2012 del Consejo de Estado, de 19 de julio de 2012. 4. Reformulación de la excepción de protección de datos en la LTAIBG.

1. Cuestiones preliminares

En la regulación de la transparencia, el acceso a la información y protección de datos personales, el legislador español ha optado por dirimir este conflicto a través de la creación en la LTAIBG de una excepción al acceso a la información en función de los datos de carácter personal.

En este apartado nos referiremos a dicha excepción y en especial, a su planteamiento desde el anteproyecto de ley hasta su aprobación final por el Senado, pues las variaciones efectuadas a la propuesta inicial hasta el texto final, han sido sustanciales y con una incidencia profunda para la solución del conflicto de derechos que se analiza en este trabajo.

Para ello se estudiarán los informes de la AEPD y el Consejo de Estado, que han terminado por moldear la excepción que estaba prevista en el anteproyecto de ley hasta la versión finalmente aprobada, así como otras cuestiones que han saltado a la luz a la hora de replantear la excepción de protección de datos inicialmente propuesta.

2. La relación entre transparencia, acceso a la información y protección de datos personales en la LTAIBG: la solución normativa al conflicto mediante una excepción relativa a la protección de datos personales

A diferencia de lo que ocurre en ordenamiento comunitario, en donde a falta de una regulación expresa[290], los esfuerzos para encontrar los puntos de convergencia entre la normativa propia del derecho de acceso a los documentos y el derecho a la protección de datos de carácter personal han dependido del desarrollo jurisprudencial del TJUE, en el ámbito doméstico el legislador español ha prestado especial atención y ha regulado con *"*especialidad e intensidad*"*[291] las relaciones y los conflictos que se suscitan en este campo, en especial a través de la configuración de los datos de carácter personal como un límite al acceso a la información pública.

El apartado I del preámbulo de la LTAIBG resalta la importancia de la transparencia y su manifestación concreta a través de la publicidad activa y el derecho de acceso a la información en cualquier sociedad democrática, en donde los ciudadanos

[290] Problema que a criterio de GUICHOT debería venir solucionado en la propuesta de reforma al Reglamento 1049/2001. Para este autor, la propuesta de reglamento debería "perfilar las relaciones entre publicidad y reserva, aportando unas directrices que creo deberían contemplarse en la regulación en aras de la seguridad jurídica y tomando los elementos más convincentes de los Derechos más evolucionados. De forma sintética: 1°) Una regulación tal debe explicitar cuál es la normativa aplicable. El principio general, acogido muy mayoritariamente en el Derecho comparado, debe ser que la normativa sobre acceso constituye ley especial en las demandas de información pública, salvo cuando se trata del propio interesado que pide acceso a información que sólo a él le concierne. 2°) Desde un punto de vista material debería partirse de la necesidad de conciliación de la transparencia y el acceso a la información y la intimidad y la protección de los datos personales, siendo ésta a mi juicio una adaptación a la nueva realidad informacional de aquélla. Probablemente, lo más coherente con la tendencia a la afirmación de la protección de datos como un derecho fundamental autónomo y a la falta de una mayor concreción de los límites de este derecho y la distinción entre lo "personal", aún en proceso de construcción dogmática acabada, consiste en entender que siempre es necesario ponderar, si bien dicha ponderación no debe hacerse a ciegas, sino que corresponde al legislador proveer al aplicador de las directrices generales que permitan restringir el por lo demás casi siempre necesario ámbito de la ponderación *ad causam*. Como directriz, podría al menos establecerse aquella según la cual, los datos más próximos al núcleo duro de la intimidad (fundamentalmente, los datos sensibles o especialmente protegidos, en la terminología de la normativa sobre protección de datos) deben ser los más resistentes a la publicidad, mientras que los directamente relacionados con la organización y la actividad pública (actividad pública de las autoridades y empleados públicos, representantes privados en reuniones con organismos públicos, subvenciones, contratos, autorizaciones y licencias, etc.) deben ser objeto de publicidad, abriendo en ambos casos un portillo para la excepción en casos singulares y justificados (conectando así con las nociones de "interés público y "derecho de oposición", que están en buena medida ínsitas en el propio principio de ponderación). 3°) Desde el punto de vista procedimental, resulta clave, cuanto menos, la información y audiencia de los afectados en las demandas de acceso, para una correcta ponderación. Debe advertirse, en todo caso, respecto al tercero cuyos datos personales figura en el documento, que derecho a ser escuchado no significa derecho de veto, y que sólo debe dársele entrada cuando legal o jurisprudencialmente no resulte claro que deba concederse o denegarse el acceso, pues de lo contrario, se corre el riesgo de generar una burocracia y una ralentización del procedimiento (p. ej., consultando a cada funcionario si su identidad o dirección profesional puede ser comunicada)…". Ver en: Guichot, Reina, E. (2011). Las relaciones entre transparencia y privacidad… *op. cit.* pp. 37-69.

[291] Cotino Hueso, L. (2014). La nueva ley de transparencia y acceso a la información. *Anuario de la Facultad de Derecho, Universidad de Alcalá*, núm. VII (2014). pp. 241-256.

participan del proceso de toma de decisiones y exigen rendición de cuentas a los responsables. Expresamente menciona el apartado citado que "la transparencia, el acceso a la información pública y las normas de buen gobierno deben ser los ejes fundamental de toda acción política Sólo cuando la acción de los responsables públicos se somete a escrutinio cuando los ciudadanos pueden conocer cómo se toman las decisiones que les afectan, cómo se manejan los fondos públicos o bajo qué criterios actúan nuestras instituciones podemos hablar del inicio de un proceso en el que los poderes públicos comienzan a responder a una sociedad que es crítica, exigente y que demanda participación de los poderes públicos".

Más adelante ese mismo apartado del preámbulo señala los tres principales objetivos o alcances de la ley, "incrementa y refuerza la transparencia en la actividad pública –que se articula a través de obligaciones de publicidad activa para todas las Administraciones y entidades públicas–, reconoce y garantiza el acceso a la información –regulado como un derecho de amplio ámbito subjetivo y objetivo– y establece las obligaciones de buen gobierno que deben cumplir los responsables públicos así como las consecuencias jurídicas derivadas de su incumplimiento –lo que se convierte en un exigencia de responsabilidad para todos los que desarrollan actividades de relevancia pública".

De esta manera, el legislador fija de forma el carácter transversal de la LTAIBG, la cual debe ser como expresamente lo indica, el eje fundamental de toda acción política. De forma tal que, como menciona BURGAR ARQUIMBAU, "resulta posible afirmar que los principios y enunciados contenidos en la LTAIBG están llamados a informar el conjunto de la actividad pública, en consonancia con los principios inspiradores contenidos en el artículo 1, párrafo segundo, del Tratado de la Unión Europea".[292] Además, sus principios y enunciados resultan aplicables a la doble vertiente de la transparencia que regula la LTAIBG: la publicidad activa y el derecho de acceso a la información pública.

No obstante lo anterior, el legislador incluyó asimismo en el preámbulo de la LTAIBG, un reconocimiento expreso de la relación existente entre transparencia, acceso a la información y protección de datos de carácter personal, así como la necesidad de

[292] Burgar Arquimbau, J. M. (2014). Aproximación a la protección de datos de carácter personal en el marco de Ley de transparencia, acceso a la información pública y buen gobierno. *Revista Digital CEMCI*, núm. 23, de abril a septiembre de 2014. Recuperado de: http://revista.cemci.org/numero-23/pdf/revista-cemci-numero-23.pdf

garantizar un equilibrio en la tutela de estos derechos, pues son claras las tensiones que derivan de definir el ámbito de aplicación de estos derechos[293]. Como acertadamente lo indica Arenas Ramiro, "la exigencia de transparencia y el acceso a la información del sector público muestra su lado más conflictivo cuando dicha información es información personal, esto es, cuando son datos personales".[294]

En ese sentido, el apartado III del preámbulo expresa con claridad que "dado que el acceso a la información puede afectar directamente la protección de los datos personales, la Ley aclara la relación entre ambos derechos estableciendo los mecanismos de equilibrio necesarios. 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".

Como bien lo indica GUICHOT REINA, "la relación entre ambos valores (publicidad y privacidad) o derechos (de acceso a la información y a la intimidad y protección de datos) es potencialmente conflictiva. Convergen en un punto de conexión, la divulgación por las autoridades públicas de información que contiene datos personales, lo que requiere dilucidar cuál es la normativa aplicable y las determinaciones sustantivas, procedimentales, de garantías y organizativas que permitan maximizar la eficacia de ambos derechos".[295]

El reconocimiento de este vínculo y su adecuada regulación, resultó en la inclusión en el texto normativo de una excepción en función de la protección de datos de carácter personal que persigue garantizar ese equilibrio en los supuestos en que el acceso a la información implique, por su contenido, la necesaria valoración del acceso a la misma a la luz de la normativa de protección de datos de carácter personal y del artículo 18.4 de la Constitución Española.

---

[293] Tejedor Bielsa, J. C. (2014). A la búsqueda del equilibrio entre transparencia administrativa y protección de datos. Primeros desarrollos en el ámbito municipal. *Gestión y Análisis de Políticas Públicas. Nueva Época, núm. 12 julio-diciembre 2014.* Recuperado de: https://revistasonline.inap.es/index.php?journal=GAPP&page=article&op=view&path%5B%5D=10205&path%5B%5D=10687

[294] Arenas Ramiro, M. (2016). Transparencia, acceso a la información pública y democracia… *op. cit*. pp. 113-131.

[295] Guichot Reina, E. (2011). Transparencia versus protección de datos… *op. cit.* p. 3.

El artículo 15 de la LTAIBG se encarga de regular estas relaciones. Si bien ahora parece estar claramente definida dicha disposición normativa, cabe notar que en un principio la excepción prevista en virtud de la protección de datos de personales en el Anteproyecto de Ley, limitaba el ámbito de aplicación de la normativa de protección de datos y no contaba con criterios objetivos de ponderación, salvo dos que hubieran resultado en la práctica de difícil precisión. Lo anterior hace que resulte necesario para entender el alcance y el ámbito para aplicar la excepción en virtud de la protección de los datos personales, hacer un breve recorrido por la redacción de la norma según se contemplaba en el Anteproyecto de Ley, según fue modificada en el Proyecto de Ley con base en las recomendaciones de la AEPD y el Consejo de Estado y, por último, la versión que fue aprobada finalmente en el Senado.

3. El régimen de excepciones contenido en el Anteproyecto de la LTAIBG

Desde sus inicios, el Anteproyecto de la LTAIBG incluyó una disposición destinada a resolver la problemática que suscita la armonía entre el derecho de acceso a la información pública y la protección de datos de carácter personal. Como menciona RODRÍGUEZ ÁLVAREZ[296], a efectos de comprender el alcance y contenido de la excepción que contempla el texto normativo finalmente aprobado (artículo 15 de la LTAIBG), resulta indispensable comprender las desventajas o las principales críticas que se le podían formular a la propuesta de excepción inicial contenida en el artículo 11 del Anteproyecto de Ley.

El Anteproyecto proponía el siguiente régimen de excepciones, en virtud de la protección del derecho a la intimidad y la protección de datos de las personas:

> "Artículo 11. Protección de datos personales.
> 1. Cuando la solicitud de acceso se refiera a información pública que contenga datos de carácter personal se aplicarán las disposiciones previstas en esta Ley. No obstante, se aplicará la normativa de protección de datos personales cuando los datos que contenga la información se refieran únicamente al solicitante.
> 2. Si la información solicitada contuviera datos especialmente e protegidos en los términos de la normativa de protección de datos personales, se denegará el acceso salvo que el titular de los datos consienta expresamente y por escrito su divulgación.

[296] Rodríguez Álvarez, J.L. (2016). Transparencia y protección de datos personales: criterios legales de conciliación. En D. Canals Ametler (ed.), *Datos. Protección, Transparencia y Buena Regulación.* Recuperado de: www.documentauniversitaria.com

3. Con carácter general y, salvo que en el caso concreto prevalezca la protección de datos personales sobre el interés público o en la divulgación que lo impidan, se concederá el acceso a información que contenga datos vinculados con la organización, funcionamiento o actividad púbica del órgano.
4. Asimismo, se podrá conceder el acceso a información que contenga datos personales que no tenga la consideración de especialmente protegidos, si previa ponderación suficientemente razonada, el órgano competente para resolver considera que no se perjudica ningún derecho constitucionalmente protegido.
5. La normativa de protección de datos personales personal será de aplicación al tratamiento posterior de los datos personales obtenidos a través del ejercicio del derecho de acceso".

Como cabe apreciar, lo que perseguía la norma era fijar los criterios de conciliación entre el derecho a la protección de los datos de carácter personal el derecho de acceso a los documentos públicos, a través de un mecanismo dual de excepciones en función de si el documento contenía datos de carácter personal de terceros o si los datos contenidos en el documento pertenecían al solicitante del acceso al documento.

Asimismo, contenía otra serie de supuestos capaces de constituirse como excepción en aras de la tutela de la privacidad de las personas, regulando de forma especial el tratamiento de acceso a los documentos públicos que contienen datos especialmente protegidos, así como una regulación particular en virtud del vínculo de los datos con la organización, funcionamiento o actividad pública del órgano al que se solicita el acceso.

También, concedía la facultad al órgano al que se solicitara el acceso a los documentos de otorgarlo, si habiendo mediado una ponderación suficientemente razonada, estimara que no existía lesión a ningún derecho protegido por la Constitución.

Para finalizar, el mecanismo de excepción dual contenido en el inciso 1 y que básicamente llevaba a la exclusión de la normativa de protección de datos salvo cuando se tratara del acceso a un documento con datos personales del solicitante, fue descartado. Otros de los supuestos mencionados en el artículo 11 del Anteproyecto sufrieron variación siendo también relevante la relativa a los criterios de ponderación a ser tomados en cuenta por la Administración cuando el documento tuviera datos de carácter personal no especialmente protegidos. Para tales efectos, resultaron determinantes tanto el Informe preceptivo sobre el Anteproyecto de Ley emitido por el Gabinete Jurídico de la AEPD y el Dictamen 707/2012 promulgado por el Consejo de Estado el 19 de julio de 2012, a los cuales haremos referencia a continuación.

A. Informe preceptivo de la AEPD sobre el Anteproyecto de la LTAIBG

En lo que se refiere a la excepción contenida en el inciso 1 del artículo 11 del Anteproyecto de Ley, la AEPD señaló que si bien la misma puede operar como una norma especial aplicable en materia de acceso a la información, se debe interpretar de forma integral con las disposiciones que contiene la LOPD, las cuales sin excepción resultan aplicables a cualquier tratamiento de datos que lleven a cabo las Administraciones Públicas. A criterio de la AEPD, la excepción según la redacción que tenía en el Anteproyecto no podía ser interpretada de forma tal que supusiera una exclusión de las obligaciones que la LOPD impone a las Administraciones Públicas.

Asimismo, el Informe señala que la regulación del acceso a la información pública contenido en el entonces Anteproyecto de LTAIBG constituye un supuesto que habilita la cesión de datos sin el consentimiento del interesado, de conformidad con lo dispuesto en el artículo 11.2.a), de la LOPD. Es decir, que la excepción contenida en el Anteproyecto, no excluye la aplicación de la LOPD, sino que por el contrario, constituye un "supuesto legal habilitante de la cesión de datos".

Con base en lo dicho, la AEPD concluye en relación con este extremo que la única interpretación viable del precepto mencionado del Anteproyecto de Ley, es la que parta de que la excepción contenida en el artículo 11.1 de la propuesta legislativa, no excluye la aplicación de la normativa de protección de datos, sino que se trata de precisiones a lo dispuesto en la LOPD. El Informe considera textualmente que "sería preciso que el Proyecto sometido a informe especificase que en los supuestos de acceso a la información pública que contengan datos de carácter personal se aplicarán las disposiciones no sólo del Anteproyecto, sino también de la Ley Orgánica 15/1999".

Por otra parte, el informe puntualiza sobre la precisión que debe realizarse en relación con la segunda frase del artículo 11.1, la cual dispone que la normativa de protección de datos aplicará cuando los datos que contenga la información se refieran exclusivamente al solicitante. A criterio de la AEPD, disponer que la normativa aplica en tales supuestos, puede llegar a limitar el acceso del interesado al documento en el que constan sus datos, el derecho de acceso a los datos de carácter personal que tutela la LOPD en su artículo 15 contempla el derecho a solicitar y obtener información sobre los datos del interesado sometidos a tratamiento, el origen de los datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos, mas no un derecho de

acceso al documento en el que constan tales datos. Esto por cuanto el acceso a los documentos quedaba sujeto a la LOPD, con el inconveniente de que dicha Ley Orgánica garantiza el derecho de acceso a los datos, pero no contiene una provisión que garantice el derecho de acceso a los documentos que los contiene.

Por tales razones, la AEPD estimó oportuno señalar que en "el Anteproyecto debería indicarse que se aplicará la normativa de protección de datos personales cuando los datos que contenga la información se refieran únicamente al solicitante, sin perjuicio de que en este caso el otorgamiento del acceso permita el conocimiento por el solicitante no sólo de los datos contenidos en el documento, sino del documento mismo en que aquéllos consten".

El artículo 11.4, a juicio del Informe presentaba también un roce con los criterios de ponderación aplicables al acceso a documentos que contuvieran datos considerados no especialmente protegidos. A efectos de conceder el acceso a la información que contuviera los datos de carácter personal no especialmente protegidos, la Administración Pública debía llevar a cabo una ponderación suficientemente razonada a efectos de determinar que la concesión del acceso a dichos datos no comportaría una lesión de un derecho constitucionalmente protegido. No obstante lo anterior, tratándose de "información que contenga datos vinculados con la organización, funcionamiento o actividad pública del órgano", debía garantizarse el acceso con carácter general, excepto en aquellos casos donde prevaleciera la protección de los datos sobre el interés público en la divulgación.

Como indica la AEPD, el problema surge ante el hecho de que el único criterio de ponderación a efectos de determinar la procedencia o no del acceso a la información es que la información verse sobre "la organización, funcionamiento o actividad pública del órgano". De más está apuntar como lo hace la AEPD, la dificultad de aplicar e interpretar en la práctica de conceptos como "funcionamiento" o "actividad pública" y que podrían conducir al establecimiento de un acceso con carácter general salvo casos de lesión grave del derecho a la protección de datos.

Sobre este punto, rescata el Informe que "no debe olvidarse […] que el derecho fundamental a la protección de datos aparece reconocido expresamente por la Sección segunda del Capítulo I del Título I de la Constitución, mientras que el derecho de acceso a la información pública, aun siendo una garantía esencial de funcionamiento de un

Estado democrático, no aparece incluido en el catálogo de derechos fundamentales y libertades públicas recogido por la Constitución".

Con el fin de solventar la problemática suscitada, la AEPD pone como ejemplo el criterio de ponderación contenido en la ya derogada Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, la cual disponía que el derecho a la protección de datos del interesado cede ante el interés legítimo del solicitante cuando el documento contenga "datos de carácter nominativo", entendidos estos como aquellos datos meramente identificativos de las personas que no afectan ni su seguridad ni su intimidad.

Otro criterio de ponderación aplicable a estimación de la AEPD es el que resulta de la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español, que dispone de un parámetro temporal a efectos de conceder el acceso a documentos del patrimonio documental cuando contengan, entre otros, datos personales que pueden afectar o perjudicar la intimidad de la vida privada y familiar. De conformidad con el artículo 57 de la Ley, tales documentos del patrimonio documental solo podrán ser accedidos sin consentimiento de los afectados cuando haya transcurrido un plazo de 25 años desde la muerte de los mismos o 50 años a partir de la fecha de los documentos, cuando se desconozca la fecha de muerte del afectado o este no haya fallecido, según ha sido la interpretación de la AEDP.

Asimismo, agrega que siendo que de conformidad con el Anteproyecto, dichos criterios no aplicarán para aquellos datos de carácter personal que hayan sido disociados, resulta indispensable que se garantice el derecho de los interesados al acceso a los documentos que fueron sometidos al procedimiento de disociación.

Concluye la AEPD sobre este punto en específico, sobre la conveniencia de la objetivación de los criterios que se van a utilizar a la hora de realizar la ponderación, con el fin de garantizar un equilibrio en la tutela, tanto del derecho de acceso a los documentos como del derecho a la protección de datos personales. Para tales efectos, considera con base en la normativa existente y los ejemplos citados, que pueden ser tomados como criterios objetivos de ponderación:

> "-La vinculación de los datos con la organización, funcionamiento o actividad pública del órgano requerido, si bien sería conveniente que precisasen en mayor medida los dos últimos conceptos.

> -El carácter nominativo o meramente identificativo de los datos contenidos en la información pública cuyo acceso se solicita.
> -El transcurso de los plazos establecidos en la normativa reguladora del Patrimonio Histórico Español.
> -Que los datos sean solicitados por investigadores que motiven el acceso en fines históricos, científicos o estadísticos;
> -Que el acceso se solicite para el ejercicio de un derecho del propio solicitante.
> -Que los datos contenidos en el documento puedan afectar a la intimidad o a la seguridad de las personas a los que se refieran".

Finalmente, propone una reforma a la redacción del artículo 11, apartados 3 y 4, para que se incluya como criterios objetivos de ponderación:

> "a) El interés público en el conocimiento de la información relacionada con la organización, funcionamiento o actividad pública del órgano requerido.
> b) El menor perjuicio a los interesados derivado del transcurso de los plazos establecidos en el artículo 57 de la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español.
> c) Que los solicitantes justifiquen su petición en el ejercicio por los mismos de un derecho o tengan condición de investigadores que motiven el acceso en fines históricos, científicos o estadísticos.
>
> d) El menor perjuicio de los derechos de los interesados en caso de que los documentos únicamente contuviesen datos de carácter meramente identificativo de aquéllos.
>
> e) La mayor garantía de los derechos de los afectados en caso de que los datos contenidos en el documento puedan afectar a su intimidad o a su seguridad".

B. Dictamen 707/2012, del Consejo de Estado, de 19 de julio de 2012

Con un enfoque distinto, pero que en el fondo coincide con las críticas hechas por la AEPD, el Consejo de Estado aborda la problemática del artículo 11 del Anteproyecto de Ley desde el punto de vista de las fuentes normativas del ordenamiento jurídico español y la imposibilidad de introducir limitaciones a una ley orgánica a través de una ley ordinaria.

En ese sentido, señala que si bien el artículo 11 del Anteproyecto persigue constituirse como un supuesto que habilite la cesión de los datos sin consentimiento del interesado, no puede entenderse que cuando la norma indica que en las solicitudes de acceso que se refieran a datos de carácter personal aplican las disposiciones especiales de la LTAIBG, se está excluyendo la aplicación preferente de la LOPD.

Desarrolla más puntualmente que el Anteproyecto "en cuanto ley ordinaria, no puede condicionar ni alterar el régimen de aplicación de la citada Ley Orgánica, ni mucho menos alterar su ámbito de aplicación o desplazarla. Solo en la medida en que se tratara

de las leyes que prevé el artículo 11.2.a) de la LOPD puede establecer reglas específicas sobre la cesión o comunicación de los datos de carácter personal de los ciudadanos (…)".

En relación con el otro tema de interés, sea el de los criterios objetivos de ponderación en los casos en que la información contenga datos personales no especialmente protegidos, al igual que la AEPD resalta los inconvenientes que pueden derivar de la utilización de conceptos como "interés público en la divulgación de la información" y "derechos de los afectados" como reglas de ponderación.

Según el criterio del Consejo de Estado, el utilizar el concepto de "interés público en la divulgación de la información", debía sustituirse por uno más apropiado y adecuado al derecho a la protección de datos personales, como por ejemplo, "el interés legítimo en el acceso", que no sólo puede constituir un criterio objetivo de ponderación, sino que además respondería mejor a la obligación de que el tratamiento posterior de los datos se ajuste a la LOPD.

Asimismo, sugiere modificar el artículo 11.4, en el tanto concede de forma automática el acceso a la información que contenga datos personales, mientras que para otros casos en que pudieran afectarse derechos o intereses de terceros debidamente identificados, el artículo 16 del Anteproyecto concede un plazo de 15 días para que estos formulen las alegaciones necesarias. Esta diferenciación, estima el Consejo de Estado, provoca un acceso fácil a la información con datos de carácter personal no especialmente protegidos con la consecuente lesión de los derechos del interesado, frente a los supuestos de posible afectación a otros derechos e intereses, en donde se concede un plazo para manifestar lo que se considere oportuno.

4. Reformulación de la excepción de protección de datos en la LTAIBG

Como se puede apreciar, eran notorios los problemas que representaba la redacción del artículo 11 del Anteproyecto de la LTAIBG.

De acuerdo con la tesis del profesor RODRÍGUEZ ÁLVAREZ, dos eran las críticas principales que pueden formularse al artículo 11 del Anteproyecto de Ley, con independencia de la falta de fundamentación o explicaciones que permitan entender la necesidad de haber propuesto o adoptado un régimen dual de excepciones, en función de la titularidad o no de los datos contenidos en el documento público sobre el cual se

solicitara el acceso. Una tercera crítica se puede formular desde la falta de definición de los criterios objetivos de ponderación.

Ahora bien, en cuanto a la primera de las críticas, la redacción del artículo 11.1, del Anteproyecto estaba escrita de forma tal que excluía automáticamente y contrario al ordenamiento español, la aplicación de la normativa de protección de datos personales, salvo en los casos en donde la solicitud de acceso a los documentos contuviera datos personales que se refiriesen exclusivamente al solicitante. En palabras de RODRÍGUEZ ÁLVAREZ, se pretendía "establecer una suerte de reserva a favor de la normativa de transparencia, cuyo efecto directo sería excluir la aplicación de las disposiciones reguladoras de la protección de datos a las solicitudes de acceso a informaciones públicas, excepto cuando los únicos datos afectados fueran los del solicitante".[297]

Este extremo fue señalado como ya lo vimos anteriormente por la AEPD, cuando hacía referencia a que las disposiciones "del artículo 11.1 únicamente podría[n] ser interpretadas de una forma sistemática con las previsiones de la Ley Orgánica" y con la precisión de que se indicase que "en los supuestos de acceso a la información pública que contenga datos de carácter personal se aplicarán las disposiciones no sólo del Anteproyecto, sino también de la Ley Orgánica 15/1999". Más enfáticamente, el Consejo de Estado señaló en su Dictamen que dicho "inciso inicial no puede ser entendido como una excepción a la aplicación preferente del régimen contenido en la LOPD".

Sobre todo, tal y como lo señaló el profesor RODRÍGUEZ ÁLVAREZ en su carácter de Director de la AEPD en la comparecencia, de 23 de enero de 2013, ante la Comisión Constitucional del Congreso de los Diputados[298], resulta difícil conocer y no fueron explicadas las razones por las cuales resultaba en principio más beneficioso contemplar un sistema de excepciones dual que parte de la diferenciación de la titularidad de los datos personales que contiene la información.

La segunda crítica que aparece formulada en el informe de la AEPD y que también menciona RODRÍGUEZ ÁLVAREZ, guarda relación con la inconveniente de la delimitación del ámbito de aplicación tanto de la LTAIBG y la LOPD a la titularidad de los datos que consta en la información pública. Según la redacción del Anteproyecto de Ley, la aplicación de la normativa de transparencia aplicaría en todos los supuestos, salvo en

[297] Rodríguez Álvarez, J.L. (2016). Transparencia y protección de datos personales… *op. cit.*
[298] *Ibíd.*

aquellos en los que los datos contenidos en la información pública se refiriesen al solicitante de acceso, en cuyo caso aplicarían las disposiciones contenidas en la LOPD.

El principal problema estriba aquí, en que como bien lo formuló la AEPD en su Informe, el alcance y el ámbito de aplicación del derecho de acceso a los datos de carácter personal y el derecho de acceso a la información pública, difiere ampliamente el uno del otro. Mientras el derecho de acceso a la información pública regula, justamente, el derecho de toda persona a acceder a la información que esté en poder de la Administración, el derecho de acceso a los datos de carácter personal, según la dimensión que otorgan al mismo tanto la Directiva 95/46 como el artículo 15 de la LOPD concede el derecho del interesado de conocer y obtener la información de los datos que le conciernen y están siendo sometidos a tratamiento.

Al estar tratando en términos homólogos ambos derechos de acceso, se podía incurrir en una limitación seria al derecho de acceso a la información en aquellos casos donde la misma contuviera datos personales del solicitante de acceso, pues este, al estar sujeto únicamente en tales casos a la normativa de protección de datos hubiera tenido solo la posibilidad de acceder a los datos personales, pero no al documento en sí, ya que esa facultad no está reconocida en la normativa de protección de datos. Lo anterior, con la diferencia de que a quienes solicitaran acceso a la información con datos de terceros, no se les vería limitada la posibilidad de acceder el documento.

Sobre este particular, resulta interesante traer a colación la sentencia del Tribunal de Justicia de la Unión Europea (STJUE), de 17 de julio de 2014, caso YS y otros, en donde el TJUE ya había indicado que el derecho de acceso a los datos de carácter personal no confiere un derecho de acceso al documento que los contienen, sino únicamente a los datos que están en poder del responsable o encargado del tratamiento de los datos que le conciernen, exigencia satisfecha cuando se pone en conocimiento del interesado dicha información sin necesidad de dar acceso a la totalidad del documento que los contiene.

Expuesto por RODRÍGUEZ ÁLVAREZ la inviabilidad de la propuesta radicaba en que "al desviar a lo previsto en la normativa de protección de datos los supuestos de ejercicio del derecho de acceso a informaciones que albergasen sólo datos personales del interesado, sin advertir el diferente contenido y alcance de ambos derechos de acceso, la regulación proyectada iba a introducir una clara discriminación entre quienes quisieran acceder a informaciones con datos propios y quienes quisieran acceder a informaciones

con datos de terceros haciendo a los primeros de peor condición, pues mientras que los segundos les sería posible obtener toda la información (tanto la personal como la no personal), los primeros sólo accederían a la información concerniente a sus datos personales que es lo único a lo que da derecho la normativa de protección de datos".[299]

La tercera crítica formulada tanto por la AEPD como por el Consejo de Estado, se vinculaba estrechamente con la redacción que mantenían los apartados 3 y 4 del artículo 11 del Anteproyecto y la falta de criterios objetivos de ponderación en aquellos casos donde la información contuviera datos de carácter personal no especialmente protegidos.

Si bien el Anteproyecto disponía que en los casos en que el documento o la información contuvieran datos de carácter personal no especialmente protegidos, se podría conceder el acceso a la misma, siempre que hubiera mediado una ponderación suficientemente razonada por parte del órgano administrativo al que se dirigiera la solicitud. No obstante, el artículo 11 únicamente preveía como criterios objetivos de ponderación conceptos sumamente amplios como por ejemplo "interés público" o "datos vinculados con la organización, funcionamiento o actividad pública del órgano", que en la práctica llegarían a suponer limitaciones en el ejercicio de los derechos por el carácter indefinido que representaban dichos conceptos.

La mayoría de observaciones y recomendaciones tanto del Consejo de Estado como de la AEPD fueron acogidas y se consignaron en el Proyecto de Ley, que en su artículo 12 mencionaba:

> "1. Cuando la solicitud de acceso se refiera a la información pública que contenga datos de carácter personal se aplicarán las disposiciones previstas en esta Ley. No obstante, se aplicará la normativa de protección de datos personales cuando los que contenga la información se refieran únicamente al solicitante, sin perjuicio de que, es este caso, el otorgamiento del acceso permita el conocimiento por el solicitante no sólo de los datos que contenga la información de los que sea titular, sino de esta en su totalidad.
> 2. Si la información solicitada contuviera datos especialmente protegidos a los que se refiere el apartado 2 del artículo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, el acceso únicamente se podrá autorizar en caso de que se contase con el consentimiento expreso y por escrito del afectado, a menos que dicho afectado hubiese hecho manifiestamente públicos los datos con anterioridad a que se solicitase el acceso.
> Si la información incluyese datos especialmente protegidos a los que se refiere el apartado 3 del artículo 7 de la Ley Orgánica 15/1999, de 13 de diciembre, o datos

[299] Rodríguez Álvarez, J.L. (2016). Transparencia y protección de datos personales… *op. cit.*

relativos a la comisión de infracciones penales o administrativas que no conllevasen la amonestación pública del infractor el acceso sólo se podrá autorizar e n caso de que se cuente con el consentimiento expreso del afectado o si aquel estuviera amparado por una norma con rango de Ley.
3. Con carácter general, y salvo que en el caso concreto prevalezca la protección de datos personales y otros derechos constitucionalmente protegidos sobre el interés público en la divulgación que lo impida, se concederá el acceso a la información que contenga datos meramente identificativos relacionados con la organización, funcionamiento o actividad pública del órgano.
4. Cuando la información solicitada no contuviera datos especialmente protegidos, el órgano al que se dirija la solicitud concederá el acceso previa ponderación suficientemente razonada del interés público en la divulgación de la información y los derechos de los afectados cuyos datos aparezcan en la información solicitada, en particular su derecho fundamental a la protección de datos de carácter personal.
Para la realización de la citada ponderación, el órgano tomará particularmente en consideración los siguientes criterios:

a) El menor perjuicio de los afectados derivado del transcurso de los plazos establecidos en el artículo 57 de la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español.

b) La justificación por los solicitantes de su petición en el ejercicio de un derecho o el hecho de que tengan la condición de investigadores y motiven el acceso en fines históricos, científicos o estadísticos.

c) El menor perjuicio de los derechos de los afectados en caso de que los documentos únicamente os de carácter meramente identificativos de aquellos.

d) La mayor garantía de los derechos de los afectados en caso de que los datos contenidos en el documento puedan afectar a su intimidad o a su seguridad.

5. No será aplicable lo establecido en los apartados anteriores si el acceso se efectúa previa disociación de los datos de carácter personal de modo que se impida la identificación de las personas afectadas.
6. La normativa de protección de datos personales será de aplicación al tratamiento posterior de los datos obtenidos a través del ejercicio del derecho de acceso".

Como se puede observar, la única recomendación que no fue acogida por parte del Congreso de los Diputados en el Proyecto de Ley ni en el texto enviado al Senado, fue la vinculada con la aplicación de dos normativas distintas en virtud de si la información contenía datos personales del interesado que estuviera solicitando acceso o si la información a la que se pretendía acceso únicamente contenía datos de terceros.

No obstante y en relación con ese apartado 1 del artículo 11 del Anteproyecto, sí se hizo la salvedad de que en los casos donde los datos personales que contuviera la información concernieran a quien solicitaba el acceso, se permitiera "el conocimiento por el solicitante no sólo de los datos que contenga la información de los que sea titular, sino de esta en su totalidad". De esta forma, parecía enmendarse la crítica hecha por la AEPD y el Consejo de Estado en relación con la imposibilidad de homologar el derecho de acceso a la información que se pretendía regular a través del proyecto de ley con el

derecho de acceso que regula la LOPD y que no otorga en sí mismo un derecho de acceso a los documentos, sino únicamente a los datos del interesado.

Fue el Senado quien terminó acogiendo la sugerencia d la AEPD y el Consejo de Estado de eliminación del régimen de excepción dual y procedió a eliminar la diferenciación en la aplicación de la normativa en función de la titularidad de los datos personales que constaren en la información.

Pese a que desde la óptica de este trabajo coincidimos con el Informe de la AEPD y el Dictamen del Consejo de Estado, resulta necesario mencionar que algunos autores, como GUICHOT REINA se han mostrado especialmente críticos con el Informe de la AEPD, al punto de afirmar que "se trató de un informe y una propuesta con graves defectos de entendimiento de la lógica del derecho de acceso a la información, que fue asumido de forma acrítica por el Gobierno y que introdujo graves distorsiones en la regulación".[300]

Finalmente, el 10 de diciembre de 2013 se publicó en el Boletín Oficial del Estado número 295, la LTAIBG con una excepción en función de la protección de datos de carácter personal que no discrimina en función de la titularidad de los datos del solicitante de acceso y que cuenta con una serie de criterios objetivos de ponderación que deben ser tomados en consideración por el órgano correspondiente en aquellos supuestos en que la información contenga datos de carácter personal no especialmente protegidos de conformidad con la LOPD.

Recapitulación

La LTAIBG parte del reconocimiento expreso de la tensión entre transparencia, acceso a la información y protección de datos personales, por lo que ha decidido ocuparse de ello mediante la creación de una excepción al acceso a la información pública en razón de los datos de carácter personal y así ha quedado plasmado en su exposición de motivos.

[300] Guichot Reina, E. (2014). La nueva Ley de Transparencia, un reto para la gestión de las organizaciones públicas. *Revista Vasca de Gestión de Personas y Organizaciones Públicas.* Núm 6/2014. pp. 94-107

Ahora bien, el planteamiento de la excepción al acceso a la información en virtud de la protección de los datos personales era uno de los temas trascendentales a resolver, y no es por ello de extrañar que haya ocupado la atención especial de la AEPD, el Consejo de Estado y el sector tanto académico, público y privado que se encontraba apoyando la LTAIBG y que abogaban por un derecho de acceso a la información lo más amplio posible y lo menos limitado, incluyendo dentro de esas limitaciones la relativa a la protección de datos personales.

En un primer momento se plantó una excepción que creaba, como lo menciona la AEPD básicamente una dualidad en cuanto al derecho a la protección de datos personales, ya que se establecía que la LOPD aplicaría únicamente en aquellos casos en que el interesado reclamara el acceso a sus datos personales. Ello traía consigo el problema de que el derecho de acceso tutelado en la LOPD no es un acceso a los documentos sino a los datos, lo que se traducía en la práctica en que un tercero bien podía obtener acceso al documento completo incluidos los datos personales del interesado pero este último sólo tendría acceso a los datos y no al documento en sí.

A criterio de algunos autores, esto se debe a que la AEPD no comprendió bien en ningún momento la excepción planteada, aunque lo cierto a criterio de esta tesis, es que la postura de la AEPD era la correcta y apegada inclusive a la jurisprudencia del TJUE que ha reconocido ya que el derecho de acceso que contiene la Directiva 95/46, es sólo a los datos y no a los documentos, por lo que resultaba necesaria la precisión y la eliminación de ese régimen de excepción.

Esto llevo a que la AEPD, en lo que algunos autores cuestionan por extralimitado, terminara sugiriendo una redacción de la excepción según lo que entendía debería constituirse como límite al derecho de acceso a la información, incurriendo en una serie de imprecisiones técnicas según los criterios más autorizados de la doctrina de derecho de acceso a la información pública.

Asimismo, no debe de dejar de señalarse como ya se hizo anteriormente, el énfasis de la AEPD en el carácter de derecho fundamental del derecho a la protección de datos personales frente al carácter de derecho de configuración legal del derecho al acceso a los documentos y la interpretación que debía hacerse de este último, de forma que resultara acorde con las disposiciones, derechos y principios de la LOPD. Posición que

fue respaldada, a criterio de algunos autores, ciegamente, por parte del Consejo de Estado que no sólo hizo suya la postura de la AEPD sino que enfáticamente señaló que bajo ningún supuesto la LTAIBG podía venir a contradecir lo dispuesto en la LOPD en el tanto su carácter de ley inferior se lo impedía.

Lo cierto es que finalmente se aprobó una excepción con luces y sombras. Si bien por un lado se logró eliminar la dualidad del sistema de excepción, que otorgaba acceso a los documentos a los terceros y sólo a los datos a los interesados, se incorporaron algunas disposiciones que para algún sector de la doctrina no resultan del todo acordes con las tendencias más modernas del derecho de acceso a la información, como por ejemplo, la –mala- referencia a los datos identificativos y los problemas que supone como limitación, cuando básicamente son los datos cubiertos bajo publicidad activa bajo la misma ley, entre otros ya señalados.

Capítulo VIII. Los criterios normativos para la solución del conflicto según la Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno

SUMARIO: 1. Cuestiones preliminares. 2. Los criterios normativos del artículo 15 de la LTAIBG. 3. Criterios normativos de conciliación. A. Datos especialmente protegidos. B. Datos meramente identificativos relacionados con la organización, funcionamiento o actividad pública del órgano. C. Datos de carácter personal no especialmente protegidos: criterios objetivos para la ponderación. a) El menor perjuicio de los afectados derivados del transcurso de los plazos establecidos en el artículo 57 de la Ley 16/1985, de 25 de junio, del Patrimonio Histórico. b) La justificación por los solicitantes de su petición en el ejercicio de un derecho o el hecho de que tengan condición de investigadores y motiven el acceso en fines históricos. c) El menor perjuicio de los derechos de los afectados en caso de que los documentos únicamente contuviesen datos meramente identificativos de aquellos. d) La mayor garantía de los derechos de los afectados en caso de que los datos contenidos en el documento puedan afectar a su intimidad o su seguridad, o se refieran a menores de edad. 4. La interpretación de los criterios normativos de conciliación en los informes conjuntos de la AEPD y el CTBG. A. Informe conjunto 1/2015 de 23 de marzo y Criterio interpretativo CI/001/2014 de 24 de junio sobre RPT, y retribuciones de empleados o funcionarios. B. Criterio interpretativo CI/002/2015 de 24 de junio – Aplicación de los límites al derecho de acceso a la información. C. Criterio interpretativo CI/004/2015 de 23 de julio – Publicidad activa de los datos del DNI y de la firma manuscrita. D. Criterio interpretativo CI/002/2016 de 5 de julio de 2016 – Información relativa a las agendas de los responsables públicos.

1. Cuestiones preliminares

El artículo 15 de la LTAIBG, que contiene la excepción al acceso a la información pública en materia de protección de datos, establece una serie de parámetros normativos con los que se pretende orientar y dar una solución reglada al conflicto entre transparencia, acceso a la información y protección de datos de carácter personal.

Para ello, ha echado mano de una categorización de los datos personales, que obedece en cierta medida a la estructura que sobre los mismos sigue la LOPD y que se analizarán en este apartado. En primer lugar, se analizará la imposibilidad del tratamiento de datos especialmente protegidos o datos que se refieran a sanciones penales o infracciones administrativas que no han sido publicadas, sobre los cuales la LTAIBG es clara en que no se admite su tratamiento salvo las excepciones de consentimiento, autorización por medio de una norma legal o que los mismos hayan sido hechos públicos de forma manifiesta por el interesado.

En segundo lugar, se estudiará el nivel siguiente de protección de datos personales, que es el que se refiere a datos meramente identificativos que se encuentren directamente

vinculados con la función, organización o actividad pública del órgano de la Administración Pública.

Seguidamente, se hará un análisis de una de las disposiciones más relevantes que contiene la excepción al acceso a la información pública, que es aquella que pretende regular, por medio de una ponderación, los datos de carácter personal que no han quedado comprendidos dentro de las dos categorías. Para ello, el legislador ha tratado de fijar una serie de criterios de ponderación que a su juicio pueden funcionar como guía a la hora de ponderar los derechos en juego.

Por último, se considerará también dentro de la explicación de este Capítulo las disposiciones de cierre del artículo 15 de la LTAIBG que están relacionadas con la disociación de datos personales y la aplicación de la LOPD a cualquier tratamiento posterior de los mismos, así como al ejercicio de la facultad que ha conferido la LTAIBG, para que de forma conjunta la AEPD y el CTBG puedan interpretar esta excepción.

2. Los criterios normativos del artículo 15 de la LTAIBG

El actual artículo 15 de la LTIABG, expresamente dispone:

> "1. Si la información solicitada contuviera datos especialmente protegidos a los que se refiere el apartado 2 del artículo 7 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, el acceso únicamente se podrá autorizar en caso de que se contase con el consentimiento expreso y por escrito del afectado, a menos que dicho afectado hubiese hecho manifiestamente públicos los datos con anterioridad a que se solicitase el acceso.
> Si la información incluyese datos especialmente protegidos a los que se refiere el apartado 3 del artículo 7 de la Ley Orgánica 15/1999, de 13 de diciembre, o datos relativos a la comisión de infracciones penales o administrativas que no conllevasen la amonestación pública del infractor, el acceso sólo se podrá autorizar en caso de que se cuente con el consentimiento expreso del afectado o si aquel estuviera amparado por una norma con rango de Ley.
> 2. Con carácter general, y salvo que en el caso concreto prevalezca la protección de datos personales u otros derechos constitucionalmente protegidos sobre el interés público en la divulgación que lo impida, se concederá el acceso a información que contenga datos meramente identificativos relacionados con la organización, funcionamiento o actividad pública del órgano.
> 3. Cuando la información solicitada no contuviera datos especialmente protegidos, el órgano al que se dirija la solicitud concederá el acceso previa ponderación suficientemente razonada del interés público en la divulgación de la información y los derechos de los afectados cuyos datos aparezcan en la información solicitada, en particular su derecho fundamental a la protección de dato de carácter personal.
> Para la realización de la citada ponderación, dicho órgano tomará particularmente en consideración los siguientes criterios:
>
> a) El menor perjuicio a los afectados derivado del transcurso de los plazos establecidos en el artículo 57 de la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español.
>
> b) La justificación por los solicitantes de su petición en el ejercicio de un derecho o el hecho de que tengan la condición de investigadores y motiven el acceso en fines históricos, científicos o estadísticos.

> c) El menor perjuicio de los derechos de los afectados en caso de que los datos contenidos en el documento puedan afectar a su intimidad o a su seguridad, o se refieran a menores de edad.
>
> 4. No será aplicable lo establecido en los apartados anteriores si el acceso se efectúa previa disociación de los datos de carácter personal de modo que se impida la identificación de las personas afectadas.
>
> 5. La normativa de protección de datos personales será de aplicación al tratamiento posterior de los obtenidos a través del ejercicio del derecho de acceso".

Este artículo como ya se indicó anteriormente, está destinado a atender la relación entre transparencia, acceso a la información y protección de datos de carácter personal. Además del avance legislativo que supone, su importancia resulta en que la LTAIBG constituye uno de los supuestos del artículo 11 de la LOPD que habilita la cesión de datos de carácter personal, sin que resulte necesario contar con el consentimiento informado, cuando la misma esté autorizada por una ley. Para los casos regulados en la LTAIBG, la cesión de los datos está autorizada por la misma Ley. Esto supone un cambio de paradigma, pues previo a la existencia de la LTAIBG, para acceder a la información pública resultaba necesario el consentimiento del interesado, mientras que con la Ley 19/2013, la cesión está autorizada por una ley.[301]

También es importante mencionar que la excepción relativa a la protección de datos de carácter personal se encuentra dentro del Capítulo III de la LTAIBG, el cual regula específicamente el derecho de acceso a la información pública, resulta también de aplicación en los casos de publicidad activa, ya que el artículo 5 de la LTAIBG, sobre principios generales que la rigen, indica en forma expresa que "serán de aplicación, en su caso, los límites al derecho de acceso a la información pública previstos en el artículo 14 y especialmente, el derivado de la protección de datos de carácter personal, regulado en el artículo 15. A este respecto, cuando la información contuviere datos especialmente protegidos, la publicidad sólo se llevará a cabo previa disociación de los mismos".

Esta forma de aplicar la excepción para los supuestos, tanto de publicidad activa como de acceso a la información pública, convierte al derecho a la protección de datos de carácter personal en *"*un auténtico principio general informador del conjunto de previsiones *de* la LTAIBG".[302] No obstante lo anterior, como lo indica RODRÍGUEZ ÁLVAREZ[303], ello no debe suscitar confusión en cuanto a la aplicación de la excepción para los casos de acceso a la información o de publicidad activa, pues la ponderación de

[301] Piñar Mañas, J.L. (2014). Transparencia y protección de datos. Una referencia a la Ley 19/2013... *op. cit.* pp. 45.-57.
[302] Burgar Arquimbau, J.M. (2014). Aproximación a la protección de datos de carácter personal… *op. cit.*
[303] Rodríguez Álvarez, J.L. (2016). Transparencia y protección de datos personales… *op. cit.*

intereses en juego que debe llevarse a cabo no puede resultar homogénea para ambos supuestos y debe tomarse en cuenta, por ejemplo, del mayor grado de difusión que implica el ejercicio de la publicidad activa.

Hechas las precisiones preliminares, corresponde ahora efectuar un análisis sobre los supuestos en que el artículo 15 permite una excepción al acceso a la información pública, en virtud de la tutela del derecho a la protección de datos personales.

3. Criterios normativos de conciliación

A. Datos especialmente protegidos

Una primera excepción al acceso a la información, es que esta contenga datos de carácter personal considerados especialmente protegidos según lo que dispone el artículo 7 de la LOPD, disposición que está en consonancia con lo regulado en el artículo 8.1 de la Directiva 95/46.

Para estos efectos, el artículo 15.1 de la LTAIBG, sigue un esquema similar al establecido en el artículo 7 de la LOPD, en cuanto al tratamiento de las tres categorías de datos de carácter personal especialmente protegidos: datos sobre ideología, filiación sindical, religión y creencias (artículo 7.2 de la LOPD), datos sobre origen racial, salud y vida sexual (artículo 7.3 de la LOPD) y datos relativos a la comisión de infracciones penales o administrativas (artículo 7.5 de la LOPD).

La primera categoría de datos especialmente protegidos que recoge como excepción el artículo 15.1 de la LTAIBG, derivan –al igual que la LOPD- en forma directa del artículo 16.3 de la Constitución española que dispone que "nadie podrá ser obligado a declarar sobre su ideología, religión o creencias", datos que pueden ser catalogados como de "ultrasensibles"[304].

Cuando se solicite acceso a información pública que contenga datos que revelen ideología, afiliación sindical, religión y creencias, según lo dispuesto en artículo 7.2 de la LOPD, únicamente podrá concederse el acceso al documento bajo dos supuestos: el primero de ellos, es que se cuente con el consentimiento expreso y escrito del interesado, entendido este como "toda manifestación de voluntad, libre, inequívoca, específica e

[304] Del Castillo Vásquez, I.C. (2007). Transparencia, acceso a la documentación administrativa y protección de datos de carácter personal. *Foro, Nueva época*, núm. 6/2007. pp. 231-254.

informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen", según lo define el artículo 3.h) de la LOPD.

El segundo escenario que faculta el acceso a la información que contenga datos referidos a ideología, afiliación sindical, religión y creencias, es en función de si el afectado hubiese hecho manifiestamente públicos tales datos previo a la solicitud de acceso a la información, supuesto que si bien no está contemplado en la LOPD, si lo está en el artículo 8.2.e) de la Directiva 95/46 que refiere que no se aplicará la prohibición del tratamiento de datos sensibles, salvo que "el tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos (…)".

La aplicación del supuesto contenido en el artículo 8.2. e) de la Directiva 95/46, sobre la posibilidad del tratamiento de datos sensibles cuando el interesado los haya hecho manifiestamente públicos, ha sido abordado en reiteradas ocasiones por la AEPD, quien ha determinado que "los datos referidos a la ideología del afectado deberán quedar restringidos en su tratamiento a menos que el propio interesado levante esta restricción, renunciando a su derecho a no declarar acerca de su ideología política, pudiendo esta circunstancia derivarse de una manifestación explícita del consentimiento, referido a un determinado responsable que vaya a proceder al tratamiento y cesión de los datos de carácter personal, o a una manifestación pública del interesado, dirigido a una pluralidad indeterminada de destinatarios pero en ningún caso limitada a un ámbito concreto, en que aquél pone de manifiesto al común los datos referentes a su ideología política".[305]

Una segunda categoría de datos especialmente protegidos condiciona también el acceso a la información pública que los contenga. En los casos donde el documento o la información contenga datos sobre el origen racial, la salud o la vida sexual del interesado, la cesión de los datos y el acceso a la información que los contiene se ve condicionado a contar con el consentimiento expreso del afectado, o bien, que el acceso de tales datos estuviera amparado en una ley.

Una tercera categoría sujeta a los mismos requisitos de la segunda, está constituida por los datos relativos a la comisión de infracciones penales o administrativas que no conllevaran una amonestación pública del sujeto infractor.

[305] Ver por todos el Informe Jurídico 0272/2010 de la AEPD. Recuperado de: http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/datos_esp_protegidos/common/pdfs/2010-0272_Datos-de-objetores-de-conciencia-en-IVE.pdf

Sin duda alguna, el aspecto y el efecto práctico más importante de la consideración jurídica de los datos especialmente protegidos en relación con la transparencia y el acceso a la información, resulta en la exclusión de la aplicación del régimen de ponderación y afectación al que si se encuentran sometidos los demás datos personales no especialmente protegidos[306]. No obstante lo anterior, en caso de que se hayan hecho manifiestamente públicos quedan siempre sujetos a la ponderación que pueda llevar a cabo el órgano de la Administración a la que se solicite el acceso. PIÑAR MAÑAS lo explica señalando que en el caso de acceso a datos especialmente protegidos "siempre será necesario el consentimiento expreso del afectado, lo que hace innecesaria la ponderación: si se cuenta con el consentimiento la cesión es posible sin que se requiera ejercicio de ponderación alguno, y si tal consentimiento no se da tampoco cabe ponderación porque ésta n puede habilitar una cesión que sólo es posible con el consentimiento del afectado. Esta regla tiene una excepción: los datos hechos manifiestamente públicos a que se refiere el artículo 15.1 párrafo primero, pues en este caso, al no ser necesario el consentimiento, será preciso llevar a cabo la ponderación con carácter previo a la comunicación de los datos".[307]

Cabría la posibilidad de plantear una crítica sobre la inflexibilidad de este régimen, en el tanto solo permite el acceso a la información que contenga datos especialmente protegidos bajo los supuestos de consentimiento informado y expreso o haber hecho públicos tales datos en forma manifiesta, para el caso de la primer categoría de datos especialmente protegidos, así como cuando exista consentimiento o ley habilitante en el caso de las otras dos categorías de datos especialmente protegidos. Cabe preguntarse sobre la necesidad y pertinencia de haber adoptado un sistema que hubiese al menos permitido valorar la posibilidad de conceder el acceso a tales datos cuando se esté en supuestos de una manifiesta y evidente trascendencia pública de los mismos[308]. Sin

[306] Rodríguez Álvarez, J.L. (2016). Transparencia y protección de datos personales… *op. cit.*

[307] Piñar Mañas, J.L. (2014). Transparencia y protección de datos… *op. cit.* p. 60.

[308] Sobre este particular, GUICHOT REINA menciona que "la opción del legislador, siendo armónica con la LOPD, es un tanto "positivista" y acaso podría pensarse que también en el caso de salud o de sanciones pudiera haber acogido un criterio último de ponderación con el interés público en la divulgación que permitiera excepcionalmente dar preferencia a este último en casos muy relevantes (el estado de salud de un alto cargo, incluyendo en particular los Presidentes de Gobiernos, relacionados con la capacidad para el ejercicio de sus funciones, las sanciones administrativas o disciplinarias impuestas a un alto cargo). Dicho de otra forma, si por ley singular se pueden establecer casos en que prevalece la publicidad de los datos sanitarios o sancionadores, tal vez en la ley general que regula la transparencia podría haberse acogido un principio más general de ponderación del interés público en la divulgación en casos relacionados con otros bienes constitucionales. (…) A mi juicio, lo más cuestionable es el efecto que supone respecto a la inaccesibilidad a la información sobre sanciones administrativas (salvo previsión legal expresa o que se trate de sanciones que conlleven amonestación pública), información que no resulta evidente que pertenezca a la intimidad de las personas y cuyo conocimiento en ocasiones es crucial para controlar la efectiva

embargo, no puede perderse de vista la naturaleza y la sensibilidad de los datos de que se trata, así como que la rigidez viene habilitada de preceptos constitucionales (artículo 16.2 de la Constitución española) y legales (LOPD) que la LTAIBG en su carácter de ley ordinaria no puede limitar, tal y como fue advertido en el Informe que rindió la AEPD sobre el Anteproyecto de la LTAIBG.

B. Datos meramente identificativos relacionados con la organización, funcionamiento o actividad pública del órgano

En paralelo al régimen previsto por el legislador para los supuestos en que se solicite acceso a información que contenga datos especialmente protegidos, la LTAIBG contiene una serie de reglas que resultan de aplicación cuando la información solicitada contenga datos de carácter personal no especialmente protegidos.

Esta categoría de datos meramente identificativos relacionados con la organización, funcionamiento o actividad pública del órgano que aparece regulada en el artículo 15.2 de la LTAIBG, se refiere a datos, como por ejemplo: el nombre, apellidos, puesto de trabajo, correo electrónico laboral, entre otros, que no representan necesariamente por sí solos, una intromisión en la intimidad de la persona ni afectan su seguridad.

Sobre estos datos nominativos o meramente identificativos, la LTAIBG indica que con carácter general se concederá el acceso a la información que los contenga, salvo que prevalezca la protección de datos de carácter personal u otro derecho constitucionalmente protegido sobre el interés público en la divulgación que lo impida. En tales casos, según dispone el artículo 15.3 de la LTAIBG, el órgano correspondiente podrá conceder el acceso a la información que contiene los datos personales no especialmente protegidos, siempre y cuando haya mediado de forma previa una ponderación suficientemente razonada del interés público en la divulgación de la información y los derechos e intereses de los afectados cuyos datos constan en la información solicitada, con especial observancia del derecho a la protección de datos de

aplicación por igual de la ley a todas las personas. Más aún considerando que incluyen, si se sigue la interpretación que se maneja en el campo de la protección de datos, las sanciones disciplinarias cuyo conocimiento puede ser de suma relevancia pública para juzgar la actuación administrativa". Ver en: Guichot Reina, E. (2014). Límites a la transparencia y el acceso a la información. En E. Guicot Reina (Coord.) Madrid: Tecnos. pp. 97-141.

carácter personal, lo cual nos lleva al siguiente tema de análisis correspondiente a los criterios objetivos de ponderación que fija la LTAIBG.

La incorporación en este supuesto del concepto de "datos meramente nominativos" representa una ventaja en el tanto puede ser medianamente precisado con base en la legislación vigente, así como interpretaciones de la AEPD, contrarrestando en cierta forma el resto de conceptos indeterminados que engloba el artículo 15.2 de la LTAIBG como son "organización" o "funcionamiento" del órgano, que podían constituir una amenaza en la consecución del equilibrio entre los derechos e intereses en juego.

Sin embargo, varios autores coinciden en que no debe dejar de advertirse la contradicción en la que incurre este apartado con lo regulado en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD y en la propia LTAIBG. Por una parte, los datos nominativos o identificativos a los que se refiere el artículo 15.2 de la LTAIBG, están expresamente excluidos del ámbito objetivo de aplicación de la LOPD según lo dispuesto en el artículo 2 del Reglamento a la LOPD, el cual señala que "este reglamento no será aplicable a los tratamientos de datos (…) consistentes únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales".

Por otro lado, incurre también en una contradicción con las disposiciones contenidas en el título de transparencia de la actividad pública, que exige la publicación de forma periódica y actualizada de la información, cuyo conocimiento sea relevante para garantizar la transparencia y el control de la actuación pública, lo que sin duda alguna puede llegar con facilidad a incluir datos meramente nominativos o identificativos.

Para autores como GUICHOT REINA[309], la crítica va más allá de la simple contradicción de normas que deberá ser superada en la práctica, sino que considera que este precepto de la LTAIBG puede conducir a lo que define como una "gran cerrazón a la transparencia de la actuación púbica". A su criterio, se introdujo una limitación a la transparencia en el tanto los datos relacionados con la organización, funcionamiento o actividad pública deben ser con carácter general públicos y no solo en lo que se refiere a datos meramente identificativos. Cita por ejemplo, que en los casos de regulación de publicidad activa, en donde interesa especialmente desde la transparencia, la publicidad

[309] Guichot Reina, E. (2014). La nueva Ley de Transparencia… *op. cit*. pp. 94-107.

de la gestión institucional y organizativa, lo que incluye no solo la identificación de los responsables, su perfil, trayectoria profesional, sino que también información que no es meramente identificativa como contratos, convenios, subvenciones retribuciones, indemnizaciones, entre otros.

C. Datos de carácter personal no especialmente protegidos: criterios objetivos para la ponderación

Con el fin de brindar una protección a los otros datos de carácter personal que están fuera del limitado ámbito de aplicación de los supuestos tutelados de los apartados 1 y 2 del artículo 15, el legislador previó en el apartado 3 de ese mismo artículo una solución para las solicitudes de acceso a información que contienen datos de carácter personal, pero que no se encuentran especialmente protegidos. En tales casos, "el órgano al que se dirija la solicitud concederá el acceso previa ponderación suficientemente razonada del interés público en la divulgación de la información y los derechos de los afectados cuyos datos aparezcan en la información solicitada, en particular su derecho fundamental a la protección de datos de carácter personal".

El primer elemento que se pone de relieve, según la redacción del artículo 15.3 de la LTAIBG, es el deber de ponderación que debe llevar a cabo el órgano al que se solicite la información[310]. Esta obligación de ponderar entre los diferentes intereses y derechos en juego, deriva de sólida construcción jurisprudencial del TJUE, que ya en varios casos ha tenido que abordar el conflicto generado entre el derecho de acceso a la información pública en poder de las instituciones de la UE y el derecho a la protección de datos de carácter personal, ambos bienes jurídicos tutelados de forma amplia en el ámbito comunitario.

[310] Autores como Cotino Hueso consideran que "se trata de una regulación loable por intentar pautar una ponderación de derechos en intereses y dotar de asideros a los operadores jurídicos. Sin embargo, del otro lado, el derecho de protección de datos –e incluso intimidad- parecen estar en una posición de prevalencia exagerada que sólo podrá ser corregida por una interpretación jurídica que tenga en cuenta el carácter fundamental del derecho de acceso a la información pública". Esto pone nuevamente, como ya se ha explicado, el grave inconveniente de que el derecho de acceso a la información siga siendo considerado a hoy como un derecho de configuración legal y se haya impedido por todos los medios y cauces su reconocimiento como derecho fundamental. En: Cotino Hueso, L. (2014). La nueva ley de transparencia y acceso a la información… *op. cit.* pp. 241-256.

Para el TJUE, "antes de divulgar información sobre una persona física, las instituciones están obligadas a poner en la balanza por una parte, el interés de la Unión en garantizar la transparencia de sus acciones, y por otra, la lesión de los derechos reconocidos en los artículos 7 y 8 de la Carta. Ahora bien, no cabe atribuir una primacía automática al objetivo de la transparencia frente al derecho a la protección de los datos de carácter personal ni siquiera aunque estén en juego intereses económicos importantes"[311], de ahí que la ponderación en cada caso concreto resulte un ejercicio necesario y clave con el fin de garantizar un adecuado equilibrio entre ambos derechos.

A diferencia del ámbito comunitario en el que se establece una ponderación general atendiendo a las particularidades de cada caso ante la ausencia de una regulación clara y expresa del conflicto entre el derecho de acceso a la información y el derecho a la protección de datos, el legislador español optó por una vía distinta. El artículo 15.3 de la LTAIBG, exige una ponderación entre derechos e intereses y en "ejercicio del margen de apreciación que [le] confiere el artículo 5 de la Directiva 95/46"[312], establece una serie de principios o criterios objetivos que deben regir la ponderación y en esencia responden, según FERNANDEZ RAMOS[313] a:

> "-Que los datos únicamente contengan datos de carácter meramente identificativos de los afectados.
> -Que los solicitantes justifiquen de su petición en el ejercicio de un derecho.
> -Que los solicitantes tengan la condición de investigadores y motiven el acceso en fines históricos, científicos o estadísticos.
> -Que los datos contenidos en el documento puedan afectar su intimidad o a su seguridad.
>
> -Que los documentos que contienen los datos personales, incluidos aquellos que puedan afectar a la seguridad de las personas y a la intimidad de su vida privada y familiar, tengan una fecha de más de cincuenta años".

Estos criterios objetivos de ponderación son el resultado de la adopción de las recomendaciones tanto del Consejo de Estado y de la AEPD y brindan además un grado mayor de seguridad jurídica, en el tanto se encargan de reducir el margen amplio de apreciación del órgano al que se solicite la información[314] ante el uso de una serie de conceptos indeterminados en la norma. Esto no significa que los supuestos mencionados

[311] STJUE de 9 de noviembre de 2010, apartado 85.
[312] STJUE de 24 de noviembre de 2011, apartado 46.
[313] Fernández Ramos, S. (2013). El acceso a la información en el proyecto de Ley de transparencia, acceso a la información pública y buen gobierno. *Monografías de la Revista Aragonesa de Administración Pública*, *n*úm. XIV. pp. 233-298.
[314] Rodríguez Álvarez, J.L. (2016) Transparencia y protección de datos personales… *op. cit.*

sean los únicos que deben ser tomados en cuenta, sino son algunos dentro de los muchos que pueden resultar en atención a las particularidades de cada caso concreto. La enumeración que hace el artículo 15.3 de la LTAIBG, no debería suponer un problema en el tanto no debe ser entendido en el sentido de que se excluye cualquier otro supuesto no mencionado en forma expresa.

a) El menor perjuicio a los afectados derivados del transcurso de los plazos establecidos en el artículo 57 de la Ley 16 /1985, de 25 de junio, del Patrimonio Histórico

El artículo 15.3.a) adopta como un elemento a ser tomado en consideración a la hora de ponderar los derechos e intereses en juego, los plazos establecidos en el artículo 57 de la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español. Cabe resaltar como lo hace RODRÍGUEZ ÁLVAREZ[315] que no se trata de una remisión a la norma contenida en la Ley 16/1985, sino que es una adopción de los plazos que establece su artículo 57. Asimismo, no es una regla de decisión sino un criterio de ponderación; por lo tanto, el órgano no está obligado a permitir el acceso hasta que hayan transcurrido dichos plazos, sino que los puede tomar en cuenta para su ejercicio de ponderación.

b) La justificación por los solicitantes de su petición en el ejercicio de un derecho o el hecho de que tengan condición de investigadores y motiven el acceso en fines históricos

Esta letra trata dos supuestos diferentes en atención a las calidades subjetivas y justificación de quien requiera el acceso a la información que contiene datos personales no especialmente protegidos. El primero de ellos, se trata del ejercicio de un derecho. El segundo supuesto se torna algo más complejo, en el tanto exige por un lado la acreditación de la condición de investigador de quien solicite el acceso, así como que la solicitud de acceso a la información esté justificada en fines históricos, científicos o estadísticos, este último es el aspecto sobre el cual debe prestarse especial atención a la hora de ponderar, pues debe apreciarse no tanto la seriedad del estudio como la demostración de la

[315] *Ibíd.*

necesidad de acceso a la información para satisfacer el interés científico, histórico o estadístico.[316]

c) El menor perjuicio de los derechos de los afectados en caso de que los documentos únicamente contuviesen datos meramente identificativos de aquellos

A través de este supuesto se tutela el acceso a datos meramente identificativos distintos a los que se hace referencia en el apartado b), que únicamente refiere a datos identificativos relacionados de forma directa con la actividad y funcionamiento del órgano.

d) La mayor garantía de los derechos de los afectados en caso de que los datos contenidos en el documento puedan afectar a su intimidad o su seguridad, o se refieran a menores de edad

La disposición d) del artículo 15.3 de la LTAIBG, incorpora, como bien lo indica su enunciado, la posibilidad de que el órgano al que corresponda decidir sobre la concesión o no del acceso a la información, tenga la posibilidad de incorporar a la ponderación, elementos de juicio como si la revelación de datos puede llegar a afectar la intimidad o seguridad del interesado, o bien si se tratan de datos de menores que requieren de una protección especial y que pueden hacer que en determinados casos la balanza se incline a favor de la protección de sus datos personales y no a favor del acceso a la información.

A modo general, puede concluirse que la inserción de una adopción de una lista enunciativa de criterios de ponderación, contribuye a una mejor resolución de los conflictos que se puedan llegar a presentar cuando se solicite el acceso a información que contenga datos no especialmente protegidos. A nuestro juicio, la incorporación de estos criterios objetivos cumplen, tal y como lo avisaba la AEPD en su Informe preceptivo, a la realización de la ponderación que le exige el apartado 3, del artículo 15, de la LTAIBG, al órgano quien deba decidir si otorga o no el acceso a la información que contiene datos no especialmente protegidos.

[316] Fernández Ramos, S. (2013). El acceso a la información en el proyecto de Ley de transparencia… *op. cit.* pp. 233-298.

D. Disposiciones de cierre del artículo 15: disociación de datos y tratamiento posterior

Finalmente, el artículo 15 contiene dos disposiciones de cierre. La primera de ellas, hace referencia a que los preceptos jurídicos contenidos en el artículo 15 de la LTAIBG no serán aplicables cuando los datos hayan sido disociados, entendido este procedimiento como "todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable", según lo define el artículo 3.f) de la LOPD. Esta disposición además resulta consonante con el Informe 0037/2010 de la AEPD, en la que dispuso de forma expresa que "cuando el tratamiento se refiere únicamente a datos disociados que no permiten identificar al afectado al que los mismos se refiere no nos encontraremos ante datos de carácter personal, y en consecuencia, no estaremos dentro del ámbito descrito en el artículo 2.1 de la Ley Orgánica 15/1999. En ese sentido, recuerda, a título de ejemplo, el artículo 11.6 de la comunicación de datos que 'Si la comunicación se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores'".

En ese sentido, en el tanto los datos personales hayan pasado por técnicas de anonimización y disociación, no debería en principio existir ningún impedimento para que se facilite el acceso a la información al solicitante, en el tanto no puedan ser identificadas las personas sin necesidad de emplear esfuerzos desproporcionados[317]. De hecho, como se verá más adelante, en la búsqueda constante del equilibrio entre acceso y protección de datos, esta ha sido una de las opciones que el CTBG ha encontrado más viables para conceder acceso a la información pública sin necesidad de causar una afectación a los datos personales.

No obstante, hay quien apunta, desde un óptica crítica que esta exclusión de la aplicación de la LOPD de los datos disociados resulta tautológica[318], pues evidentemente al perder estos su consideración de dato de carácter personal –que permita vincular a una persona física identificada o identificable- están excluidos del ámbito de protección de la LOPD y el artículo 15 de la LTAIBG[319].

[317] Rodríguez Álvarez, J.L. (2016) Transparencia y protección de datos personales… *op. cit.*
[318] Guichot Reina, E. (2014). La nueva Ley de Transparencia… *op. cit.* pp. 94-107.
[319] Piñar Mañas, J.L. (2014). Transparencia y protección de datos… *op. cit.* p. 62.

La segunda es en relación con la aplicación de la normativa de protección de datos a cualquier tratamiento posterior de los datos que hayan sido obtenidos a través del acceso a la información pública, lo que resulta consonante con las exigencias que derivan de la LOPD. Si bien esta disposición entendemos busca asegurar la sujeción de la información obtenida a los principios del derecho a la protección de datos de carácter personal, algunos autores tachan de desafortunada esta inclusión porque resulta una limitación o al menos en una dificultad a la hora de definir los alcances en la divulgación de los datos que pudieron haber sido obtenidos mediante el ejercicio de los derechos contenidos en la LTAIBG[320], aunque otros, señalan con claridad, la imposibilidad de invocar las disposiciones de la LOPD con el fin de impedir la divulgación de los datos obtenidos[321].

4. La interpretación de los criterios normativos de conciliación en los informes conjuntos de la AEPD y el CTBG

La disposición adicional quinta de la LTAIBG, dispone que la AEPD y el CTBG adoptarán de forma conjunta los criterios de ampliación de las reglas que contiene el artículo 15 de la LTAIBG, en particular en cuanto a la ponderación del interés público en el acceso a la información y la garantía de los derechos de los interesados, cuyos datos personales se contuvieran en la información. Esta posibilidad de la emisión de criterios conjuntos reside en la necesidad de interpretar y aclarar los criterios de ponderación de derechos e intereses establecidos por el legislador en el artículo 15 de la LTAIBG.

En palabras de CANALS ATMELLER estos "criterios de ponderación son orientaciones para los órganos administrativos que podrán ser con posterioridad interpretadas por los organismos públicos independientes que tienen a su cargo la

[320] En este sentido, MATIA PORTILLA cita: "Para algunos autores, "no puede dejar de observarse que esta sujeción a la LOPD comporta una seria limitación para la divulgación de los datos obtenidos en la aplicación de la LTBG, al aplicarse el régimen de comunicación de datos previsto en dicha Ley –art. 11-. Es decir, que un eventual intento de ulterior difusión pública del dato al que se accede de esta forma exigirá el consentimiento del titular del dato." No son de la misma opinión todos los tratadistas, para quienes, a pesar de la dicción literal del precepto citado, "no cabe invocar la normativa sobre protección de datos para impedir la divulgación general por el solicitante de información de la obtenida conforme a la LTAIBG." Ver en: Maria Portilla, E. (2017). Derecho a la información de los representantes políticos, protección de datos y transparencia. *Revista Jurídica de Castilla y León. Revista jurídica de Castilla y León, núm.* 42, mayo 2017. Recuperado de: http://www.jcyl.es/web/jcyl/AdministracionPublica/es/Plantilla100/1131978346397/_/_/_

[321] De esta última posición es GUICHOT REINA, quien diáfanamente sobre este particular indica que: "no está de más recordar que dicha normativa tiene como presupuesto la integración de los datos en ficheros y su tratamiento, es decir que, fuera de esos presupuestos, no cabe invocar la normativa sobre protección de datos para impedir la divulgación general por el solicitante de información de la obtenida conforme a la LTBG." [321] Guichot Reina, E. (2014). La nueva Ley de Transparencia… *op. cit.* pp. 94-107.

protección, en vía administrativa, de los respectivos derechos, y, en última instancia lo serán por los Tribunales. Estos organismos o autoridades independientes poseen importantes facultades para crear criterios de interpretación o aclarativos de las pautas establecidas por el legislador". [322]

En el contexto de la LTAIBG, la facultad de la interpretación conjunta se incluyó a solicitud de la AEPD, quien en su informe preceptivo apuntó la conveniencia de que pudiera dictar normas que facilitaran a los órganos competentes efectuar la ponderación establecida en el entonces artículo 11, apartado 4 del Anteproyecto de Ley (actual artículo 15), potestad que le fue conferida en forma conjunta con el CTBG.

No obstante, la visible conveniencia de que los dictámenes se formulen de forma conjunta, pues se trata de un área que incumbe tanto a la interpretación del derecho a la protección de dato conferida a la AEPD y el derecho a la transparencia en las actividades públicas conferido al CTBG, hay quien considera necesario precisar esta provisión, en el sentido de que no debe olvidarse que la aplicación de la normativa de la LTAIBG, incluidos los criterios interpretativos del artículo 15, corresponde al CTBG y no a la AEPD[323].

A. Informe conjunto 1/2015, de 23 de marzo y Criterio interpretativo CI/001/2014, de 24 de junio sobre RPT, y retribuciones de empleados o funcionarios

Por medio de solicitud dirigida a la AEPD y al CTBG, la Oficina de Ejecución de la Reforma de la Administración (OPERA) solicitó la adopción de un criterio uniforme sobre la posibilidad de admitir y conceder el acceso a solicitudes que tuvieran por objeto:

1. La retribución de un determinado puesto de trabajo del sector público, ya sea de personal funcionario, laboral o de carácter eventual con o sin la identificación del empleado público que lo desempeñe.

[322] Canals Ametller, D. (2016). El acceso público a datos en un contexto de transparencia y buena regulación. En Dolores Canals Ametller (ed.) Datos. Protección, Transparencia y Buena Regulación. Recuperado de: www.documentauniversitaria.com

[323] Sobre este particular GUICHOT menciona: "La previsión podría saludarse como positiva. Ahora bien, a nuestro juicio (y no por casualidad) la propuesta viene de la AEPD. Y es que no debe olvidarse que es la normativa sobre acceso la que se aplica a la publicidad activa o pasiva de información que contiene datos de terceros y en ese sentido, siendo deseable una interpretación armónica de ambos bloques normativos, dicha interpretación ha sido precisamente la efectuada por el legislador en el artículo 15 LTBG, es de la competencia de las autoridades de transparencia".

2. La RPT de los distintos órganos administrativos así como la identidad de la persona que desempeña un determinado puesto de trabajo.
3. La productividad que ha percibido cada empleado público de manera individualizada.

Previo al análisis de fondo de las consultas específicas formuladas por la OPERA, el dictamen realiza una serie de apreciaciones sobre el ámbito de aplicación y los alcances del mismo. En primer lugar, delimita la aplicación del dictamen únicamente a la Administración General del Estado, pues de conformidad con el artículo 12 de la LTAIBG, en las Comunidades Autónomas la delimitación y aplicación de las relaciones consultadas corresponde a los órganos constituidos para tales efectos, según sus Leyes de Transparencia y las disposiciones de la LTAIBG que resultase aplicables.

Seguidamente, en el tanto la consulta se refiere a solicitudes de acceso a la información pública, se limita el alcance del dictamen únicamente a los supuestos de derecho de acceso a la información pública y publicidad no activa y, en consecuencia, se excluye de su alcance los supuestos de publicidad activa.

Contiene también una última precisión preliminar que incide directamente sobre el fondo de la consulta y se relaciona con el concepto de "retribuciones" que aparece mencionado en la primera consulta de la OPERA. Sobre este particular, indica que de acuerdo con la Ley 7/2007, de 12 de abril, del Estatuto Básico del Empleado Público (EBEP), las retribuciones difieren según se trate de personal funcionario de carrera, personal laboral o personal eventual, siendo que en el caso de funcionarios de carrera, una segunda división surge en torno a si son retribuciones básicas (suelto y trienios) y retribuciones complementarias complemento de destino, complemento específico y complemento de productividad). Mientras que algunos de estos datos están asociados al puesto de trabajo (sueldo, complemento de destino y complemento específico), otros están asociados directamente a la persona titular del puesto de forma que no puede separarse la retribución del empleado (trienios, asociados a la antigüedad y complemento de productividad, asociado al desempeño del puesto de trabajo). Adicionalmente, señala que en relación con las retribuciones variables, información referida a la productividad o cualquier otro concepto equivalente, solo puede facilitarse el acceso a tales datos a período vencido y con una clara advertencia de que el monto es variable en función de desempeño y cumplimiento de objetivos. Por último, precisa el dictamen que la información sobre la productividad como elemento variable en función del desempeño,

puede llegar a tener una incidencia directa sobre datos especialmente protegidos y lo ejemplifica con los datos de salud en el supuesto de suspensión de un abono por baja laboral.

Ahora bien, avocados los órganos a la aplicación de la ponderación exigida en el artículo 15.3 de la LTAIBG, señalan que el derecho a la protección de datos de carácter personal, debe ceder cuando el acceso a la información que los contenga permita un mejor control del funcionamiento de las instituciones o la asignación de los recursos. Cuando este sea el supuesto, podría entonces atribuirse una prevalencia del interés público sobre el derecho a la protección de datos de carácter personal, en los términos establecidos por la misma LTAIBG. Si ese no fuese el supuesto y el acceso a la información no contribuyese a un mayor o mejor control de las instituciones públicas y su funcionamiento, cabe denegar el acceso a la información pública que contiene los datos, pues en ese sentido prevalece el derecho de toda persona a la protección de sus datos personales.

Con base en lo anterior, consideran entonces que la información que se refiere a puestos de trabajo de mayor responsabilidad y autonomía en la toma de decisiones, así como de los que posean un cierto grado de discrecionalidad o provengan de la existencia de una especial relación de confianza, prevalece el interés público como regla general. *Contrario sensu*, aquellos puestos cuya asignación se verifica por procedimientos previamente determinados o no conllevan una especial relación de confianza, prevalece el derecho a la protección de datos de carácter personal.

Del análisis del párrafo anterior, la AEPD y el CTGB derivan varias categorías de empleados públicos, según la relevancia de la vinculación entre la información relativa a las retribuciones y la mejor consecución del objetivo de la transparencia.

La primera categoría se encuentra integrada por empleados públicos que sean titulares de los órganos directivos de la Administración General del Estado, ya que desarrollan una actividad de ejecución esencial dentro de la estructura estatal que hace que el conocimiento de su identidad y retribución, como gestores directos de la actividad pública esté cubierta por el principio de transparencia. No obstante, de esta categoría debe excluirse a los empleados que sean objeto de publicidad activa de conformidad con el artículo 8.1.f) de la LTAIBG así como quienes posean un carácter de personal directivo por una atribución normativa.

La segunda categoría la vendría a integrar el personal eventual (artículo 12 EBEP), que es aquel que adquiere su condición de empleado público como consecuencia de su nombramiento y cuya actividad tiene por objeto la realización de funciones calificadas de confianza o asesoramiento especial. Siendo que el nombramiento del personal eventual depende directamente del cargo público al que presta sus servicios y la relación de confianza con este, sin que sea necesario mérito alguno para el acceso a la función pública o promoción interna, permitir el conocimiento de la retribución del empleado puede ayudar a comprender mejor la organización administrativa y el manejo de los fondos públicos. Por este motivo, en estos supuestos prima también el derecho de acceso a la información por encima del derecho a la protección de los datos de carácter personal del personal eventual.

Una tercera categoría viene a estar integrada por el personal funcionario de libre designación que pese a ser un puesto de especial confianza, está reservado a quienes posean la condición de funcionario y cuenten con la idoneidad para el desempeño de las labores, lo cual se determina a través de procedimientos que tienen como base los principios de publicidad y concurrencia. Para este tipo de personal, deberá ponderarse caso por caso, pues la relevancia del interés público en conocer determinados datos de carácter personal varía según el nivel del puesto.

La última categoría está integrada por el resto de funcionarios públicos que han obtenido un puesto a través de los procedimientos establecidos en la ley. Según el Informe conjunto, la información de este grupo de personas no resulta lo suficientemente relevante como para que se vea limitada en virtud del interés público. En este caso, salvo que exista una justificación que acredite la necesidad de conocer la información sobre esta categoría de funcionarios, prima el derecho a la protección de datos de carácter personal frente al derecho de acceso a la información.

En virtud de lo considerado hasta ahora, la AEPD y el CTBG concluyen que procede otorgar el acceso a la información relativa a las remuneraciones cuando se trate de titulares de las subdirecciones generales, las subdelegaciones del gobierno en las provincias y los órganos directivos de las agencias estatales, entes y otros organismos públicos que tengan atribuida la condición de directivos, siempre y cuando no sean objeto de publicidad activa. Asimismo, debe concederse el acceso a los datos de remuneraciones del personal eventual y los puestos de trabajo de libre designación, según sea su relevancia de acuerdo con el nivel de responsabilidad. La información a la que se concederá acceso,

deberá versar sobre las retribuciones íntegras anuales, sin exclusión de las deducciones aplicables ni desglose de los conceptos retributivos. En caso de que se hubiera solicitado acceso expresamente a conceptos retributivos, el órgano administrativo deberá valorar cada situación de forma individual.

En cuanto a la información sobre las relaciones de puestos de trabajo, la AEPD y el CTGB consideran que se trata de información meramente identificativa relacionada con la organización, funcionamiento o actividad de los organismos públicos y además es información que debe publicarse –sin identificación de las personas que ocupan los puestos- por lo que debe con carácter general concederse el acceso dicha información. Únicamente podría verse limitado el acceso cuando esta información, en relación con un determinado empleado público y en atención a su situación específica, deba prevalecer el derecho a la protección de datos personales u otros derechos constitucionalmente protegidos, según lo dispuesto en el artículo 15.2 de la LTAIBG.

De acuerdo con el Criterio, en relación con la productividad que han percibido los empleados públicos de forma individualizada, deberá valorarse la concesión del acceso a dicha información con base en los parámetros de responsabilidad, confianza y participación en el proceso de toma de decisiones. En caso de que proceda el acceso a la información, la misma deberá ser entregada en cómputo íntegro anual, salvo que se hubiera solicitado de una forma distinta expresamente y siempre haciendo la salvedad del carácter variable que posee el complemento de productividad.

B. Criterio interpretativo CI/002/2015, de 24 de junio, sobre aplicación de los límites al derecho de acceso a la información

El Criterio interpretativo CI/0002/2015, tuvo por objeto la adopción de una interpretación conjunta sobre la aplicación de los límites al derecho de acceso a la información contenidos en los artículos 14 y 15 de la LTAIBG, ante la observación por parte del CTBG de una aplicación extensiva de los límites que contienen dichas disposiciones.

El Criterio fija un proceso de valoración, el cual deriva de la aplicación directa de la limitación contenida en el artículo 15 de la LTAIBG y la posibilidad de aplicar las

limitaciones del artículo 14 de la LTAIBG[324], lo cual a su vez resalta el carácter no automático de la denegación de acceso o publicidad, sino que debe realizarse un test del daño concreto, definido y evaluable, así como valorar el interés existente en la publicidad o acceso a la información.

En ese sentido, el órgano deberá verificar primeramente si la información solicitada o que debe soportar la publicidad activa, contiene o no datos de carácter personal según la LOPD. Seguidamente, en caso de que la información contenga datos de carácter personal, deberá verificar si estos son datos especialmente protegidos, según el artículo 7 de la LOPD y si existe la concurrencia de alguno o varios de los supuestos que permiten la revelación de tal información.

Ahora bien, en caso de que los datos que contenga la información no fuesen especialmente protegidos, entonces el órgano debe valorar si los mismos son o no datos meramente identificativos relacionados con la organización, funcionamiento o actividad pública del órgano o entidad. En el tanto los datos sean meramente identificativos y vinculados a la organización, funcionamiento o actividad pública del órgano, debe facilitarse el acceso o publicar la información respectiva, salvo que prevalezca en el caso concreto la protección de los datos personales. Una vez superado este procedimiento, cabe valorar la aplicación de los límites que contiene el artículo 14 de la LTAIBG.

Si en virtud de este examen el órgano determinara que no precede otorgar el acceso total a la información, podrá conceder o publicar la información previa omisión de los puntos específicos que caen dentro de las excepciones, siempre y cuando de ello no resulte una información distorsionada o que carezca de sentido, según lo dispuesto en el artículo 16 de la LTAIBG.

C. Criterio interpretativo CI/004/2015, de 23 de julio, en relación con la publicidad activa de los datos del DNI y de la firma manuscrita

El Criterio[325] tiene como objeto atender varias consultas que se han presentado ante el CTBG, en relación con la publicación activa que exige el artículo 8 de la LTAIBG, en el marco de la información relativa a los convenios y contratos que se firmen, del DNI

[324] El apartado 1, del artículo 14, está expresado en una posibilidad de los organismos de limitar el acceso a la información cuando suponga un perjuicio a alguna de las situaciones mencionadas en el artículo. En ese sentido, literalmente menciona: "1. El derecho de acceso podrá ser limitado cuando acceder a la información suponga un perjuicio para: (…)".
[325] Este criterio tiene como base el Informe 0502/2014 de la AEPD.

y de la firma manuscrita de los firmantes con independencia de que estos ocupen o no un cargo público.

Como punto de partida, el Criterio se encarga de establecer si el DNI forma un dato de carácter personal según la normativa vigente. Con base en el artículo 3 de la LOPD y el artículo 5.1.f) del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD, concluye que en el tanto el DNI constituye una información relativa a una persona física identificada o identificable y contiene además información numérica, alfabética, gráfica, fotográfica o de cualquier otro tipo que concierne a personas físicas identificadas o identificables, se trata de un dato de carácter personal. Igual consideración para la firma manuscrita, pues se trata de una información gráfica que permite identificar a una persona física, toda vez que los convenios ya tienen la identidad de los firmantes.

En ese sentido, el DNI y la firma manuscrita de las partes firmantes de un convenio, en el tanto sean de personas físicas, tienen la consideración de un dato de carácter personal, por lo que resultan aplicables las disposiciones establecidas en el artículo 15 de la LTAIBG.

En relación con el objeto de la consulta, el Criterio señala que si bien el artículo 8.1.a) y b), prevén la publicación de la identidad del adjudicatario de un contrato y los convenios con mención de las partes firmantes, estas obligaciones de publicidad activa tienen un carácter de mínimos por lo que los organismos pueden publicar o conceder el acceso a mayores informaciones que las estrictamente necesarias para cumplir con lo estatuido en dichos artículos, que en todo caso se vería satisfecho con la publicación del nombre, apellidos y cargo de los firmantes. Por ese motivo, estiman la conveniencia de pronunciarse sobre la ponderación de la publicidad del DNI y la firma manuscrita aún y cuando estos datos de carácter personal no resulten necesarios para satisfacer las obligaciones de los preceptos citados de la LTAIBG.

En relación con la publicación del DNI, tanto la AEPD como el CTGB en su Criterio conjunto consideran que no es relevante para efectos de alcanzar el objetivo que persigue la LTAIBG. El objetivo de transparencia que persigue se cumple con la publicación de los nombres y apellidos o del acta de nombramiento –en el caso de los cargos públicos– de los firmantes. El DNI es un dato de carácter personal que se encuentra

fuera de la esfera pública de los firmantes y su conocimiento por terceros puede generar riesgos de suplantación de identidad.

Sobre la firma manuscrita, considera el Criterio que si fuese la de representantes de organismos o entidades públicas, cuyo nombramiento ha sido publicado y la aceptación del cargo ha sido refrendada por medio de la firma de quien ostenta el cargo, puede considerarse que la misma tiene cierta relevancia y, por lo tanto, la ponderación entre transparencia y datos de carácter personal se inclina en favor de la primera, ya que permite que el documento esté dotado de mayor integridad y exactitud en cuanto a la firma como manifestación de voluntad del órgano. Caso contrario, si se tratase de personas físicas o particulares que no ostentan un cargo público, la ponderación se inclina a favor de la protección de datos de carácter personal.

Es decir, que el objetivo de transparencia se vería cumplido si el documento incorporase la firma manuscrita de quien ostente el cargo público, mas no así de los demás firmantes que no ostenten dicha condición. No obstante lo anterior, con el fin de dotar de homogeneidad al documento, el Criterio señala como buena práctica no consignar ninguna firma pero sí la indicación de que el documento original ha sido debidamente firmado por todas las partes firmantes.

D. Criterio interpretativo CI/002/2016, de 5 de julio, sobre información relativa a las agendas de los responsables públicos

Este Criterio interpretativo tiene como fin pronunciarse sobre las reclamaciones presentadas al amparo del artículo 24 de la LTAIBG por la denegación de algunos organismos de dar acceso a la información relacionada con reuniones celebradas por miembros del Gobierno, altos cargos o empleados públicos, así como la respectiva identificación de quienes asistieron a dichas reuniones. La información a la que se solicita acceso es sobre los datos relacionados con el cargo o posición de las personas asistentes a la reunión y, en algunos casos, la identificación por nombre y apellido tanto de los representantes de la Administración como los de las entidades de carácter privado.

Previo a pronunciarse sobre el fondo, el Criterio indica que el alcance de la solicitud puede constituirse como límite al acceso a la información. Esto implica que en los casos en que proceda, el acceso deberá concederse sobre la información de las reuniones o actos concretos mencionados, o bien, al período temporal al cual se refiera la solicitud. Asimismo, en aquellos casos donde la solicitud se refiera al conocimiento de

las personas o entidades de derecho público o privado que han participado o han estado presentes en una reunión, la respuesta queda delimitada a la relación de las entidades u organizaciones participantes, sin necesidad de dar indicación sobre las personas físicas que participaron de la reunión. En los casos en que se solicita solo la indicación del cargo o posición de las personas físicas participantes, sin solicitar identificación por nombres y apellidos, la información queda delimitada solo a tales datos sin que deba añadirse la identificación de la persona física.

Finalmente, la información facilitada solo es la que esté disponible, pues a la fecha no existe una norma legal que obligue a los sujetos obligados a llevar una agenda de sus actividades. En ese sentido, solo puede ser otorgada la información que haya sido conservada, archivada o se pueda recabar o recopilar, siempre y cuando no suponga un entorpecimiento grave del funcionamiento del organismo.

El Criterio llama la atención sobre la posible concurrencia de datos especialmente protegidos en las solicitudes de acceso de información a las agendas de determinados organismos (artículo 15.1 de la LTAIBG), por ejemplo, los casos en que la reunión se celebrase con representantes o miembros de partidos políticos, sindicados, confesión religiosa o una asociación cuya pertenencia revele información sobre las creencias filosóficas de los miembros. Si la información contuviera este tipo de datos especialmente sensibles, únicamente se podría dar acceso a la misma bajo las excepciones que la propia ley tutela. Un ejemplo de lo anterior es que el dato especialmente protegido se haya hecho manifiestamente público por el interesado, como lo es el caso de los cargos relevantes de un partido político.

La información sobre la agenda de los organismos también puede conducir a que el acceso recaiga sobre datos de salud cuando las reuniones sean sostenidas por asociaciones de enfermos de una determinada dolencia, discapacidad, colectivos de una determinada etnia o personas de una determinada preferencia sexual. En estos casos, procede conceder el acceso si ha mediado consentimiento expreso o exista una ley que faculte la transmisión de tales datos.

Ahora bien, en relación con la ponderación que exige el artículo 15.3, debe partirse de la contribución al mejor conocimiento y funcionamiento de las instituciones, así como de los procesos de toma de decisiones por parte de los poderes públicos. Esta consecución del interés público a través de la solicitud de acceso a la información resulta

determinante en que la misma reciba una ponderación favorable al acceso. Por ello, aún y cuando de conformidad con el artículo 17 de la LTAIBG no cabe exigir al solicitante que motive o justifique su solicitud, una motivación por parte del interesado en este sentido puede contribuir a que la ponderación se incline favorable hacia el acceso.

También, según el Criterio, debe considerarse que la ponderación sea más favorable al acceso en función del grado de responsabilidad del interviniente en la reunión en la eventual toma de decisiones derivada de la misma, así como cuando su identidad tuviera un carácter público. Cabría la denegación del acceso a la información en aquellos casos en que la identidad del asistente a una reunión no brinde, por su posición jerárquica y poca influencia en el proceso de la toma de decisiones, elementos añadidos a la descripción del órgano u ente. En este último supuesto, el objetivo de la transparencia se puede satisfacer mencionando el órgano a que pertenece quien asiste a la reunión sin necesidad de una identificación física.

Con base en lo anterior, cabría facilitar la identificación por ejemplo de los titulares de los órganos directivos y sus asimilados, en el tanto desarrollan una actividad de ejecución esencial que justifica el acceso a la información, según fue reconocido también en el Informe conjunto 1/2015 de 23 de marzo. De forma que el acceso a la información identificativa de los participantes que tuvieran la condición de titulares de las Subdirecciones Generales o unidades asimiladas, Subdelegaciones del Gobierno en las provincias, órganos directivos de las Agencias Estatales, Entes y otros organismos públicos que tengan condición de directivos, según los estatutos o su normativa, resulta acorde con la LTAIBG.

En el caso de que la información a la cual se solicite acceso se refiera a entidades privadas, debe facilitarse información identificativa de los administradores, miembros de los órganos de gobierno o dirección, o altos directivos o asimilados.

Existen otra serie de supuestos específicos como lo es el caso de que la reunión haya sido celebrada con personas físicas o asesores o consultores que acompañen a la persona jurídica en a la reunión. La revelación de la identidad de los asesores puede llegar a suponer un quiebre en la relación de la persona jurídica con su asesor al hacerse público quien le presta una asesoría y más aún si se revela la identidad física de la persona que asesora y esto podría exceder los fines que persigue la LTAIBG. Para estos supuestos, el objetivo perseguido puede satisfacerse únicamente indicando que la persona jurídica

asistió a la reunión con un asesor externo, sin indicar la firma, despacho ni los datos identificativos del asesor.

En relación con las personas físicas que asisten a una reunión en su condición de expertos o particulares, debe valorarse caso por caso si procede o no conceder el acceso a la información identificativa, teniendo en consideración la finalidad que justificaría el acceso en los términos que contribuya a un mejor conocimiento y control de los procesos de toma de decisión.

Indica el Criterio que debe tomarse en consideración si los participantes prestaron su consentimiento para la comunicación de sus datos de los solicitantes de acceso. Este consentimiento debe cumplir con las exigencias establecidas en la LOPD y debe ser libre, inequívoco, específico e informado, no siendo posible que el consentimiento sea un requisito indispensable para la celebración de la reunión.

Recapitulación

El artículo 15 de la LTAIBG está destinado a atender la relación entre trasparencia, acceso a la información y protección de datos personales, mediante el establecimiento de una excepción al acceso en favor de la protección de los datos de carácter personal.

A diferencia del modelo que sigue el sistema comunitario en el que se debe seguir una ponderación pero sin señalarse en la normativa de forma expresa algún criterio a seguir en esta conciliación, el ordenamiento jurídico español si ha establecido tanto criterios para la conciliación, así como parámetros que deben ser tomados en cuenta a la hora de ponderar si en un caso particular prevalece el acceso a la información o por el contrario, prevalece la protección de los datos personales del interesado.

Estos criterios de conciliación están fijados en primer lugar, por la prohibición expresa para poder llevar a cabo un tratamiento de datos especialmente protegidos, según lo que dispuesto en el artículo 7 de la LOPD, el mandato expreso del artículo 16.3 de la Constitución española, así como el artículo 8.1 de la Directiva 95/46. Existe una prohibición para tratar esta categoría de datos salvo que exista un consentimiento expreso del interesado, hayan sido hechos públicos de forma manifiesta o exista una ley

que permita la cesión o transmisión de los mismos a terceros. Sobre este supuesto, si bien se entiende que su rigidez deriva de las propias previsiones constitucionales y el tratamiento que otorga la LOPD a datos muy sensibles, queda la duda respecto de no haber dejado un espacio para la ponderación cuando claramente el dato especialmente protegido tenga una incidencia pública directa o manifiesta como lo puede ser el estado de salud del jefe de gobierno, o si existen sanciones en su contra, aún y cuando no hayan sido publicadas, lo que reviste claramente un interés público.

Un segundo criterio de conciliación viene dado por la categoría de datos meramente identificativos relacionados con la organización, funcionamiento o actividad pública del órgano cuando ello no suponga una afectación al derecho a la protección de datos personales y otros derechos constitucionalmente protegidos. Existe claridad en este supuesto de que los datos meramente identificativos se refiere a datos como el nombre, apellido, puestos de trabajo, correo electrónico laboral, entre otros datos, que por sí solos no representan una intromisión a la intimidad. En principio, parece que el legislador tuvo la intención de dar una presunción a favor de la publicación o garantizar el acceso a estos datos meramente identificativos.

No obstante, la salvedad que hace de que procede la transmisión de tales datos cuando no supongan una intromisión al derecho a la protección de datos de carácter personal u otro derecho constitucionalmente protegido, complica la aplicación de este supuesto, pues en muchos de los casos, la presunción a favor de la publicidad o acceso a estos datos, terminará en una ponderación. Inclusive, se está ante el inconveniente de que esta previsión entra en contradicción con la normativa de protección de datos personales que justamente excluye estos datos meramente identificativos de la aplicación de la LOPD.

El tercer supuesto y uno de los más importantes que incluye el artículo, es el de la ponderación en todos los casos en que el documento contenga datos personales y estos no puedan ser incluidos en la categoría de datos especialmente protegidos ni en la de datos meramente identificativos en relación con la actividad del órgano. Según lo dispone el artículo 15.3, en estos casos, el órgano ante quien se ejercite el derecho de acceso a la información deberá ponderar entre la protección de los datos personales de los interesados y el interés que reviste el acceso a la información, aunque no puede denegarse la solicitud por el simple hecho de que el solicitante no justifique o acredite el

acceso. Ello nos lleva al dilema que se ha presentado en el marco normativo europeo, en el que el TJUE parte de la premisa de que si no se justifica el acceso, no hay manera de poder llevar a cabo la ponderación, pues quien debe decidir no cuenta con los elementos necesarios para determinar cuál de los derechos tiene una prevalencia sobre el otro el caso concreto.

Para ayudar a esta ponderación, el legislador español ha utilizado una serie de criterios de ponderación, que se entiende son numerus apertus y que en la práctica realmente han sido de poca o nula aplicación como se verá más adelante, estos criterios que en algunos casos no terminan de aportar la claridad pretendida, como hemos dicho, no son más que orientadores y su inclusión dentro de la LTAIBG no implica que sean los únicos o los que necesariamente tiene que tener en cuenta el órgano a la hora de ponderar. Esto nos deja, como se expuso ya, en un panorama similar al de la jurisprudencia del TJUE: el conflicto será al final de cuentas dirimido por una ponderación casos por caso, y para atribuir un fin a la transparencia y el acceso a la información pública, en muchos casos se requiere que se justifique o acredite la necesidad en el acceso.

La excepción contiene finalmente como cláusula de cierre dos disposiciones. La primera de ellas, avisa que no será de aplicación la LOPD cuando haya existido previa disociación de los datos personales, lo que como ya se apuntó con base en la doctrina, pareciera ser redundante, pues si ya los datos han sido disociados no existen datos personales –no hay una persona física identificable-, sin perjuicio de la complejidad que puedan revestir aquellos casos en que aún disociados los datos se permita la identificación de la persona física.

La segunda cláusula de cierre y lo que a criterio de esta exposición puede llegar a resultar en un serio inconveniente para la consecución del objetivo que persigue la transparencia y la protección de datos personales es la aplicación de la LOPD a cualquier tratamiento posterior de los datos obtenidos. Sobre este particular ya se ha pronunciado la AEPD, a instancia del CTBG y nos ocuparemos de ello más adelante, pero no puede dejar de advertirse que puede ser, junto con la falta de reconocimiento del derecho de acceso como un derecho fundamental, el talón de Aquiles de la LTAIBG. De qué sirve el acceso a la información y a los datos, si su tratamiento posterior estará limitado de forma tajante a lo dispuesto la LOPD? Se podrá hacer uso de los datos de

forma que se contribuya al debate público y a la rendición de cuentas? Será la AEPD quien tiene la última palabra siempre en materia de transparencia, acceso a la información y protección de datos personales?

Por último, la LTAIBG, como el fin de dar seguridad jurídica en cuanto a la interpretación de esta excepción –téngase en cuenta que tanto el CTBG como la AEPD tienen competencia para interpretarla-, ha creado una facultad para que se emitan criterios de forma conjunta, la cual hasta este momento si bien ha sido clarificadora y orientadora en este caso, no tiene el impacto deseado, pues tanto el CTBG como la AEPD se encuentran resolviendo lo más variado de casos, cada agencia siguiendo sus propios criterios. Puede que esta desazón que deja la emisión de criterios conjuntos se deba más a una cuestión estructural y con ello nos referimos a lo difícil que resulta tener dos autoridades independientes con competencia en un mismo tema pero analizando casos con ópticas muy diferentes: la AEPD interpretando la LTAIBG bajo la normativa de protección de datos personales y por otro lado el CTBG interpretando la LOPD bajo la perspectiva propia del derecho de acceso a la información pública.

Quinta Parte

La aplicación de los criterios de conciliación por parte del Consejo de Transparencia y Buen Gobierno y la Agencia Española de Protección de Datos

Capítulo IX. La aplicación de los criterios de conciliación por parte del Consejo de Transparencia y Buen Gobierno

SUMARIO: 1. Cuestiones preliminares. 2. El rol del CTBG en la aplicación de los criterios de conciliación. A. El establecimiento de una autoridad independiente de control. B. La potestad para conocer reclamaciones. 3. Resoluciones de reclamaciones. A. Datos sobre nombres de dominio. B. Información sobre concursos para plazas públicas. a) Información sobre otros candidatos que se presentaron en el mismo concurso y acceso a información sobre evaluadores. b) Solicitud de acceso a información sobre participantes, puntuaciones y motivaciones de valoración. C. Expedientes sancionatorios. a) Expedientes sancionatorios contra personas jurídicas. b) Expedientes sancionatorios contra personas físicas. D. Información sobre agendas públicas y reuniones de altos cargos. a) Agendas públicas. b). Reuniones de altos cargos. E. Información sobre pasaportes diplomáticos. F. Condecoraciones policiales. G. Datos de autores de notas técnicas. H. Datos contenidos en expedientes relativos a trámites migratorios. I. Datos especialmente protegidos. a) Información sindical. b) Datos sensibles derivados del conocimiento de otros documentos, por ejemplo, declaración patrimonial de altos cargos. J. Datos meramente identificativos. K. Datos de pasajeros de transportes oficiales. L. Disociación de datos personales. a) Aplicación de la disociación con independencia del soporte que contenga la documentación. b) Disociación de datos como condición para el acceso a la información. c) Disociación de datos en casos en que con la información solicitada se permite la individualización de la persona física beneficiaria de becas universitarias. d) Disociación como requisito para acceso a actas en las que pueden constar datos sensibles o relativos a infracciones administrativas. M. Exclusión de las personas jurídicas del ámbito de aplicación de la excepción contenida en el artículo 15. N. Listado de asistentes y participantes de actividades oficiales. O. Ejercicio de ponderación. a) Interés público en conocer evaluadores de planes de agencias estatales. b) Autorización a funcionarios públicos para realizar actividades privadas. c) Procedencia de entregar datos totalizados cuando se permite la identificación física de los interesados. d) Improcedencia de denegaciones con base en argumentos genéricos sobre la puesta en peligro o perjuicio al derecho a la protección de datos personales. P. Retribuciones y RPT. a) Acceso a la información sobre retribuciones de altos cargos y personal directivo. b) La LTAIBG constituye un título habilitante para la cesión de datos y no se requiere el consentimiento de los interesados. c) Concepto de "altos cargos y personal directivo" refiere a funciones y no a una denominación únicamente formal. d) Acceso a información sobre retribución de asesores y puestos de confianza. e) Improcedencia de acceso a la información de retribuciones en casos en que no existiese relación laboral pese a que le pago se haya hecho con fondos públicos. f) acceso a información de retribuciones de abogados sustitutos nombrados por períodos cortos de tiempo.

1. Cuestiones preliminares

Este Capítulo tiene por fin abordar la interpretación que ha hecho el CTBG de los criterios de conciliación que establece el artículo 15 de la LTAIBG.

Con el fin de llevar a cabo este análisis haremos una breve reflexión sobre el modelo de autoridad independiente de control en materia de transparencia y acceso a la información que ha seguido el legislador español y la tensión que puede llegar a

presentarse en determinado momento con el establecimiento de dos autoridades encargadas de interpretar la relación entre transparencia, acceso a la información y protección de datos personales desde paradigmas diferentes.

Posteriormente, se hará una breve referencia a la potestad atribuida al CTBG para conocer reclamaciones y se expondrá un breve recuento de las que se han estimado más relevantes según las reclamaciones publicadas en la página del CTBG hasta abril de 2017. La exposición se hará agrupándolas en los temas recurrentes que ha conocido el CTBG así como en algunos otros temas que por su relevancia merecen una atención individualizada.

2. El rol del CTBG en la aplicación de los criterios de conciliación

A. El establecimiento de una autoridad independiente de control

La doctrina coincide en que en materia de transparencia y acceso a la información, corresponde la aplicación, en virtud del principio de ley especial, de la normativa específica, en este caso, la normativa de la LTAIBG[326]. No obstante la claridad de lo anterior, existen críticas por parte de la doctrina que considera que en materia de protección de datos, quien debe ejercer la potestad de interpretación y control, es la AEPD como agencia estatal llamada a la tutela de la protección de datos personales[327].

[326] GUICHOT REINA, ha sido especialmente enfático en este sentido. De forma clara menciona que "una de las enseñanzas del Derecho supranacional y comparado es que la normativa sobre acceso a la información, y no la normativa sobre protección de datos, es de aplicación a las solicitudes de información realizadas por un tercero distinto del afectado". Ver en: Guichot Reina, E. (2014). Límites a la transparencia y el acceso a la información... *op. cit.* pp. 97-142. Sobre este particular, GARCÍA MUÑOZ explica que "en virtud del principio de *lex especialis*, las solicitudes de información que contengan datos personales han de regirse, no obstante, por las leyes de transparencia y acceso a la información pública vigentes aplicables en cada caso y no por la LOPD. Esta preferencia en la aplicación legal es la aceptada en derecho comparado y supranacional, bien porque así lo prevé expresamente un ordenamiento (Francia) o porque así lo han interpretado las respectivas autoridades independientes y los tribunales". García Muñoz, O. (2017). La protección de los datos de carácter personal. En VV.AA, Los límites al Derecho de Acceso a la Información Pública. Madrid: INAP. Recuperado de: https://www.libreriavirtuali.com/inicio/Los-l%C3%ADmites-al-derecho-de-acceso-a-la-informaci%C3%B3n-p%C3%BAblica-p83707115

[327] Piñar Mañas es partidario de esta posición, y menciona que: "parece claro que lo que quiero plantear es las reservas que genera el hecho de haber creado un órgano específico y nuevo como el Consejo de Transparencia, que no debe tener competencias en materia de protección de datos y que, sin embargo, va a verse abocado a ejercerlas, pese a que es la Agencia de Protección de Datos la que, de acuerdo con la LOPD, la Directiva 95/46/CE y el propio artículo 8 de la Carta Europea de Derechos Fundamentales, está llamada a tutelar y proteger el derecho fundamental a la protección de datos personales". Ver en: Piñar Mañas, J.L. (2014). Transparencia y derecho de acceso a la información pública. Algunas reflexiones en torno al derecho de acceso en la Ley 19/2013, de transparencia, acceso a la información y buen gobierno. *Revista catalana de dret públic*, Núm 40 (diciembre 2014). pp. 1-19.

Partiendo de lo anterior, el legislador español pudo optar, según la tendencia internacional, entre dos modelos para garantizar la aplicación y ejecución de las disposiciones contenidas en la LTAIBG por medio de una autoridad pública independiente: la instauración de una autoridad *ad hoc*, o bien, atribuir la competencia de la interpretación y aplicación del derecho de acceso a la información a una agencia ya existente, como la AEPD. Esta última opción para algún sector doctrinal resultaba conveniente por la evidente conexión entre ambos derechos[328], pero otros alertaban sobre el panorama restrictivo al derecho de acceso a la información en caso de que fuese tutelado por una agencia especializada en proteger los datos personales[329].

Finalmente, el legislador se decantó por la opción de crear un órgano independiente llamado Consejo de Transparencia y Buen Gobierno, como uno organismo público con personalidad jurídica propia, con plena capacidad de actuar y con plena independencia en el cumplimiento de sus fines, según lo define el artículo 33 de la LTAIBG, que desde el punto de vista de "complejidad técnica, de necesidad de independencia y de conveniencia"[330], parece ser una solución correcta.

El CTBG tiene por finalidad, como lo indica su artículo 34, la transparencia de la actividad pública, velar por el cumplimiento de las obligaciones de publicidad,

---

[328] Al respecto, PIÑAR MAÑAS ahonda más en detalle sobre ambos modelos y concluye que "hay que resaltar que la tendencia actual es atribuir las competencias a la Autoridad de Protección de Datos. De hecho, los modelos recientes inglés y alemán, se han mostrado sumamente eficaces. En mi opinión, esta sería la solución más conveniente para nuestro país. La estrecha relación existente entre transparencia y protección de datos justifica e incluso aconseja que sea una misma autoridad la que tutele ambos derechos, aportando así una perspectiva de conjunto que se pierde, sin duda, al atribuir las funciones a entidades distintas". En: Piñar Mañas, J.L. (2009). Seguridad, transparencia y protección de datos: el futuro de un necesario e incierto equilibrio. Madrid: Fundación Alternativas. p. 55.

[329] SENDÍN GARCÍA, por el contrario, señala las razones por las cuales resulta conveniente que la interpretación de la LTAIBG no quedara en manos de la AEPD, como por ejemplo: "a) la especialización de la agencia en materia de protección de datos, que hace que le resulten ajenas las cuestiones de acceso a la información no relacionadas con la protección de datos; b) sus orígenes ligados a la protección de datos le pueden llevar a actuar con un criterio restrictivo al acceso; c) su actuación en el ámbito de protección de datos afecta también a los sujetos públicos; d) la importante carga de trabajo que ya soporta". En: Sendín García, M.A. (2014). El Consejo de Transparencia y Buen Gobierno. *Revista jurídica de Castilla y León*, Número 33. Mayo de 2014. Recuperado de:http://www.jcyl.es/web/jcyl/AdministracionPublica/es/Plantilla100Detalle/1215245063566/_/1284319275652/Redaccion. Jiménez Asensio, también resalta el "sesgo "defensivo" de un derecho específico como es el de protección de datos" por parte de la AEPD, por lo que resultaba conveniente que la tutela del derecho se confiara a una autoridad administrativa independiente. Ver en: Jiménez Asensio, R. (____). El Proyecto de Ley de Transparencia, Acceso a la Información y buen Gobierno: su posible impacto sobre los Gobiernos Locales. Recuperado de: https://www.gobiernolocal.org/historicoBoletines/nueva_web/RJA.pdf

[330] Martín Delgado, I. (2016). La reclamación ante el Consejo de Transparencia y Buen Gobierno. Un instrumento necesario, útil y ¿eficaz?. En F. López Ramón (Coord.) Las vías administrativas de recurso a debate: Actas del XI Congreso de la Asociación Española de Profesores de Derecho Administrativo, Zaragoza, 5 y 6 de febrero de 2016. Madrid: INAP pp. 291-328.

salvaguardar el ejercicio del derecho de acceso a la información pública y garantizar la observancia de las disposiciones de buen gobierno.

B. La potestad para conocer de reclamaciones

Las resoluciones que dicte la Administración Pública en materia de acceso a la información pública, ya sea su desestimación por razones expresas o por silencio administrativo, según el artículo 20 de la LTAIBG son recurribles en la jurisdicción contencioso-administrativa, sin perjuicio de que se pueda interponer ante el CTBG la reclamación que tutela el artículo 24 de la misma ley.

De conformidad con lo que dispone el artículo 24 de la LTAIBG, contra cualquier resolución expresa o presunta en materia de acceso, puede interponerse reclamación ante el CTBG con carácter potestativo y previa a su impugnación en vía contencioso-administrativo.

La reclamación, según regula el mismo artículo, debe interponerse en el plazo de un mes contado desde el día siguiente de la notificación del acto impugnado o del que se produzcan los efectos del silencio administrativo y prevé que en los casos en que la denegación se fundamente en la protección de derechos o intereses de terceros, previo a la resolución de la reclamación se dará audiencia a las personas que se pudiesen ver afectadas.

Asimismo, se otorga al CTBG un plazo máximo de tres meses para responder; sin una vez transcurrido este plazo no se hubiera emitido la resolución respectiva, se deberá entender que se ha desestimado la reclamación interpuesta.

Por último, se impone la obligación al CTBG de publicar sus decisiones[331] por medios electrónicos –previa disociación de datos personales- y comunicar al Defensor del Pueblo las resoluciones que dicte en aplicación del artículo 24 de la LTAIBG.

[331]En relación con la publicación de las resoluciones por parte del CTBG, MESEGUER YEBRA hace una anotación importante respecto de aquellas decisiones que han sido publicadas y que posteriormente ante sido impugnadas en la vía judicial. Indica que "no parece una decisión muy prudente la publicación de las resoluciones del CTyBG, estando aún abierto el plazo para la presentación de recurso contencioso-administrativo, o, interpuesto éste, hallándose todavía pendiente de resolver. Es cierto que la publicación de la resolución estimatoria no tiene por qué equivaler al acceso material a la información solicitada, pero piénsese en aquellos casos en lo que las resoluciones del CTyBG a publicadas sean anuladas en vía contencioso-administrativa. ¿Se suprime en ese momento su publicación? ¿No se suprime y se da cuenta de su anulación?". Ver en: Meseguer Yebra, J. (2014). El procedimiento administrativo para el ejercicio del derecho al acceso… *op. cit.*

Al día de hoy, según la información estadística publicada al 30 de abril de 2017, en el sitio web del CTBG[332], se han resuelto 1.738 reclamaciones, dentro de las cuales ha tenido la oportunidad de pronunciarse de forma amplia sobre la excepción del derecho a la protección de datos de carácter personal contenida en el artículo 15 de la LTAIBG como límite del derecho de acceso a la información.

A continuación se presentará una selección de las resoluciones más destacadas del CTBG en materia de transparencia, acceso a la información y protección de datos de carácter personal.

3. Resolución de reclamaciones

A. Datos sobre nombres de dominio

En un caso en que el reclamante acusa la denegación de la entidad pública RED.ES de conceder acceso a la información sobre las resoluciones dictadas en procedimientos de cancelación de dominios con especial referencia al nombre de dominio afectado por la cancelación, el CTBG emitió la R/0489/2015. En esta resolución consideró que los nombres de dominio contienen información de personas físicas identificadas o identificables así como información de personas jurídicas que resultan excluidas de la protección que concede la LOPD. Considera que en este tipo de casos lo que resulta relevante a efectos de garantizar la transparencia de los órganos públicos es el conocimiento de los criterios jurídicos aplicados por RED.ES en sus resoluciones de cancelación del dominio, siendo que conocer el titular de un dominio cancelado puede conllevar una violación del derecho a la protección de datos y a criterio del CTBG no aporta información de relevancia adicional a efectos del fin perseguido por la LTAIBG.

B. Información sobre concursos para plazas públicas

a) Información sobre otros candidatos que se presentaron en el mismo concurso y acceso a información sobre evaluadores

Por medio de la R/0312/2015, conoció de una reclamación contra la empresa Servicios y Estudios para la Navegación Aérea y la Seguridad Aeronáutica (SENASA) que se negó a conceder acceso al solicitante a información de otros candidatos que se presentaron a una misma convocatoria en la que participó. En particular, solicitó que se

[332] http://www.consejodetransparencia.es/ct_Home/consejo/Reclamaciones/reclamaciones_resueltas.html

le concediera acceso a la relación de admitidos y excluidos con sus respectivas puntuaciones, las causas concretas de desestimación de su candidatura y la composición de los tribunales en cada caso. En relación con la información de los otros candidatos que participaron en el procedimiento, el CTBG considera que si bien son datos meramente nominativos, no corresponde conceder el acceso porque se trata de personas cuya incorporación a la empresa aún no ha sido concretada o bien, que no han sido en todo caso incorporadas a la planilla al culminar el proceso. Es decir que no se trata de personas vinculadas a la organización. No obstante lo anterior, considera que los datos pueden ser facilitados de forma disociada. Asimismo, estimó que hecha la ponderación que exige el artículo 15.3 de la LTAIBG, procede entregar la información sobre los miembros que compusieron el tribunal en cada ocasión y no únicamente hacer referencia a los departamentos o unidades encargadas de seleccionar personal.

b) Solicitud de acceso a información sobre participantes, puntuaciones y motivaciones de la valoración

En la R/0005/2016 conoció de la denegación parcial por parte del Ministerio de Hacienda y Administraciones Públicas (MINHAP) de suministrar copia de un expediente administrativo y la documentación de un candidato aspirante a las plazas de un concurso específico de dicho Ministerio. Adicionalmente, el solicitante pedía se le diera acceso a la información sobre las puntaciones obtenidas por los demás candidatos, los puntos de valoración de los méritos específicos y la motivación de la valoración. No obstante, el Ministerio negó acceso a parte de la solicitud por considerar que dar acceso a la documentación aportada por el resto de aspirantes es improcedente en el tanto contiene datos de carácter personal. El CTBG considera que una vez hecha la ponderación que exige el artículo 15.3 de la LTAIBG, corresponde determinar el acceso a la información relevante del proceso selectivo que permita comprobar la limpieza e imparcialidad del procedimiento en el que participó el solicitante y los demás concursantes, lo que incluye los datos de carácter personal de las personas con quien el solicitante compitió por las mismas plazas.

C. Expedientes sancionatorios

a) Expedientes sancionatorios contra personas jurídicas

En la R/0296/2015 en la que el reclamante acusó la denegación del MINHAP de conceder acceso a un expediente sancionador seguido por la Dirección General de Coordinación de la Administración Periférica del Estado a la empresa Sacyr por una infracción grave a la Ley de Seguridad Privada y de la Protección Social, el CTBG dispuso que era procedente conceder el acceso al expediente sancionatorio en el tanto la infracción había sido cometida por una persona jurídica y no aplica la excepción contenida en el artículo 15.1 relativo a información sobre infracciones penales o administrativas.

Dicho criterio fue repetido en la R/0013/2016, en la que se solicitó acceso a un expediente sancionador abierto a Barclays Bank, S.A. por la Comisión Nacional del Mercado de Valores (CNMV) por haber cometido una infracción muy grave que posteriormente dio lugar a una publicación en el Boletín Oficial del Estado (BOE). En este caso la CNMV denegó la solicitud de acceso por considerar aplicables los supuestos del artículo 15.1; no obstante, la CTBG aclaró que la excepción aplica para personas físicas y que en caso de que en el expediente conste información personal relativa a personas físicas, debe procederse con la disociación de datos de forma que se impida la identificación de la persona física.

b) Expedientes sancionatorios contra personas físicas

Por su parte en la R/0431/2016, en la que un reclamante solicitó acceso a los nombres de los 9 cargos a los que la Oficina de Conflictos de Intereses incoó un procedimiento sancionador, estimó procedente el actuar de la Administración de sólo fueran facilitar los nombres de 5 de los funcionarios cuya sanción había sido publicada en el BOE. Estima el CTBG que de conformidad con lo dispuesto en el artículo 15.1 de la LTAIBG no corresponde otorgar el acceso a la información de la totalidad de las personas, pues la norma es clara en señalar que se suministrarán los datos únicamente en aquellos casos en que la comisión de una infracción conlleve la publicación de la sanción.

c) Acceso a datos sobre infracciones penales y administrativas

Sobre este tema, el CTBG ha avalado por ejemplo en la R/0258/2015, la negativa del Ministerio del Interior de dar acceso a una denuncia administrativa presentada ante la

Inspección de Personal y Servicios de Seguridad. A juicio del Consejo, procede denegar la solicitud con base en lo dispuesto en los artículos 15.1. No sólo pueden constar datos especialmente protegidos dentro del expediente al que se solicitaba acceso, sino que además se tratan de datos relativos a la comisión de infracciones administrativas y no se cuenta con el consentimiento expreso del interesado ni existe una ley que permita el acceso al expediente por terceros distintos al interesado.

D. Información sobre agendas públicas y reuniones de altos cargos

a) Agendas públicas

En 2015 el CTBG conoció de una reclamación presentada contra el Ministerio del Interior por haber denegado al reclamante el acceso al listado de reuniones del Ministro durante la legislatura, con indicación de la fecha, persona o entidad con quien se reunió, lugar y el asunto que fue tratado. En esta ocasión, el Ministerio del Interior deniega parte de la información solicitada y argumenta que la agenda oficial del Ministro del Interior dispone de una parte pública que es consultable en el sitio web y otra parte que no es de conocimiento general porque su difusión no es necesaria, oportuna o conveniente. En la R/0393/2015, el CTBG aborda este tema y critica el absurdo en que incurre en esa ocasión el Ministerio del Interior de distinguir entre una agenda oficial con informaciones públicas y una "agenda no oficial", ya que siendo que una agenda es el reflejo del desempeño de las funciones del alto cargo, debe procurar ser pública en su mayoría salvo que aplique un límite legalmente previsto.

Resalta el CTBG que analizadas las agendas oficiales, lo informado a la ciudadanía es sólo excepcional, siendo que se extrae del conocimiento de los ciudadanos lo que atañe al proceso ordinario de toma de decisiones y responsabilidad de los funcionarios. Y dispone que si bien la LTAIBG hace referencia a la rendición de cuenta del dinero público, la rendición de cuentas del tiempo público es un derecho esencial de la transparencia también.

Ahora bien, reconoce también que el acceso a la información puede llegar a afectar los datos de carácter personal, que en todo caso alcanza a las personas físicas y no a las jurídicas quienes como ha sido claro, quedan excluidas del ámbito de aplicación las personas jurídicas. En ese sentido, es criterio del Consejo que la información que se recoja en la agenda debe evitar incluir datos personales de personas físicas que no representen a empresas, organizaciones o administraciones y entidades públicas y privadas. En caso de

que existan tales datos de carácter personal deben sustraerse dicha información y hacer de conocimiento del solicitante que los mismos han sido disociados. Esta tesis fue sostenida por el CTBG en las resoluciones R/0397/2015, R/0398/2015, R/0404/2015, R/0410/2015, R/0415/2015, R/0416/2015, R/0424/2015, R/0425/2015, en las que concedió el acceso a las agendas oficiales del Ministro de Empleo y Seguridad Social, Ministro de Asuntos Exteriores y de Cooperación, Ministerio de Defensa, Ministro de Fomento, Ministro de Educación, Cultura y Deporte, Ministro de Industria, Energía y Turismo, Ministro de Agricultura, Alimentación y Medio Ambiente y del Ministro de Justicia.

b) Reuniones de altos cargos

(*Cambio de criterio sobre acceso a la información de agendas y reuniones)*

El avance que supuso inicialmente la posición del CTBG en relación con el acceso a la información contenida en las agendas públicas de los funcionarios, si bien no varió en cuanto al reconocimiento de la importancia de la publicación y acceso a esta información, si se reconsideró en la R/0091/2016 esta posición. En ese caso, el CTBG conoció de una reclamación presentada contra la denegación parcial del Ministerio de Asuntos Exteriores y Cooperación (MAEC) de conceder acceso a la información sobre el listado de los viajes del Ministro, el destino, acompañantes, agenda completa de visita, reuniones, personas con quien se reunió, motivo de la reunión, contenidos de la conversación, acuerdos entre otros. El Ministerio únicamente concedió acceso a la información que consta en la página web, decisión ante la cual el solicitante interpuso reclamación ante la CTBG.

En la resolución mencionada, el Consejo recuerda en primer lugar, que las reuniones mantenidas y celebradas por los altos cargos en el ejercicio de sus responsabilidades constituye actividad pública según el artículo 13 de la LTAIBG y está cubierta por el fin que persigue la ley. Posteriormente, hace un llamado a la necesidad de definir y regular la necesidad de recoger la participación en reuniones así como a formular una obligación y un compromiso en la rendición de cuentas en estos términos. Seguidamente, hace alusión a que debe tenerse en consideración que la información relativa a reuniones o agendas públicas puede contener datos personales de quienes hayan asistido y que resultan merecedoras de la protección de la LOPD. Esto implica, por ejemplo, que al no haberse recabado inicialmente el consentimiento del titular de los datos

para la cesión de la información, el acceso a la misma debe resolverse no sólo de acuerdo con el artículo 15 de la LTAIBG, sino también con los criterios y disposiciones en materia de protección de datos. Asimismo, resuelve que en el hipotético caso en que se hubieran guardado datos relativos a reuniones, su acceso debe analizarse de acuerdo a las reglas que regulan la relación entre el derecho de acceso a la información y el derecho a la protección de datos.

Añade además que no es posible, para estos efectos, utilizar los datos que se recogen en los registros de entrada de los edificios como elementos susceptibles de confirmar visitas de trabajo, ya que dichos ficheros se rigen por la LOPD y la Instrucción 1/1196 de la AEPD en la que se indica que los datos que se obtienen como parte de los registros de entrada de los edificios no pueden ser utilizados ni cedidos para fines distintos a la seguridad y control, salvo con el consentimiento del interesado y deben ser destruidos cuando haya transcurrido el plazo de un mes a partir del momento en que fueron recabados.

Con base en lo expuesto concluye que si bien en varias ocasiones ha respaldado solicitudes de acceso a la información de reuniones mantenidas por los responsables públicos, entiende las dificultades que encuentran las Administraciones para recabar y proporcionar esta información que no ha sido organizada, clasificada o sistematizada de forma que se pueda dar acceso en los términos en los que solicita el reclamante. Igualmente, considera que es necesario que se delimite lo antes posible qué debe considerarse "agenda" a efectos de la transparencia y que se defina qué información debe incorporarse, los eventuales límites y se comprometa a los responsables públicos a proporcionar de manera clara, sistemática y actualizada información sobre la actividad que desarrollan en el ejercicio de sus funciones públicas. Esta tesis ha sido sostenida al menos en las siguientes 18 resoluciones: R/0120/2016, R/0121/2016, R/0122/2016, R/0123/2016, R/0124/2016, R/0125/2016, R/0126/2016, R/0127/2016, R/0128/2016, R/0129/2016, R/0130/2016, R/0131/2016 R/0139/2016, R/0140/2016, R/0143/2016, R/0143/2016, R/0154/2016, R/0155/2016.

E. Información sobre pasaportes diplomáticos

En la R/0171/2016 el CTBG resolvió una reclamación que tuvo como origen la denegación parcial del MAEC de dar acceso a un listado que contuviera el número de pasaportes diplomáticos válidos, expedidos y caducados o que perdieron su validez en los

años 2008 a 2015, así como una relación de titulares de pasaportes con detalle de nombre y apellidos del titular, cargo del titular, fecha de expedición del pasaporte diplomático, fecha de renovación y fecha de pérdida de validez. El MAEC concedió acceso a un cuadro que contenía el número de pasaportes expedidos en los años solicitados así como los pasaportes caducados o que perdieron validez en ese tiempo. No obstante lo anterior no concedió acceso a la relación de personas que solicitó el reclamante por considerar que es contrario a los preceptos 15.1 y 15.3 de la LTAIBG.

A este respecto, el CTBG estimó que la identificación de quienes ocuparon los cargos que ameritan pasaporte diplomático equivaldría a una revisión de cada uno de los expedientes sobre pasaportes concedidos con el fin de poder identificar el cargo con la persona que lo ocupaba en cada momento, por lo que procede negar el acceso en dichos términos según el artículo 18.1.c) de la LTAIBG. Por otra parte, considera que no son sólo titulares de pasaportes diplomáticos los cargos que aparecen mencionados en la ley, sino que los hijos menores y otros miembros de la familia en determinadas situaciones específicas. Sobre estas personas que ostentan un pasaporte diplomático en razón de su lazo familiar con el titular, conceder el acceso a sus datos personales supondría una vulneración al derecho a la protección de datos personales que no está previsto ni amparado por la LTAIBG dada la condición privada que ostenta esa categoría de titulares.

F. Condecoraciones policiales

En la R/0490/2015 el CTBG conoció de una reclamación interpuesta contra la decisión del Ministerio del Interior de negar el acceso al reclamante al historial profesional de las propuestas de ingreso en la Orden del Mérito Policial con Distintivo Rojo, tanto de los funcionarios del Cuerpo Nacional de Policía como de terceros a los cuáles se les había otorgado dicha condecoración. El Ministerio del Interior niega el acceso a la información por considerar que la misma contiene datos de carácter personal y hecha la ponderación del artículo 15.3 de la LTAIBG no procede la entrega de la misma. Manifiesta que tampoco ha existido consentimiento por parte de los interesados. Esta posición la avala el CTBG que considera que tal y como lo argumenta el Ministerio del Interior, conceder acceso a la información sobre las personas a las que se otorga dicha condecoración junto con los méritos por los cuáles le fue otorgada, conlleva a poner en riesgo la integridad de las personas así como el buen término de las operaciones que estén en curso. Asimismo, a su juicio existe un riesgo previsible y no hipotético tanto a la

integridad personal como al derecho a la protección de datos personales, por lo que no procede facilitar la información solicitada. Adicionalmente, resalta el carácter discrecional de la condecoración. Por todo esto, estima que hecha la ponderación que exige la LTAIBG, no prevalece el interés público en conocer la información solicitada y por ende, se desestima la reclamación.

Por sentencia 162/2016, de 2 de diciembre, dictada por el Juzgado Central Contencioso-Administrativo *núm.* 10 de Madrid, se resolvió la demanda interpuesta por el reclamante contra la resolución del CTBG que confirmó la negativa del Ministerio del Interior de otorgar el acceso a la información solicitada. A criterio del Juzgado Central, el acceso a la información no supone un riesgo en los términos señalados por el CTBG y considera que la información a la que se pretende acceder, es necesaria para comprobar si se ha cumplido la normativa para concesión de esta condecoración y discernir si la Administración se ha movido en el ámbito de la discrecionalidad sin incurrir en arbitrariedad. Asimismo, resalta que se trata de información pública que tiene trascendencia presupuestaria.

Esta sentencia fue posteriormente confirmada por la sentencia de la Audiencia Nacional (SAN), de 17 de abril de 2017, que indica que el carácter discrecional del otorgamiento de las condecoraciones no desvirtúa lo apuntado por el a quo, así como que el acceso tampoco afecta datos personales, no implica la colocación de los mismos en una situación de inseguridad ni pone en riesgo las operaciones iniciadas por medio de las cuales se han otorgado los méritos. A criterio de la AN el carácter discrecional no lleva a que el sindicato reclamante deje de tener acceso a los expedientes con el historial por el cual se concede el mérito, si ello responde a fines perseguidos por el sindicado y las condecoraciones tienen efectos presupuestarios. Por otra parte, señala que como quedo expuesto en el proceso ante el a quo, la Dirección General de Policía anunció dar publicidad a los expedientes de otorgamiento de dichos méritos, los cuales además no suponen la divulgación de un dato sensible. Con base en lo anterior, estima que lo que procede con base en el artículo 13 de la LTAIBG es la ponderación de los intereses en conflicto, la cual fue hecha de forma correcta por el Juzgado que termino por conceder el acceso a la información solicitada. Por estas razones y la trascendencia presupuestaria de las resoluciones adoptadas en dichos expedientes, desestima el recurso de apelación interpuesto por el CTBG contra la resolución del Juzgado.

G. Datos de autores de notas técnicas

En la R/0433/2015, el CTBG conoció de una reclamación contra ENAIRE por la denegación parcial de acceso a información sobre una nota técnica con identificación y firma del autor. En esta ocasión, el CTBG consideró que si bien el nombre y apellidos del autor de una nota técnica constituyen datos meramente identificativos al tenor del artículo 15.2 de la LTAIBG, no procede conceder el acceso a dicha información, por cuanto el conocimiento del autor de una nota técnica no tiene incidencia pública desde el momento en que el contenido de la misma es asumido por ENAIRE. Es decir, que esa condición hace que la identidad del autor inicial de la información carezca de relevancia pública para los efectos de la solicitud de información.

H. Datos contenidos en expedientes relativos a trámites migratorios

En la R/0466/2015 el CTBG conoció de la denegación de la Dirección General de los Registros y del Notariado de conceder acceso a la copia de una resolución dictada con ocasión de la interposición de un recurso de reposición en un proceso de nacionalidad por residencia. Pese a que el solicitante indicó que la información debía remitirse con los datos personales suprimidos y únicamente sobre los fundamentos y resolución final, la Dirección General de los Registros y del Notariado negó el acceso por considerar que la información se refiere a un tercero así como que los documentos que se aportan en este tipo de procedimientos incluyen datos sobre partida de nacimiento, certificación de antecedentes penales, entre otros. Esto, a criterio de la Dirección General de los Registros y del Notariado hace que prevalezca el derecho a la protección de datos de carácter personal sobre el derecho de acceso a la información.

En su resolución, el CTBG considera que la copia de la resolución que solicitó el reclamante contiene al menos el nombre y apellidos de una persona que está en trámites de residencia, así como datos asociados a su personalidad que no necesariamente son datos especialmente protegidos pues no se refieren a ideología, afiliación sindical, religión, creencias, origen racial, salud, vida sexual o comisión de infracciones penales o administrativas. Si bien en el caso concreto el CTBG reconoce que en el expediente puede constar información como la certificación de antecedentes penales del tercero, el reclamante al menos en esa ocasión no solicitaba acceso al expediente completo sino a una copia de la resolución final.

Dispone el Consejo que si la Administración proporciona al reclamante copia de la resolución de manera disociada o anonimizada, queda eliminada la información de carácter personal y no sería de aplicación el límite a la protección de datos en el caso concreto. Sin embargo, hace la aclaración de que en este caso, el reclamante identifica exactamente el expediente en el que se dio trámite al recurso de reposición del cual solicita una copia de la resolución final, la fecha de interposición del recurso y la fecha de la resolución. Esto a criterio del CTBG permite entender, o cuando menos suponer, que el reclamante conoce suficientes detalles del expediente como para conocer ya de antemano la identidad de la persona que lo interpuso, por lo que disociar los datos no cumpliría con la función de proteger la identidad del tercero. En este caso, el CTBG entiende que de concederse el acceso a la información no respeta el derecho a la protección de datos.

I. Datos especialmente protegidos

a) Información sindical

En la R/0049/2016, el CTBG resolvió una reclamación que tenía por objeto impugnar la decisión de la Agencia Portuaria de no conceder copia de las resoluciones de Puertos del Estado sobre reconocimiento de perfil competencial a liberados sindicales por considerar que la misma hace referencia a datos de carácter personal. En su resolución, el CTBG indica que el nombre y apellidos de un libertado sindical constituye un dato especialmente protegido en el artículo 7 de la LOPD en el tanto está vinculado a la condición de afiliación sindical de la personal. En estos casos la ley condiciona el acceso al consentimiento del afectado o que este haya hecho manifiestamente público el dato y dentro del expediente no consta que haya concurrido ninguna de ambas causales. No obstante lo anterior, apunta que la LTAIBG permite la disociación o anonimización de datos personales, por lo que la Administración puede suministrar copia de las resoluciones eliminando el nombre y apellidos del titular así como el sindicato al que pertenecen, de forma que se pueda cumplir con el objetivo de la transparencia. Lo contrario conllevaría a vulnerar el derecho a la protección de datos personales.

b) Datos sensibles derivados del conocimiento de otros documentos, por ejemplo, declaración patrimonial de altos cargos

Por su parte, la R/0051/2016 resolvió un caso que tenía por objeto rebatir una denegación parcial de acceso a la información por parte de la Oficina de Conflictos de Intereses del MINHAP. El solicitante reclamaba acceso a la información sobre la declaración de actividades a la toma de posesión, declaración de bienes a la toma de posesión y declaraciones anuales para los años 2012, 2013 y 2014 del Presidente y sus ministros. La denegación de la Agencia estribó en que dichas declaraciones tienen un carácter reservado así como que conceder el acceso a las mismas supondría una vulneración al derecho a la protección de datos. En este caso, el CTBG coincide con la posición de la Administración en el tanto es diferente conocer una eventual variación patrimonial de un alto cargo y otra acceder a la totalidad de sus declaraciones patrimoniales fuera de su esfera laboral o profesional, que contienen datos de localización e identificación de los bienes inmuebles así como datos del ISR de las personas físicas.

Asimismo, considera que dar acceso a esta información conlleva al conocimiento y potencial vulneración de otros datos especialmente protegidos como la orientación sexual (en el supuesto de matrimonio con una persona del mismo sexo), la ideología (si el alto cargo contribuye a organizaciones políticas), la religión (si el declarante optara por contribuir a la iglesia católica), la salud (en caso de que tanto el alto cargo o alguno de sus familiares directos padezcan algún tipo de discapacidad), así como los datos identificativos tanto del cónyuge como de sus descendientes. Con base en lo anterior, el Consejo concluye que existen datos especialmente protegidos y que se encuentran en la esfera íntima, personal y familiar de los titulare de los datos por lo que no puede divulgarse dicha información sin atención a lo que exige la normativa vigente.

Por otra parte, en la R/0360/2016 resolvió una reclamación en la que el solicitante acusaba la negativa del Ministerio de Interior de remitir toda la información relativa a los expedientes sancionadores tramitados por la Administración General del Estado en aplicación de la Ley Orgánica 4/2015 de 30 de marzo, de protección de la seguridad ciudadana. Asimismo, solicita se desglose por provincia, Comunidad Autónoma y con un periodo del 2015 en adelante. En esta ocasión, al igual que las anteriores, el CTBG es enfático en señalar que la solicitud del reclamante incide en datos especialmente

protegidos y no consta en el expediente que los afectados hayan dado su consentimiento o exista una norma legal que habilite la cesión de tales datos.

J. Datos meramente identificativos

En la R/0099/2015, dispuso que los datos –nombre, apellido y cargo- que constan en los Planes Operativos Anuales (POA) de la Secretaría de Estado de Cultura (SEC) son datos meramente identificativos e indican el responsable de cada una de las medidas contenidas en el POA, por lo que procede hacer entrega de la información sin disociar los datos, tal y como lo pretendía la Administración. En este caso es evidente la vinculación de la identificación personal con la actividad pública del órgano y la responsabilidad en el ejercicio del cargo, por lo que prevalece el acceso a la información sobre la protección de datos de carácter personal.

Por su parte, en la R/0418/2015 por medio del cual se solicitada el acceso a una memoria científica de un proyecto estatal con referencia a los datos identificativos de los investigadores (nombre, universidad, facultad, teléfono, dirección y e-mal en la universidad de contacto, el CTBG estimó que si bien es cierto la información que se solicita es información meramente identificativa vinculada con la organización, funcionamiento y actividad pública, en este caso, del Ministerio de Economía y Competitividad, siendo que los investigadores no están vinculados al Ministerio, corresponde solicitar la información directamente a la universidad a la que pertenecen.

K. Datos de pasajeros de transportes oficiales

El CTBG resolvió por medio de la R/0429/2015 una reclamación que tenía como objeto conocer el listado de pasajeros que acompañaron a las autoridades transportadas por la flota del Grupo 45 de la Fuerza Aérea Española con un desglose de las fechas de vuelo, ciudad, aeropuerto, origen y destino. El Ministerio de la Defensa deniega parcialmente acceso y apunta que la información sobre vuelos de la Presidencia o la Casa Real es clasificada. Asimismo apela a que el hecho de que el personal transportado sean representantes de primer orden y que el gasto sea sufragado con fondos públicos no lleva implícita la prevalencia del interés público sobre la divulgación de la información.

En la resolución citada, el CTBG trae como un primer elemento que el Grupo 45 de la Fuerza Área Española se dedica de forma exclusiva a realizar misiones de transporte público, lo que permite concluir que los datos solicitados son meramente identificativos

y están dirigidos a obtener información sobre las personas que han sido transportadas por el Grupo 45 dentro de su actividad pública por lo que es posible su encuadramiento dentro de los supuestos del artículo 15.2 de la LTAIBG. Asimismo, indica que la información tiene relevancia en el tanto permite el control de los desplazamientos y que los mismos no se efectúen al margen de actos o reuniones inherentes al cargo público.

Ahora bien, analiza el CTBG que la información solicitada puede contener datos personales que se refieren a las autoridades y sus acompañantes. Los primeros –datos de las autoridades transportadas- deben recibir un tratamiento de datos identificativos relacionados con la organización del órgano o entidad en el que prestan los servicios. Consideración diferente debe aplicarse a los datos de los acompañantes cuya actividad no está enmarcada en el funcionamiento del organismo o entidad pública y por ende queda excluido del conocimiento de los terceros.

Por su parte, la R/0381/2016 desestimó la reclamación del solicitante por medio de la cual impugnaba la decisión del Ministerio de Industria, Energía y Turismo, de únicamente facilitar acceso a los datos que constaban en su expediente, cuando lo solicitado era que se concediera el acceso a los expedientes terminados relativos al reconocimiento de cualificación profesional para el ejercicio de Agente de la Propiedad Industrial. A juicio del CTBG en este caso no se está ante un supuesto de concurrencia competitiva y siendo que la puntuación obtenida por los otros candidatos no tiene incidencia directa en las posibilidades del interesado en el proceso de selección, prevalece el derecho a la protección de datos personales.

L. Disociación de datos personales

a) Aplicación de la disociación con independencia del soporte que contenga la documentación

Sobre este particular, el CTBG ha señalado que la disociación de datos personales procede con independencia del soporte en que el que se haya solicitado o se vaya a facilitar el acceso a la información. En la R/0099/2015, conoció de una reclamación presentada contra la SEC por no dar acceso en soporte digital a los POA de los años 2012 a 2015. La negativa de la Administración radica en que dada la dificultad de disociar los datos personales que constan en dichos documentos, no puede facilitarse la información en formato digital pero si puede ser puesta a disposición en sus dependencias para

consulta del reclamante. En este caso, el CTBG indica que la disociación aplica tanto como si la información es facilitada en formato físico o digital. Es decir, que con independencia de que sea entregada en soporte digital o sea puesta a disposición, si existen datos de carácter personal, deben ser disociados.

b) Disociación de datos como condición para el acceso a la información

En la R/0109/2015 – y posteriormente en un similar sentido en a R/110/2015- se estimó procedente el mecanismo de disociación propuesto por el reclamante ante la Administración. El reclamante, quien solicitó acceso a información sobre la productividad de directores y subdirectores de distintos centros penitenciarios así como gratificaciones e indemnizaciones por servicio, recibió de parte de la Entidad Estatal de Trabajo Penitenciario y Formación para el Empleo dicha información pero no de forma individualizada por considerar que ello podría suponer una afectación al derecho a la protección de datos. A criterio del CTBG en este caso procedía facilitar la información requerida previa disociación de los datos personales, siendo para ello válido el mecanismo propuesto por el reclamante, sea que no se indique el nombre y apellidos del titular, sino que únicamente se indique si la información relativa es al director 1, director 2 y así sucesivamente, sin que se permita la individualización de cada puesto.

c) Disociación de datos en casos en que con la información solicitada se permite la individualización de la persona física beneficiario de becas universitarias

La R/0407/2015 resolvió una reclamación que tiene como origen la denegación parcial de acceso a una solicitud planteada ante el MECD en la que el reclamante solicitaba el acceso a una base de datos anonimizada con los estudiantes de universidades que fueron beneficiados con una beca en la convocatoria 2014-2015, en la que se detallara, sin identificación o nombre del becario, el sexo, universidad, área o rama de estudios, cuantía variable a percibir, cuantía variable mínima, nota media, renta per cápita de becario, entre otros. En este caso, el CTBG hace uso de la definición de dato personal que contiene la normativa de protección de datos y recuerda que no sólo los datos identificativos de una persona física como el nombre o apellidos son datos personales, sino que lo son todos aquellos que hacen a una persona física identificada o identificable. En el caso concreto, conceder el acceso a información de un beneficiario de una beca para cursar un máster con un número reducido de estudiantes, permite la identificación de la

persona física y también conocer información que atañe a su situación socioeconómica. Partiendo de ello, considera que la información solicitada por el reclamante puede ser facilitada si es desagregada, con porcentajes y con fines estadísticos, sin perjuicio de la protección de los datos personales que contiene la base. Así por ejemplo, menciona que se puede conceder el acceso a los siguientes datos de esta forma: sexo (porcentaje de hombres y mujeres), universidad en la que se han matriculado (identificación, en porcentaje respecto del total, de las universidades con beneficiarios de becas), área o rama de los estudios universitarios (identificación, en porcentaje del total, de lo estudios con beneficiarios de becas), medias de las notas media de los beneficiarios y renta per cápita media.

d) Disociación como requisito para acceso a actas en las que pueden constar datos sensibles o relativos a infracciones administrativas

En otro caso, el CTBG consideró que no procedía la entrega de la información pues aún con la disociación de los datos de carácter personal se permitía la identificación de la personal. En la R/0296/2015, en la que conoció de una reclamación contra el MAEC por denegar el acceso a las actas de cada una de las sesiones de la Junta de la Carrera Diplomática, el CTBG estimó que la solicitud de acceso planteada podía incidir en datos especialmente protegidos, pues las actas pueden llegar a contener la valoración de aspectos como infracciones administrativas con carácter sancionados. Considera, además, que los datos contenidos en las actas constituyen un perfil laboral de cada uno de los funcionarios designados para asumir tareas inherentes al puesto, de manera que los datos no pueden ser disociados, pues aun así se puede identificar a la persona física de manera sencilla.

M. Exclusión de las personas jurídicas del ámbito de aplicación de la excepción contenida en el artículo 15

Desde sus primeras resoluciones, el CTBG se ha encargado de reiterar que la excepción que establece el artículo 15 de la LTAIBG, aplica a personas físicas según lo dispuesto por tanto por el artículo 1 y el artículo 3 de la LOPD.

Así por ejemplo, en la R/0026/2015, estimó una reclamación presentada ante la negativa de Confederación Hidrográfica del Ebro de conceder acceso al reclamante a un certificado de reversión de una finca así como copia de un plano de expropiación de una

finca urbana. En dicha ocasión, la Administración entendió que los títulos de propiedad que habían sido otorgados tanto al Obispado de Barbastro como al Ayuntamiento de Ainsa-Sobrabe contenían datos personales de difícil disociación. En esta ocasión, el CTBG enfatizó que la información que afecta a organismos públicos, entidades o personas jurídicas de cualquier tipo, no está cubierta por la protección que sí otorga la normativa de protección de datos a las personas físicas. En un caso en el que el titular de las fincas es un Ayuntamiento o un Obispado resulta improcedente denegar el acceso bajo la excepción de protección de datos de carácter personal.

Por otra parte, en la R/0214/2015, en la que el Ministerio de la Presidencia negó a el acceso a las opiniones que habían sido remitidas voluntariamente dentro del proceso de consulta pública en la tramitación de la LTAIBG, estimó que la excepción de que contiene el artículo 15 de la LTIABG únicamente protege los datos de las personas físicas que remitieron opiniones mas no así respecto de las empresas, asociaciones, organismos o cualquier otra persona jurídica. También aclaró que la excepción del artículo 15 lo es respecto de los datos personales y no de los contenidos de cada opinión remitida.

En similar sentido, en la R/0393/2015, en relación con una solicitud de acceso a la agenda del Ministerio del Interior, recordó que de aplicar la excepción de protección de datos contenida en el artículo 15 de la LTAIBG, la misma alcanza únicamente a personas físicas, según lo dispone la LOPD, quedando excluidas del ámbito de aplicación las personas jurídicas.

N. Listado de asistentes y participantes de actividades oficiales

Por medio de una solicitud de acceso a la Casa Real, el posteriormente reclamante solicitó se le otorgara información sobre el gasto y la lista de asistentes e invitados a la recepción en el Palacio de Oriente tras el desfile de las Fuerzas en el Día de la Hispanidad. A su solicitud en lo que se refiere a la protección de datos, la Secretaría General de la Presidencia del Gobierno se limitó a indicar que entre los asistentes se encontraban personas pertenecientes a diferentes instituciones (Gobierno, Congreso, Senado, Tribunal Constitucional, Consejo General del Poder Judicial, Defensor del Pueblo, etc.) así como otras personas de diferentes sectores sociales de la vida pública española. Entendiendo el solicitante que esto no satisfacía su solicitud, presentó reclamación ante el CTBG. Sobre el listado completo de asistentes, considera el CTBG que no puede desconocerse que es acorde con el espíritu de la LTAIBG conocer el perfil institucional o social de los

asistentes a una recepción por medio de la que conmemora una fiesta nacional. De ahí que solicitar acceso a la lista de los asistentes es acorde al objetivo que persigue la ley; no obstante lo anterior, conocer el listado completo de asistentes, incluido acompañantes, excede el concepto de actividades sujetas a Derecho administrativo reguladas en la LTAIBG, por lo que opera un límite al derecho de acceso a la información en ese sentido.

O. Ejercicio de ponderación

a) Interés público en conocer evaluadores de planes de agencias estatales

(En un sentido similar se puede ver la STJUE de 16 de julio de 2015, caso Client Earth y PAN Europe/EFSA)

Asimismo, en aplicación de la ponderación que exige el artículo 15.3, dispuso en la R/0080/2016 que procede conceder el acceso a una Declaración de conflicto de intereses y confidencialidad de la Agencia Española de Medicamentos y Productos Sanitarios –que contiene datos identificativos de personas físicas-, ya que existe un interés público en conocer si se ha desarrollado por parte de los revisores externos del plan alguna actividad que pueda entrar en conflicto con ese rol de revisión dentro de uno de los comités de la Agencia Española de Medicamentos. A juicio del CTBG, es acorde con el fin que persigue la LTAIBG conocer si existen conflictos de interés entre los revisores de un plan así como que la planificación obedezca a fines privados y no a fines públicos.

b) Autorizaciones a funcionarios públicos para realizar actividades privadas

En la R/0075/2016, conoció de la denegación parcial del MINAHP de conceder acceso a una solicitud de información que tenía por objeto acceder a la información sobre la relación de abogados del Estado en activo que tenían autorización de la Oficina de Conflictos de Intereses para realizar actividades en el sector privado, con indicación del detalle del puesto, actividades para las que se concedió la compatibilidad, fecha en que se concedió y la empresa en las que las realiza. El MINHAP denegó el acceso a la información por considerar que hecha la ponderación del artículo 15.3 de la LTAIBG no procede conceder el acceso a los datos nominativos solicitados. En la resolución, el CTBG considera que la finalidad perseguida con la divulgación de la información a la que se solicita el acceso, sea el conocimiento y control público de determinados funcionarios que han sido autorizados para llevar a cabo determinadas actividades particulares sólo se cumple si se hace pública la identidad. De ahí que no lleva razón el Ministerio en negar

el acceso a la información porque no puede presuponerse una limitación absoluta al acceso a la información con fundamento en la aplicación del derecho a la protección de datos.

c) Procedencia de entregar datos totalizados cuando se permite la identificación física de los interesados

En otro caso consideró que la información que solicitaba el reclamante, hecha la ponderación exigida, excedía más allá de lo estrictamente relacionada con la organización, funcionamiento o actividad del órgano. En la R/0250/2016 resolvió la negativa de acceso parcial del Ministerio del Interior a una solicitud del reclamante que tenía por objeto conocer el número de funcionarios con prolongación o prorroga en servicio activo hasta los 70 años de edad, desglosado por cuerpos, puestos y centros de trabajo. El Ministerio del Interior únicamente dio acceso a información sobre el número de funcionarios de algunos centros penitenciarios y siendo que en algunos de ellos cuentan únicamente con un funcionario, dio un número global de las personas y los centros penitenciarios (22 funcionarios en 22 centros penitenciarios). Al hacer la ponderación del artículo 15.3 de la LTAIBG, el CTBG considera que informar sobre el cuerpo o puesto de trabajo que ocupa un funcionario en centros en los que es el único destinatario o no existe un número elevado de empleados de forma que se pueda identificar al titular sin esfuerzos desproporcionados resulta en una injerencia a la protección de los datos personales de ese tercero. En ese sentido, determinó que la información globalizada brindada por el Ministerio del Interior satisface el fin de la transparencia que persigue la LTAIBG.

d) Improcedencia de denegaciones con base en argumentos genéricos sobre la puesta en peligro o perjuicio al derecho a la protección de datos personales

Por su parte, la R/0258/2016 resolvió una reclamación que tenía como objeto rebatir la denegación de acceso parcial a una solicitud dirigida al Ministerio del Interior para que brindara información sobre las personas que habían sido nombradas comisionarios honorarios. El Ministerio del Interior envió al reclamante una nota en la que indica que los honorarios nombrados en la última legislatura son 148 personas pertenecientes a la Policía Nacional y 7 personas ajenas a ese cuerpo. Omite dar el nombre de esas 7 personas por considerar que ello atenta contra su seguridad y la protección de

datos personales. Considera el CTBG que la información solicitada tiene incidencia en el mecanismo de rendición de cuentas previsto en la LTAIBG. Continua su análisis indicando que la información que requiere el solicitante (el nombre de las 7 personas nombradas Comisionarios Honorarios ajenas al Cuerpo Nacional de Policía) no son datos especialmente protegidos ni tampoco se trata de datos meramente identificativos relacionados con la organización, funcionamiento o actividad pública del órgano, pues dichas personas no forman parte del Cuerpo Nacional de Policía. En relación con el alegato sobre el perjuicio de la seguridad de los Comisionarios Honorarios, el CTBG indica que puede constatarse en algunos de los casos pero no en todos, pues de una búsqueda en internet se encuentran datos de personas reconocidas como Comisionarios Honorarios y en las cuales no se ha estimado que dicha publicación afectase la seguridad de los individuos.

Con base en lo anterior, el Consejo determina que no cabe hacer consideraciones generales en la aplicación de las excepciones y límites al derecho de acceso a la información previstos en la LTAIBG. De igual forma, recrimina al Ministerio del Interior no haber hecho una ponderación adecuada en todos los casos ni haber procedido con la apertura de un trámite que permitiese a los afectados alegar lo que estimaran conveniente en relación con sus derechos. Este trámite además de permitir obtener el consentimiento del interesado, hubiese permitido a la Administración contar con mayores elementos para ponderar adecuada y justificadamente la incidencia de la solicitud de acceso a la información en los derechos de los afectados.

P. Retribuciones y RPT

En relación con el acceso a información sobre las retribuciones de funcionarios públicos, existen además del criterio de interpretación conjunta emitido por el CTBG junto con el AEPD, numerosos casos que ya han sido resueltos en sede administrativa bajo dichos parámetros. En este apartado nos referiremos a algunas de las que nos parecen más relevantes para el efecto de esta investigación.

a) Acceso a la información sobre retribuciones de altos cargos y personal directivo

El CTBG ha estimado solicitudes de acceso en aquellos casos en que las Administraciones Públicas se niegan a conceder el acceso a la información sobre

retribuciones por considerar que se tratan de datos de carácter personal o cuya revelación contribuye poco a la consecución del objetivo de la transparencia que persigue la LTAIBG. Sobre este particular, en la R/0087/2015, reconoció que debía facilitarse al solicitante, las retribuciones que percibían los puestos de Director adjunto de Administración y Recursos Humanos y Director adjunto de operaciones de una determinada empresa, bajo el entendido de que al ser puestos de alto nivel en la jerarquía prima el interés público sobre la privacidad de las personas. Asimismo, reconoció que para los demás casos, por ejemplo, información sobre retribuciones de otros cargos de la empresa o Administración Pública que no sean los de alta jerarquía, debe facilitarse la información de forma disociada y que no se permita la identificación física del funcionario.

b) La LTAIBG constituye un título habilitante para la cesión de datos y no se requiere del consentimiento de los interesados

Asimismo, en la R/0209/2015, conoció de un caso en el que la Fábrica Nacional de Moneda y Timbre se negó a entregar la información en la falta de consentimiento de los interesados, así como en la publicación de los datos en la memoria anual de la institución, el CTBG señaló que la LTAIBG es título habilitante para la cesión de datos sin el consentimiento previo de los interesados, salvo con las excepciones previstas por ley, de forma que no resulta necesario el consentimiento para publicar o conceder acceso a las retribuciones de los altos cargos. Asimismo, en línea con la resolución anteriormente mencionada, refuerza la base de que en el caso de personal directivo prevalece el interés general sobre la protección de datos y menciona que el interés de los ciudadanos de conocer las retribuciones de los empleados públicos forma parte de su derecho a conocer el funcionamiento de las instituciones y el modo en que estas emplean los recursos.

c) Concepto “altos cargos y personal directivo” refiere a funciones y no a una denominación únicamente formal

Por su parte, la R/0423/2015 resolvió de la denegación por parte de Ingeniería y Economía del Transporte (INECO) de conceder el acceso a información sobre 19 miembros del equipo directivo que aparecían como tales en la página web de la institución, con base en que el único alto cargo de la compañía es el presidente y su información aparecía ya publicada en el sitio web. En esta ocasión, el CTBG entendió que también constituye personal directivo, aquel personal que por su calificación como

tal, desempeña funciones de responsabilidad en la organización. Por lo tanto, no sólo debe suministrarse información sobre el alto cargo –presidente- sino sobre todo aquel personal que desempeñe funciones de responsabilidad en la organización. Esto conecta, además, con su tesis de que existe un interés público de los ciudadanos en conocer las retribuciones de los empleados de sociedades mercantiles que ocupan puestos directivos, pues esto es parte del derecho a conocer el funcionamiento de las instituciones y la forma en que se emplea el erario público. Esta posición fue ratificada por medio de la sentencia 138/2016, de 17 de octubre, del Juzgado Central Contencioso Administrativo *núm.* 10 de Madrid, quien confirma que tal y como lo dispuso el CTBG, las personas respecto de las cuales se solicita información, están incluidas en el concepto de personal directivo, en el tanto son trabajadores que tienen la facultad de ejercer poderes inherentes a la titularidad jurídica de la empresa, con autonomía y responsabilidad que sólo se ve limitada por los criterios o instrucciones de los órganos superiores de gobierno y administración de la entidad. Menciona que lo relevante en el caso concreto es que los salarios tanto del presidente como del personal directivo constituyen información en el sentido del artículo 13 de la LTAIBG y resulta necesaria para que el solicitante y los ciudadanos puedan conocer cómo se manejan los fondos públicos de INECO.

Bajo este mismo argumento, en la R/0463/2015 estimó una reclamación por un supuesto similar contra ENAIRE, que ante la solicitud de un organigrama con las retribuciones del personal directivo, únicamente facilitó al solicitante de acceso un organigrama en el que no constan los nombres del personal directivo y que además dio como respuesta que el único cargo directivo era el puesto de Director General.

d) Acceso a información sobre retribución de asesores y puestos de confianza

Por su parte, en la R/0170/2016, el CTBG consideró que cabía la reclamación ante la negativa del Ministerio de la Presidencia de suministrar de forma completa la información sobre la retribución de las personas que hubieran desempeñado el puesto de asesor con carácter general. Dispuso en esa ocasión que la identificación y retribuciones de los funcionarios de carácter eventual en los Gabinetes de los Ministros y los Secretarios de Estado, en el tanto son puestos de confianza, reviste un interés general en conocer sus retribuciones. Anota que deben facilitarse los datos teniendo en consideración lo dispuesto en los criterios interpretativos conjuntos emitidos con la AEPD y ya anteriormente mencionados.

e) Improcedencia de acceso a la información de retribuciones en casos en que no existe relación laboral pese a que el pago se haya hecho con fondos públicos

No obstante el amplio acceso que se ha concedido, el CTBG desestimó una solicitud de acceso a la información dirigida a Corporación de Radio y Televisión Española (CRTVE) a sobre la cantidad de dinero percibida por los presentadores de la emisión de las campanadas para el año 2015. En esta ocasión, el CTBG estima que el dinero que percibieron los presentadores no corresponde a una relación laboral[333] directa con CRTVE, por lo que no existe un interés superior en la divulgación de la información frente al perjuicio que puede causarse a los interesados. Estima que en este caso, no existe un interés superior que justifique la divulgación de la información frente al perjuicio que puede derivarse para los interesados, y bajo este supuesto, no existe una norma con rango de ley o consentimiento, para poder ceder tales datos a un tercero. Considera que no existe un interés público o privado que permita dar acceso a la información con el único fin de conocer el salario de los presentadores, por lo que la solicitud de acceso planteada no resulta amparable en lo dispuesto por la LTAIBG.

f) Acceso a información de retribuciones de abogados sustitutos nombrados por períodos cortos de tiempo

Por último, en la R/0267/2016 conoció de un caso en el que se reclamaba la decisión del Ministerio de Justicia de conceder acceso a información sobre la retribución percibida por un funcionario de una empresa pública que actuó por un corto periodo de tiempo determinado como abogado sustituto. En esta ocasión, el CTBG consideró que el funcionario sobre el que se solicitaba la información no ocupaba un puesto de especial confianza o alto nivel y que excepcionalmente había ejercido el puesto de Abogado del Estado. Bajo esa lógica, indica que el nombramiento de dicho funcionario se hizo en condiciones específicamente reguladas y que además debe contar con un informe favorable de sus responsables y conceder el acceso a la información sobre la retribución

[333] Esta posible exclusión ya había sido avisada por SÁNCHEZ DE DIEGO y la crítica formulada al carácter netamente administrativista del que se dotó al derecho de acceso a la información, cuando menciona que: "esta vinculación al Derecho Administrativo Genera una situación grotesca en cuanto que la información relativa a los funcionarios públicos se rige por el Derecho Administrativo, pero para el personal contratado, el derecho que se aplica es el Derecho Laboral. Esto significaría que la obligación de informar se extiende a los funcionarios pero no respecto al personal con una relación laboral. Incomprensible y absurdo". Ver en Sánchez de Diego Fernández de la Riva, M. (2014) Transparencia y acceso a la información… *op. cit.* pp. 30-55.

no contribuye a lograr el objetivo que persigue la LTAIBG ni ayuda a conocer o controlar la toma de decisiones dentro del Ministerio de Justicia.

4. Tabla de casos resueltos

A continuación se presenta una tabla con la totalidad de los casos analizados para este trabajo junto con una descripción y la resolución que dio el CTBG a los mismos.

Resolución	Objeto	Fundamentos jurídicos
R/0026/2015 y R/0071/2015, de 9 de septiembre	Denegación de acceso parcial por parte de Confederación Hidrográfica del Ebro a una solicitud de acceso del reclamante sobre un certificado de reversión de una finca así como copia de un plano de expropiación de una finca urbana. La empresa concede el acceso a la información pero deniega el acceso a los títulos de propiedad otorgados en su día al Obispado de Barbastro y al Ayuntamiento Ainsa-Sobrabe por considerar que contienen datos de carácter personal cuyo contenido está anotado en el Registro de la Propiedad y que son difícilmente disociables.	De conformidad con la LOPD y el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD, la información que afecta a organismos públicos o a entidades o personas jurídicas de cualquier tipo no está amparada por la normativa de protección de datos. (FJ 4) El titular de las fincas es un Ayuntamiento o un Obispado según lo manifiesta la propia Administración, por lo que la información a ellos referida no encuentra amparo en la normativa de protección de datos de carácter personal. (FJ 4)
R/0080/2016, de 25 de junio[334]	Negativa del Ministerio de Sanidad, Servicios Sociales e Igualdad de dar acceso a la Declaración de Intereses de los revisores externos del Plan Estratégico para el abordaje de la Hepatitis C en el Sistema Nacional de Salud. La negativa se fundamenta en que se indicó al reclamante que los revisores externos no tienen la obligación de realizar la firma de la Declaración de Conflictos de Intereses por no ser los responsables de la elaboración del Plan, así como que entregar copia de las Declaraciones sería contrario al artículo 7 de la LOPD y en todo caso hubiera requerido del consentimiento de los titulares.	La información que contiene la Declaración pública de conflicto de intereses y confidencialidad de la Agencia Española de Medicamentos y Productos Sanitarios (AEMPS) contiene únicamente datos identificativos de la persona, los de su empresa y correo electrónico, así como datos sobre las actividades privadas que puedan suponer un conflicto de intereses. Ninguno de ellos puede ser considerado como dato especialmente protegido. (FJ 7) En relación con los datos personales que contiene, procede la aplicación del artículo 15.3 de la LTAIBG. La información que contiene la declaración de intereses, en especial si se ha desarrollado alguna actividad que pueda entrar en conflicto con su rol de revisores externos dentro de uno de los comités de la AEMPS es relevante para alcanzar el objetivo de la transparencia que persigue la LTAIBG. Conocer si existen eventuales conflictos de intereses entre los encargados de realizar un Plan Estratégico en el campo de la Sanidad y evitar que dicha planificación obedezca a fines diferentes al interés público, es el objetivo que persigue la Ley de Transparencia. Existe un interés

[334] En similar sentido ver: R/0225/2016.

		público en conocer la información denegada. (FJ 8)
R/0087/2015, de 1 de julio	Denegación de acceso parcial por parte de la Sociedad de Salvamento y Seguridad Marítima (SASEMAR) a la solicitud del reclamante sobre las retribuciones del Director, Director Adjunto de Administración y Recursos Humanos, Director Adjunto de Operaciones y de los Jefes de SASEMAR. La empresa concede el acceso a la información relativa a la retribución anual de los directores de SASEMAR. Deniega la información relativa a las retribuciones de los jefes de servicio, pues estima que son datos de carácter personal cuya revelación resulta de escasa relevancia para la consecución del objetivo de la transparencia.	La información solicitada por el reclamante es relativa a retribuciones percibidas por el Director adjunto de Administración y Recursos Humanos y por el Director Adjunto de Operaciones. Al ser puestos de alto nivel en la jerarquía del organismo, prima e interés público sobre la privacidad y corresponde facilitar el acceso a las retribuciones percibidas (sueldo bruto y trienios). (FJ 6) En relación con la información solicitada sobre los jefes de servicio, en aplicación de los criterios de ponderación, la misma debe proporcionarse de forma desagregada o anonimizada de forma que no permita la identificación inequívoca de los titulares de los datos. (FJ 6)
R/0099/2015, de 6 de julio	Negativa de la Secretaría de Estado de Cultura (SEC) de dar acceso en soporte digital a los Planes Operativos Anuales (POA) de los años 2012 a 2015 según solicitud de acceso de la reclamante. La SEC justifica la negativa de brindar la información en la imposibilidad de disociar los datos personales que contiene debido a su volumen. En razón de lo anterior, la información sólo puede ser puesta a disposición en sus dependencias.	Tanto como si la información es puesta a disposición de la reclamante en las dependencias de la SEC como si le es entregada en forma digital, debe velarse por la protección de los datos personales. Por lo tanto la disociación de datos personales, en caso de proceder, tendría que hacerse con independencia de si es puesta a disposición o entregada en soporte digital. (FJ 3.b) Los datos de carácter personal que contiene la información solicitada (nombre, apellido y cargo) son meramente identificativos e indican el responsable de cada una de las medidas contenidas en el POA. Esta identificación personal está vinculada con la actividad pública del órgano y con la responsabilidad en el ejercicio del cargo de los titulares de los datos. Prevalece el acceso a la información sobre la protección de datos, en el tanto la información es meramente identificativa, relacionada con las funciones encomendadas al titular de la información y resulta patente el interés público en conocer la información de forma que permita su estudio, análisis y comparación. (FJ 3.c)
R/0109/2015, de 8 de julio	Acceso parcial por parte de la Secretaría General de Instituciones Penitenciarias (SGIIPP) a la información solicitada por el reclamante sobre el módulo de productividad abonado por la SGIIPP a los Directores y Subdirectores de los distintos centros penitenciarios, las gratificaciones por servicios extraordinarios abonados por la SGIIPP a dicho personal así como las indemnizaciones por razón de servicio previstas en el Real Decreto 462/2002	Si bien parece que en el caso concreto procede aplicar la ponderación del artículo 15.3, lo cierto es que procede la aplicación del artículo 15.4 en el tanto la SGIIPP puede facilitar la información solicitada anonimizando o disociando los datos de carácter personal. (FJ 4) Así por ejemplo, se puede utilizar la opción dada por el reclamante quien pide que no se indique el nombre y apellidos del titular, sino que se consigne director 1, director 2 (…) (FJ 5)

	de 24 de mayo, todas las anteriores de forma individualizada. El SGIIPP concedió el acceso a la información pero no de forma individualizada por considerar que ello vulnera el derecho a la protección de datos.	Dado que el reclamante no tiene interés particular en conocer la identidad de los altos cargos receptores de las retribuciones y que ha propuesto un sistema de acceso a la información alternativo que no identifica a los titulares de los datos, procede la estimación de la reclamación (FJ 6)
R/110/2015, de 13 de julio	Acceso parcial por parte de la Entidad Estatal Trabajo Penitenciario y Formación para el Empleo (EETPFE) a la información solicitada por el reclamante sobre parte de las retribuciones del personal directivo y nombrado mediante el sistema de libre designación, en concreto las gratificaciones extraordinarias y el complemento de productividad abonado en 2008-2014. EETPFE concede el acceso a la información sobre el módulo de productividad del personal directivo pero indica que no se puede dar información sobre el personal designado por procedimiento de libre designación ya que vulnera el derecho a la protección de datos personales.	La información solicitada en el tanto se refiere a retribuciones percibidas de forma individualizada, podría permitir la identificación de una persona (dato personal), por lo que procede la aplicación del artículo 15 LTAIBG. (FJ 3) En el caso concreto, la información puede proporcionarse al solicitante de forma que no ocasiones perjuicio a los datos personales de los afectados mediante la disociación de los datos. (FJ 4) En el tanto el reclamante no tiene un interés particular en conocer la identidad de los funcionarios ni del personal directivo de los receptores de las retribuciones y ha propuesto un sistema de acceso a la información alternativo (sustitución de nombres y apellidos), procede estimar la reclamación. (FJ 5)
R/209/2015, de 25 de septiembre	Denegación de la Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda (FNMT) de una solicitud de acceso a la información de los salarios de 41 altos cargos de la Casa de la Moneda, que se encuentran fuera del Convenio Colectivo, donde sí se publican los salarios del resto de los trabajadores. La FNMT fundamenta su denegación en la falta de consentimiento a la divulgación de los datos personales solicitados (art. 19.3 LTAIBG). Ante la interposición de la reclamación, la FNMT dio acceso al importe total de la retribución de los 41 directivos, dato publicado en la Memoria Anual de 2014.	El artículo 8.1.f) de la LTAIBG prevé la publicidad de las retribuciones de los altos cargos y máximos responsables de las entidades. En ese sentido, de conformidad con el artículo 11 de la LOPD, no resulta necesario el consentimiento de los interesados para publicar las retribuciones de los altos cargos. Respecto de los funcionarios que no tengan consideración de altos cargos, aplica lo dispuesto en el artículo 15 de la LTAIBG. (FJ 3) Aplicados los criterios objetivos del artículo 15.4 de la LTAIBG y los criterios interpretativos conjuntos del CTBG y la AEPD, concluye que en el caso concreto, en el tanto se trata de datos sobre personal directivo, prevalece el interés general sobre la protección de datos, ya que el interés de los ciudadanos en conocer las retribuciones de los empleados públicos que ocupan dichos cargos está directamente relacionado con el derecho a conocer el funcionamientos de las instituciones públicas y el modo en que se emplean los recursos. (FJ 5). Procede la entrega de los salarios individualizados de los 41 altos cargos fuera del Convenio Colectivo de la FNMT en cómputo anual y en términos íntegros, sin incluir deducciones ni conceptos retributivos. (FJ 7)

		En relación con la información sobre los nuevos contratos de los 5 Directores Generales, debe concederse el acceso a la información relativa a la gestión administrativa con repercusión económica o presupuestaria, como por ejemplo, el objeto, su duración y su importe en cómputo anual y en términos íntegros, sin incluir deducciones ni desglose de conceptos retributivos. (FJ 6)
R/0250/2015, de 22 de octubre[335]	Denegación parcial de Confederación Hidrográfica del Miño – SIL de una solicitud de información sobre las cantidades percibidas por los funcionarios por concepto de productividad. Confederación Hidrográfica del Miño denegó parcialmente el acceso a la información argumentando que entregar los datos de forma individualizada vulneraría el derecho a la protección de datos personales. En aplicación de los criterios interpretativos del CTBG y la AEPD, facilita la información individualizada sobre los funcionarios elegidos por libre designación superior a nivel 28, especificando nombre y apellidos, cargo y productividad anual, así como la información no individualizada por Unidad, respecto del personal que trabaja en la Presidencia, la Comisaría de Aguas, la Dirección Técnica, la Oficina de Planificación Hidrológica y la Secretaría General, indicando el número de personas y la productividad anual total. Deniega el acceso a la información del resto de los funcionarios.	De conformidad con lo dispuesto en el Criterio interpretativo CI/0001/2015, de 24 de junio, cuando la información sobre la productividad incluya la identificación de todos o alguno de sus perceptores, procede la ponderación del artículo 15.3 de la LTAIBG. Los criterios interpretativos son orientaciones para realizar la ponderación que exige el artículo 15 LTAIBG y no pueden tomarse como una conclusión directa que no tenga en cuenta las circunstancias que no pudieran estar presentes en cada caso concreto. (FJ 3) Así como se proporcionó la información desagregada de los ocupantes de puestos de libre designación distintos al nivel 28, 29 y 30, pudo proporcionarse la información del resto de los puestos ocupados por concurso sin identificar al perceptor de la productividad. De forma tal que se hubiera garantizado la protección de los datos personales así como el derecho del solicitante de acceder a la información pública. El Criterio interpretativo señala que cunado la información de la productividad no incluya la identificación de los perceptores, debe facilitarse con carácter general. (FJ 3)
R/0214/2015, de 7 de octubre[336]	Denegación de acceso parcial por parte del Ministerio de la Presidencia a la información solicitada por el reclamante en relación con el expediente de elaboración de la LTAIBG. El Ministerio de la Presidencia concede acceso a una cantidad significativa de documentos. En relación con el acceso	El límite previsto en el artículo 15 de la LTAIBG, según la LOPD y el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD, protege únicamente los datos personales de las personas físicas. En ese sentido, las personas jurídicas (empresas, asociaciones, organismos, etc.) que hubieran participado en el proceso de consulta pública

[335] Adicional a esta reclamación, se presentaron otras reclamaciones contra Confederación Hidrográfica del Miño – SIL por la misma denegación de acceso parcial a la información percibida por los funcionarios por concepto de productividad. El CTGB se pronunció en idénticos términos en las resoluciones R/0251/2015, R/0252/2015, R/0263/2015, R/0264/2015, R/0265/2015, R/0266/2015, R/0267/2015, R/0268/2015, R/0269/2015, R/0270/2015 y R/0275/201. Asimismo, en relación con este tema y en un sentido similar puede verse la R/0093/2016.

[336] En similar sentido puede verse la resolución R/0491/2015 de 10 de marzo de 2016, en la que se concedió acceso a información con la que se elaboró el Real Decreto 900/2016 de 9 de octubre por el que se regulan las condiciones administrativas, técnicas y económicas de las modalidades de suministro de energía eléctrica con autoconsumo y de producción de autoconsumo.

	a la información del proceso de consulta pública, únicamente se remitió al reclamante el informe elaborado sobre la misma. Fundamenta la negativa en que el Gobierno garantizó que se mantendría el secreto de la correspondencia y anonimato de los datos personales de los participantes. Con base en lo anterior y con la consideración de que los ciudadanos que participaron voluntariamente en el proceso de consulta pública autorizaron la difusión de sus datos y aportaciones, el Gobierno decidió que la documentación que debía acompañar al proyecto de Ley, además de los dictámenes preceptivos y las memorias, era un informe resumen sobre el proceso de consulta. Consideran que dar acceso a las observaciones remitidas por distintos interesados (ciudadanos, sociedad civil y otros organismos públicos y privados) resulta contrario al derecho a la protección de datos personales.	están fuera de la excepción contenida en el artículo 15 LTAIBG. (FJ 4) Hecha la ponderación que exige el artículo 15.3 de la LTAIBG en relación con los datos de las personas físicas que participaron en el proceso de consulta pública, se concluye que la identidad de los participantes no contribuye al objetivo de la transparencia perseguido. No procede la comunicación de tales datos de los participantes ya que puede suponer una vulneración a la LOPD. (FJ 4) En el caso concreto, el derecho a la protección de datos tutela la identificación de la persona física que ha hecho la aportación, mas no el contenido de la misma. La denegación del acceso a un contenido determinado que fue expresado de forma voluntaria en un proceso de consulta pública, no puede ampararse en la normativa de protección de datos. (FJ 5) El objetivo de la consulta no era otro que elaborar un texto de la forma más participativa posible y esa participación es relevante no sólo para los redactores del proyecto, sino para otros ciudadanos interesados en conocer los aspectos principales sobre los que giró el debate y la consulta desarrollada. (FJ 5) Procede conceder el acceso a la información solicitada previa eliminación de los datos personales de los participantes de forma que se impida la identificación de las personas físicas (artículo 15.4 LTAIBG). (FJ 6 y 7)
R/0258/2015, de 6 de noviembre	Negativa del Ministerio del Interior de dar acceso al reclamante a una denuncia administrativa presentada ante la Inspección de Personal y Servicios de Seguridad (IPSS). La negativa de dar acceso a la información se basa en el carácter repetitivo y abusivo de la solicitud.	Al margen de la argumentación sobre el motivo de rechazo indicado por el Ministerio del Interior, el CTGB se pronuncia sobre los límites contenidos en los artículos 14 y 15 de la LTAIBG. Existiendo la posibilidad de que existan datos especialmente protegidos en el expediente al que se solicita acceso, pues se trata de datos relativos a la comisión de infracciones administrativas de un miembro de las FFCC de Seguridad y no existiendo consentimiento expreso del mismo ni Ley que permita el acceso al expediente por parte de terceros distintos de los interesados, la aplicación del límite previsto en el artículo 15.2 de la LTAIBG. (FJ 6)
R/0296/2015, de 15 de diciembre	Denegación del MINHAP de dar acceso al reclamante a un expediente sancionador. El reclamante solicita con base en una noticia publicada en un diario, se le dé acceso y copia del expediente sancionador incoado por la Dirección General de Coordinación de	No procede la denegación con base en el artículo 15 de la LTAIBG en el tanto la información se refiere a personas jurídicas y está fuera del ámbito de protección de la LOPD que aplica únicamente a personas físicas. La infracción contenida en el expediente sancionador que se pretende

	la Administración Periférica del Estado a la empresa SACYR al poder constituir los hechos que se denunciaban una infracción grave a la Ley de Seguridad Privada y la de Protección de la Seguridad Ciudadana. El MINHAP deniega el acceso a la información con base en el artículo 15.1 de la LTAIBG, ya que consultada la empresa, no otorgó el consentimiento informado para la cesión de datos que se refieren a infracciones penales o administrativas.	acceder fue supuestamente cometida por SACYR, que es una persona jurídica. (FJ 3) Las infracciones graves a las que se refieren la Ley de Seguridad Privada y la de Protección de la Seguridad Ciudadana están vinculadas directamente con la forma en que las empresas de seguridad prestan sus servicios. Esta información puede entenderse forma parte de la estrategia económica o comercial de la empresa y su divulgación a terceros puede poner en riesgo los intereses comerciales y económicos. Por esta razón, aplican los límites establecidos en el artículo 14.h) y j) de la LTAIBG. (FJ 4) El concepto "podrán" incluido en el artículo 14.1 de la LTAIBG implica que los límites contenidos en dicho numeral no aplican de forma directa. La invocación de estos motivos debe estar ligada con la protección concreta de un interés racional y legítimo. Su aplicación no es automática y requiere de un test del daño, que analice si el supuesto perjuicio es concreto, definido y evaluable. Asimismo, debe ser aplicado de forma justificada y proporcional, atendiendo al caso concreto y siempre que no exista un interés que justifique la publicidad o el acceso. (FJ 5) La información a la que pretende acceder el reclamante –copia de la resolución del expediente sancionador- contiene información sensible para la empresa cuyo conocimiento o divulgación puede suponer un perjuicio real y previsible, por lo que procede desestimarse la reclamación en aplicación del artículo 14.h) y j) de la LTAIBG. (FJ 5) En el caso concreto el objetivo de la transparencia se ve garantizado en razón de la publicidad de la sanción que eventualmente pueda imponer la AEPD a la empresa. (FJ 5)
R/0312/2015, de 2 de diciembre	Denegación de la solicitud del reclamante que tenía como fin conocer, en relación con ciertas plazas vacantes ofertadas por Servicios y Estudios para la Navegación Aérea y la Seguridad Aeronáutica (SENASA), los criterios de valoración aplicados a las convocatorias en que se presentó como candidato, la relación de candidatos participantes en las convocatorias, la relación de admitidos y excluidos con las respectivas puntuaciones, las causas concretas de la desestimaciones de sus candidaturas y la composición de los tribunales en cada caso.	La relación de personas físicas que solicita el reclamante es meramente identificativa por lo que procede la ponderación establecida en el artículo 15.3 de la LTGAIB. (FJ 5) La información solicitada por el reclamante, si bien es sobre datos meramente identificativos de las personas que participaron los tres concursos en que participó, se refiere a candidatos o participantes cuya incorporación a la sociedad mercantil estatal no ha sido confirmada. Es decir, que no es una información vinculada a la organización de la entidad, pues los datos que solicita no son de personas incorporadas a la entidad, ya que el

	SENASA negó el acceso a la información por cuanto se refiere a datos personales de otros candidatos. Asimismo, que no se ha impedido el acceso a la información pública del reclamante, quien ha podido conocer las desestimaciones de sus candidaturas y las causas a través del correo electrónico que facilitó para tales efectos.	proceso no culminó con la incorporación a la planilla de todos los participantes. De forma que la información únicamente puede facilitarse de manera anonimizada o disociad, informando sólo el número de candidatos que concurrieron a las pruebas de selección en que participó el reclamante así como el número de admitidos y excluidos, sin que sea necesario identificarlas de forma inequívoca. (FJ 5). En relación con la solicitud de información sobre los integrantes de los tribunales, no basta con la indicación de los Departamentos o Unidades encargados de seleccionar personal, sino que debe indicarse con claridad la composición de los tribunales, si existiesen, en cada convocatoria en que participó el reclamante.
R/0327/2015, de 11 de diciembre	Denegación de acceso parcial por parte del Ministerio de Sanidad, Servicios Sociales e Igualdad a una solicitud de acceso a información sobre el detalle de los inmuebles decomisados, provincia por provincia, entre 1995 y 2014, el precio de la adjudicación en subasta y su fecha de adjudicación, así como la persona física o jurídica a la que se hubiera adjudicado cada inmueble. El Ministerio de Sanidad concede el acceso a la información sobre el detalle de los inmuebles decomisados y el precio de adjudicación de subasta. No obstante, niega el acceso a la información sobre la persona física o jurídica adjudicataria por considerar que ello vulnera el derecho a la protección de datos personales, no reviste ninguna relevancia pública, es un dato que revela la situación personal del adjudicatario. Además señala dar acceso a esta información requiere de un proceso manual previo y complejo de reelaboración de la información.	Identificar a las personas físicas o jurídicas (a través de sus representantes) que hayan sido adjudicatarios de cada inmueble no se enmarca dentro del interés público en la divulgación de la información que recoge la LTAIBG. (FJ 3) Aún y cuando exista un interés privado del reclamante en conocer la identidad de los beneficiarios del Fondo de Bienes Decomisados, resulta de un interés público superior mantener en el anonimato a dichas personas, tanto físicas como jurídicas, con el fin de impedir que la revelación de sus identidades perjudique el buen desarrollo del Fondo y su innegable labor social en la lucha contra el narcotráfico y la reinserción social y laboral de toxicómanos. (FJ 3) El Pliego de condiciones para la enajenación de bienes muebles, mediante subasta pública, que convoca la Delegación del Gobierno para el Plan Nacional sobre Drogas incluye una cláusula de confidencialidad de los datos personales y de todo tipo a los que se pudiese acceder por la participación en dicho procedimiento, lo que impide a la Administración a otorgar la información solicitada. (FJ 3)
R/0328/2015, de 9 de diciembre	Denegación de la solicitud del reclamante que tiene por objeto obtener copia de los expedientes de reconocimiento de servicios previos por trabajos de funcionarios en RENFE, al amparo de la Ley 70/1978, de 26 de diciembre, de reconocimiento de servicios previos en la Administración Pública. El MINHAP deniega la solicitud de información por considerar que no es el	Pese a que la cuestión no es planteada por ninguna de las partes, el CTBG hace especial pronunciamiento sobre el artículo 15 LTAIBG. Teniendo en cuenta que lo solicitado son los expedientes de reconocimiento de servicios previos de funcionarios que trabajan en RENFE, que contienen datos de carácter personal, procede a aplicación de lo dispuesto en el artículo 15.3 de la LTAIBG. Hecha la ponderación que exige dicho artículo, se

	órgano competente y que no tiene en su poder la información solicitada.	concluye que la información solicitada es relevante a efectos de conocer los criterios que han sido aplicados a la hora de reconocer los servicios prestados, y por lo tanto, para evitar discrecionalidades y situaciones de desigualdad en dichos reconocimientos. (FJ 6) Este objetivo se puede alcanzar sin necesidad de proporcionar información de carácter personal, facilitando al reclamante la información solicitada previa disociación de los datos personales. Deben proporcionarse sólo los elementos que permitan identificar el criterio seguido por el organismo en el reconocimiento de dichos servicios previos. (FJ 6)
R/0381/2015, de 13 de enero de 2016	Denegación de acceso parcial por parte del Ministerio del Interior a una solicitud del reclamante por medio de la que pedía todos los documentos asociados a su prueba de entrevista personal y la revisión de la misma (resultados del test de personalidad, biodata, desarrollo de la entrevista valoración, etc.), copia de los acuerdos del Tribunal de Selección por los que se determinan los criterios a valorar en la entrevista y los requisitos para superarlos, criterios del test de personalidad y guion semiestructurado correspondiente a la entrevista personal. El Ministerio de Interior concede el acceso a la información de los documentos solicitados. Deniega el acceso a los documentos de trabajo de los entrevistadores, por cuanto considera que tienen carácter auxiliar o de apoyo. Limita la posibilidad de obtener copia de la documentación técnica de las pruebas psicotécnicas ya que considera que se está bajo el supuesto del artículo 14.1.K de la LTAIBG, que permite la limitación del derecho con el objetivo de garantizar la confidencialidad en el proceso de toma de decisión.	La documentación generada por los entrevistadores y con base en la cual el Tribunal va a adoptar su decisión es determinante en el proceso y, por ende, no puede calificarse de auxiliar o apoyo. Este tipo de información tiene una incidencia directa y es determinante en la decisión final adoptada. (FJ 3) La Administración no justifica la aplicación del límite contenido en el artículo 14.1.K LTAIBG. No demuestra como facilitar el acceso a la información de la propia entrevista personal y revisión de la misma puede perjudicar el proceso de toma de decisión, sobre todo cuando en el caso concreto ya ha sido adoptada la decisión final. (FJ 4) Las Bases de la convocatoria aplicables al caso concreto disponen que para garantizar la confidencialidad e igualdad, las pruebas de ortografía, conocimientos, lengua extranjera y psicotécnica, se corrigen y califican mediante un sistema que impide la identificación personal de los admitidos. Por esta razón no puede alegarse la confidencialidad como motivo para limitar el acceso y más si se tiene en consideración que el sistema protege los datos personales de los participantes frente a una injerencia de terceros. Se considera que las pruebas médicas y psicofísicas gozan de esta confidencialidad por ser datos especialmente protegidos que quedan al margen del conocimiento de terceros (FJ 4)
R/0393/2015, de 4 de febrero de 2016[337]	Denegación de acceso parcial por parte del Ministerio del Interior a la solicitud de información sobre el listado de reuniones del Ministro del Interior	La calificación de la agenda oficial que hace el Ministerio del Interior como aquella que afecta las responsabilidades oficiales del cargo de Ministro, se contradice con la

[337] El CTBG ha reiterado esta posición en las resoluciones R/0397/2015, R/0398/2015, R/0404/2015, R/0410/2015, R/0415/2015, R/0416/2015, R/0424/2015, R/0425/2015, en las que concedió el acceso a las

	durante la legislatura, con indicación de la fecha, persona o entidad con que se reunió lugar y asunto que se trató. El Ministerio del Interior deniega parcialmente la solicitud de acceso con base en que la agenda oficial del Ministro de Interior dispone de una parte pública y de otra no pública. La parte pública se puede consultar en la página web o a través de las notas de presa. La parte no pública de la agencia oficial no es de conocimiento general por considerarse que su difusión no es necesaria, oportuna o conveniente.	afirmación subsiguiente de que tiene una parte no pública cuya difusión no se hace por razones de necesidad, oportunidad o conveniencia. Siendo que la agenda es el reflejo del desempeño de las funciones del alto cargo, debe ser pública en la mayor extensión posible, salvo que aplique alguno de los límites previstos en la Ley (FJ 3) Está fuera de toda duda la capacidad de las agendas oficiales de informar a los ciudadanos y de posibilitar el ejercicio de un control de la actividad pública. (FJ 4) Si se analizan las agendas oficiales, lo que se informa es sólo excepcional, extrayendo del conocimiento de los ciudadanos lo referente al proceso ordinario de toma de decisiones y responsabilidad de los funcionarios. Si bien es cierto la LTAIBG exige la rendición de cuentas del dinero público, la rendición de cuentas del tiempo público es también un derecho esencial de la transparencia (FJ 6) No hay duda de que el acceso a la información puede afectar datos de carácter personal. La protección que da la LOPD alcanza únicamente a personas físicas, quedando excluidas del ámbito de aplicación personas jurídicas. (FJ 8) La información que se recoja en las agendas debe evitar incluir datos personales de personas físicas que no representen a empresas, organizaciones o administraciones y entidades públicas y privadas. De existir dichos datos personales, debe sustraerse de la información que se otorgue al interesado, haciéndoselo saber. (FJ 9.b)
R/0407/2015, de 28 de enero de 2016	El reclamante solicita al Ministerio de Educación Cultura y Deporte (MEDC) acceso a la base de datos anonimizada con los estudiantes universitarios que han sido beneficiarios de una beca en la convocatoria 2014-2015, de acuerdo con la información que publica el MEDC en su página web. Solicita para cada registro de becario la siguiente información sin nombre ni identificación del beneficiario: sexo, universidad en que ha matriculado, área o rama de estudios universitarios, estudios universitarios específicos del	La LOPD define los datos de carácter personal como cualquier información concerniente a personas físicas identificadas o identificables. No sólo datos claramente identificativos de una persona física como el nombre y apellidos son datos personales. Por ejemplo, ser el único beneficiario de una beca para cursar un Máster con un número reducido de alumnos, permite la identificación de la persona física y conocer información relativa a su situación socioeconómica. (FJ 4)

agendas oficiales del Ministro de Empleo y Seguridad Social, Ministro de Asuntos Exteriores y de Cooperación, Ministerio de Defensa, Ministro de Fomento, Ministro de Educación, Cultura y Deporte, Ministro de Industria, Energía y Turismo, Ministro de Agricultura, Alimentación y Medio Ambiente y del Ministro de Justicia. También puede verse la resolución R/0069/2016 en la que el reclamante solicita acceso a la agenda del Ministerio de la Presidencia en relación con las reuniones celebradas dentro del marco de aprobación de un proyecto de ley.

	becario, cuantía variable a percibir, cuantía variable mínima y nota media, renta per cápita del becario, entre otros. El MECD considera que si bien se ha solicitado la información de forma anonimizada, a través de ciertos datos de carácter personal (rentas, patrimonio familiar, expediente académico) puede identificarse al becario en concreto. Hecha la ponderación que exige el artículo 15.3 de la LTAIBG, estima que no corresponde dar acceso a la base de datos anonimizada. Entiende que debe darse por satisfecha la solicitud del reclamante con la información que oportunamente le facilitó.	Atendiendo a la definición de datos de carácter personal, sí es posible suministrar alguna información cuando haya sido desagregada, con porcentajes y a efectos estadísticos, sin perjuicio del derecho a la protección de datos personales, como por ejemplo: sexo (porcentaje de hombres y mujeres), universidad en la que se ha matriculado (identificación, en porcentaje respecto del total, de las universidades con beneficiarios de becas), área o rama de los estudios universitarios (identificación, en porcentaje del total, de los estudios universitarios con beneficiarios de becas), medias de las notas media de los beneficiarios, renta per cápita media. (FJ 5)
R/0409/2015	El reclamante solicitó a la Casa Real información sobre el gasto total de la recepción en el Palacio de Oriente tras el desfile de las Fuerzas Armadas en el Día de la Hispanidad, desglosado por los diferentes conceptos como personal, catering, etc. Asimismo, solicitó la lista de los asistentes e invitados. El reclamante acusa que pese a que solicitó la lista completa de los invitados y asistentes a la actividad, la Secretaría General de la Presidencia del Gobierno se limitó a indicar que entre los asistentes se encontraban personas pertenecientes al Gobierno de la Nación, Congreso de los Diputados, Senado, Tribunal Constitucional, Consejo General del Poder Judicial, Tribunal Supremo, Comunidades Autónomas, ex presidentes del Gobierno, Consejo de Estado, Tribunal de Cuentas, Fiscalía General del Estado, Defensora del Pueblo, Secretaría General Iberoamericana, cuerpo diplomático, así como personas de diferentes sectores sociales de la vida pública española.	En relación con el listado completo de asistentes, no puede desconocerse que es acorde con el espíritu de la norma el conocer el perfil institucional o social de los asistentes a la recepción por la que se conmemora la Fiesta Nacional. Se entiende que la respuesta a la solicitud del reclamante, indicando la procedencia general de los asistentes, es acorde al objetivo que persigue la LTAIBG. Por el contrario, conocer el listado completo de asistentes, incluidos los acompañantes, excede el concepto de actividades sujetas a Derecho Administrativo que, según el legislador, actúa como límite a la aplicación de la LTAIBG a la Casa Real. (FJ 4)
R/0418/2015, de 21 de enero de 2016	Denegación de acceso parcial por parte del Ministerio de Economía y Competitividad (MINECO) a la solicitud del reclamante que tenía por objeto acceder a la memoria científica que se acompañó a la solicitud del proyecto "Oportunidades del cine español en Internet", 2013. Asimismo, de una serie de investigaciones de las que identifica el investigador, solicitó: título, referencia del número del proyecto y convocatoria, boletín o medio en que se publicó la resolución, nombre del investigador principal,	Los datos de contacto de los investigadores principales de los proyectos a los que se solicita el acceso, son datos de carácter meramente identificativo relacionados con la organización, funcionamiento y actividad pública del órgano. No obstante lo anterior, toda vez que los titulares de los datos no están vinculados al MINECO, deben solicitarse directamente a la universidad a la que pertenece el investigador, quien deberá suministrarla en los términos del artículo 15.2 de la LTAIBG. (FJ 5)

	universidad y facultad a la que pertenece, así como teléfono, dirección o e-mail de contacto en la universidad, resumen del proyecto y memoria científica, así como la cantidad concedida y estado del proyecto de investigación. Se concede el acceso parcial a la información. El MINECO considera que no es procedente suministrar el teléfono, dirección o e-mail de contacto del investigador principal por tratarse de datos protegidos por la LOPD y además son datos que debe solicitarlos directamente a la universidad o institución a la que pertenece el investigador.	
R/0423/2015, de 21 de enero de 2016[338]	Denegación de acceso por parte de Ingeniería y Economía del Transporte S.A. (INECO) a una solicitud de información relativa a las retribuciones percibidas por los miembros del equipo directivo (19 personas en total que aparecían como tales en la página web de la entidad). Fundamenta la negativa en que de conformidad con la Ley 5/2006, de 10 de abril, el único alto cargo y que es el máximo responsable de la compañía es el presidente, cuyas retribuciones de conformidad con la LTAIBG son publicadas en el sitio web.	Aplicados los criterios objetivos de ponderación del artículo 15.3 de la LTAIBG así como el Criterio interpretativo conjunto del CTBG y la AEPD, el CTBG concluye que la solicitud del reclamante es sobre las retribuciones del equipo directivo de INECO, en el entendido de que se trata de personal, que por su calificación de directivo, desempeña funciones de responsabilidad en la organización. En ese sentido, prevalece el interés general sobre el interés individual, ya que existe un interés de los ciudadanos en conocer las retribuciones de los empleados de sociedades mercantiles que ocupan puestos directivos, lo que conecta con su derecho a conocer el funcionamiento de las instituciones y la forma en que emplean los recursos públicos. Se obliga a INECO a suministrar la información solicitada por el reclamante. (FJ 5)
R/0429/2015, de 15 de febrero de 2016[339]	Denegación de acceso parcial por parte del Ministerio de Defensa a la solicitud del reclamante de un listado de los pasajeros que han acompañado a las autoridades transportadas por la flota del Grupo 45 de la Fuera Aérea Española u otras unidades que han transportado autoridades españolas, con desglose de las fechas de vuelo, ciudad o aeropuerto, origen y destino, desde el año 1976 o el primer año disponible. El Ministerio de Defensa alega que la información sobre la ejecución de los vuelos cuando se trata de la Presidencia o Casa Real es clasificada, así como que el hecho de que el personal transportado sean representantes	El Grupo 45 de la Fuerza Aérea Española se dedica exclusivamente a misiones de transporte de autoridades. Esto permite concluir que una solicitud de datos meramente identificativos dirigidos a conocer información sobre las personas que han sido transportadas por dicho Grupo entra dentro de su actividad pública, y por lo tanto, se encuadra en lo previsto en el artículo 15.2 de la LTAIBG (FJ 5) La información solicitada puede contener al menos dos tipos de datos personales relativos a autoridades y sus acompañantes. Respecto de los primeros, sus datos personales deben considerarse relacionados con la organización del órgano o entidad en el que prestan sus servicios. En relación con los acompañantes, debe considerarse que su

[338] Ver en similar sentido: R/0288/2016.

[339] En relación con este tema se presentó otra reclamación que dio origen a la R/0409/2016, que se suspendió hasta que se resolviera en vía judicial el recurso interpuesto por el Ministerio de Defensa.

	públicos de primer orden y de que el gasto sea sufragado con fondos públicos, no implica la prevalencia del interés público sobre la divulgación de los datos.	actividad está enmarcada en el funcionamiento del organismo o entidad púbica, por lo que su identidad no tiene razón de quedar excluida del conocimiento de terceros. (FJ 5) La información tiene relevancia en el tanto permite el control de los desplazamientos y que los mismos no se efectúen al margen de actos o reuniones que deban efectuarse en el desempeño público de los cargos. (FJ 5)
R/0433/2015, de 15 de febrero de 2016	Denegación de acceso parcial por parte de ENAIRE a una solicitud de acceso a una nota técnica con identificación y firma del autor. ENAIRE facilita el acceso al a información pero deniega el acceso al nombre y firma de su autor.	Si bien el nombre y apellidos del autor de una nota técnica constituyen datos meramente identificativos, en el caso concreto no pueden ser subsumidos en los supuestos del artículo 15.2 LTAIBG en el tanto dicha información incide más allá de la organización, funcionamiento o actividad pública del órgano. El conocimiento del autor de una nota técnica no tiene incidencia pública desde el momento en que el contenido de la misma es asumido por ENAIRE. Las conclusiones a las que llegó el autor han sido respaldadas por ENAIRE, ya que es en ellas en que ha basado la respuesta al solicitante. Esta condición hace que la identidad del autor inicial de la información carezca de relevancia pública para estos efectos. (FJ 3)
R/0463/2015, de 3 de febrero de 2016	Denegación de acceso parcial por parte de ENAIRE a la solicitud del reclamante sobre el organigrama y las retribuciones de los directores en 2014. ENAIRE da acceso a un organigrama en el que no constan los nombres de los responsables. Señala que de conformidad con la LTAIBG el único alto cargo es el puesto de Director General, que al no estar cubierto en el 2014, no tuvo retribución alguna.	El reclamante solicita información sobre las retribuciones de los directores (personal directivo) de ENAIRE, en el entendido de que se trata de personal que, por su consideración de directivo, desempeña funciones de responsabilidad en la organización. En estos casos prevalece el interés general sobre el interés individual. El interés de los ciudadanos en conocer las retribuciones de los empleados de una entidad pública conecta con su derecho a conocer el funcionamiento de las instituciones y la gestión de los recursos públicos. (FJ 6) Debe proporcionarse la información relativa a la identidad y retribuciones de todos los directores de ENAIRE salvo que existan causas suficientemente justificadas que lo impidan, como por ejemplo, que se configure uno de los límites al derecho de acceso o que las plazas no hayan sido cubiertas. (FJ 7)
R/0466/2015, de 25 de febrero de 2016	Denegación de acceso a una solicitud del reclamante de una copia de una resolución dictada por la interposición de un recurso de reposición en un proceso de nacionalidad por residencia ante la Dirección General de los Registros y del Notariado (DGRN). El reclamante solicita la información con los datos personales suprimidos y únicamente sobre los fundamentos y la resolución final.	El documento que solicita el reclamante contiene al menos el nombre y apellidos de una persona a la que se le concede la nacionalidad por residencia, así como datos asociados a su personalidad que no son especialmente protegidos ya que no se refieren a ideología, afiliación sindical, religión, creencias, origen racial, salud, vida sexual o comisión de infracciones penales o administrativas. Si bien el expediente puede llegar a contener los antecedentes penales del

	La DGRN niega el acceso con base en la aplicación del artículo 15.2 y 15.3 de la LTAIBG, en el tanto la información solicitada se refiere a un expediente de nacionalidad de otra persona. Para la formación del expediente de nacionalidad, se requiere la aportación de una serie de documentos que contienen datos personales como partida de nacimiento, certificación de antecedentes penales, etc. Debe prevalecer el derecho a la intimidad sobre el de acceso a la información.	solicitante, en el caso específico el reclamante no solicitaba acceso al expediente sino únicamente a una copia de la resolución final. (FJ 3) Si la Administración proporciona al reclamante copia de la resolución de manera disociada o anonimizada quedaría eliminada la información de carácter personal y no sería de aplicación el límite a la protección de datos en el caso concreto. No obstante, el reclamante identifica exactamente el expediente en el que fue presentado el recurso de reposición al que solicita acceso, la fecha de interposición del recurso y su fecha de resolución. Esto permite entender, o al menos suponer, que el reclamante conoce tanto detalle del expediente que conoce a la persona que lo interpuso, por lo que disociar los datos no cumpliría con su función de impedir que se conozca la identidad de la persona a la que se refiere el documento. El acceso a la información no salvaguarda el derecho a la protección de datos y por ende debe desestimarse la reclamación. (FJ 4) La obligación de transparencia la cumple la DGRN por medio de los boletines de carácter mensual que contienen información de las resoluciones dictadas (FJ 5)
R/0489/2015, de 1 de marzo de 2016	Denegación de acceso parcial por parte de la entidad pública empresarial RED.ES, a la solicitud de información del recurrente sobre las resoluciones dictadas en procedimientos de cancelación de dominios y que contenga el nombre del dominio afectado por la cancelación. La Denegación parcial de RED.ES es en cuanto al nombre del dominio afectado en cada resolución.	Los nombres de dominio contienen información de personas físicas identificadas o identificables y de personas jurídicas. Respecto de las primeras, la información a la que solicita acceso el reclamante tiene condición de dato de carácter personal por lo que procede la aplicación del artículo 15 de la LTAIBG. (FJ 4) El conocimiento de los criterios jurídicos aplicados por RED.ES en sus resoluciones de cancelación de dominio es lo que resulta relevante a efectos de garantizar la transparencia en la actuación de dicho organismo. Conocer el titular de un dominio que ha sido cancelado puede conllevar a una vulneración del derecho a la protección de datos y no aporta información adicional de relevancia a efectos de la LTAIBG. (FJ 5)
R/0490/2015, de 29 de febrero de 2016	El reclamante solicita al Ministerio de Interior se le dé acceso a la información sobre el contenido del historial profesional de las propuestas de ingreso en la Orden del Mérito Policial con distintivo rojo, de los funcionarios del Cuerpo Nacional de Policía y personas ajenas a él, con el fin de conocer cuáles han sido los méritos acreditados de los condecorados respecto de la legislación que contiene estos reconocimientos.	A juicio del CTBG, transmitir la información sobre la identidad de los condecorados y los méritos que le son atribuidos puede poner en riesgo la propia identidad personal y el buen término de las operaciones que se están llevando acabo y en el marco de las cuales se haya accedido a la condecoración. (FJ 5) El riego previsible y no hipotético así como el ámbito de discrecionalidad para conceder las condecoraciones mencionadas, lleva a

	El Ministerio del Interior niega el acceso a la información al amparo del art. 15.3 de la LTAIBG en el tanto la información solicitada por el reclamante contiene datos de carácter personal.	considerar al CTBG que aplica el límite previsto en el artículo 15 de la LTAIBG. (FJ 5)
R/0005/2016, de 29 de marzo	Denegación de acceso por parte del MINHAP a la copia del expediente administrativo y de la documentación de un candidato aspirante a las plazas de un concurso específico del Ministerio de Hacienda y Administraciones Públicas, así como a las puntuaciones obtenidas tanto por su persona como por otro candidato, los puntos de valoración de los méritos específicos y la motivación en la valoración. El MINHAP concede el acceso a una parte de la información pero niega la copia de la documentación aportada por el resto de aspirantes en el tanto contiene datos de carácter personal.	Hecha la ponderación que exige el artículo 15.3 LTAIBG, la Administración debe proporcionar a la interesada el acceso a aquella información relevante del proceso selectivo que le permita comprobar la limpieza e imparcialidad del procedimiento en el que concurren, incluidos los datos de carácter personal de terceros también participantes en el mismo proceso selectivo con los que el solicitante compite por las mismas plazas. (FJ 5)
R/0013/2016, de 30 de marzo	El reclamante solicita acceso en formato digital a la copia completa del expediente sancionador abierto a Barclays Bank, S.A. por la Comisión Nacional del Mercado de Valores, por la que se sancionó a dicha entidad por una infracción muy grave y que dio lugar a una publicación en el BOE. La Comisión Nacional del Mercado de Valores (CNMV) deniega el acceso a la información por considerar que se encuentra dentro de los supuestos de los límites al acceso contenidos en los artículos 14 y 15 de la LTAIBG.	El artículo 15 LTAIBG no resulta de aplicación en el caso concreto en el tanto se trata de información relativa a una persona jurídica y tanto la LOPD como la LTAIBG tutelan la protección de los datos de carácter personal de las personas físicas. (FJ 3) En caso de que dentro de la información solicitada existiese información de carácter personal en los expedientes, podría procederse a la anonimización o disociación de datos, de forma que se impida la identificación de las personas físicas afectadas. (FJ 3)
R/0023/2016, de 7 de abril	Denegación por parte de la Agencia Nacional de Evaluación de la Calidad y Acreditación (ANECA) a la solicitud del recurrente de acceso a los nombres y apellidos de los expertos que emitieron el informe correspondiente, o que intervienen en la actualidad, en las evaluaciones de la ANECA en las que ha participado. La ANECA justifica la denegación en el perjuicio para la garantía o el secreto requerido en procesos de toma de decisión que implicaría conceder el acceso a dicha información.	La información de los expertos permanece desconocida con vistas a garantizar una adecuada independencia y libertad Si bien en el caso concreto se solicita acceso a los datos de la identidad de los expertos a posteriori, es decir, una vez que el procedimiento de acreditación ya ha finalizado, la denegación o no de la información podría vincular futuros procedimientos, ya que cambiaría el marco conforme al cual se elaboran los informes los expertos. Si bien el acceso tendría un impacto más moderado una vez concluido y que los datos forman parte de un listado publicado en el sitio web de ANECA, una cesión de la información personal, que vincule los datos con su participación en un procedimiento de evaluación, resulta contrario a la normativa de protección de datos (SAN de 30 de junio de 2011 sobre comunicación de datos de

		expertos a concursantes de una convocatoria pública). (FJ 3)
R/0049/2016, de 3 de mayo	El reclamante solicita a la Autoridad Portuaria de la Bahía de Algeciras, copia de las resoluciones de Puertos del Estado, remitidas a esa autoridad, sobre reconocimiento de perfil competencial a libertados sindicales. La Agencia Portuaria manifiesta que no puede conceder acceso a dicha información, pues contiene datos de carácter personal.	El dato referente al nombre y apellidos de los liberados sindicales, constituye un dato especialmente protegido según el artículo 7 de la LOPD, en el tanto se refiere a la condición de afiliación sindical de una persona. El acceso a la información de estos datos únicamente puede concederse con su consentimiento o cuando conste que el titular haya hecho manifiestamente público el dato, elementos que no concurren en el caso concreto. No obstante lo anterior, el artículo 15.4 de la LTAIBG permite la disociación o anonimización de los datos personales, por lo que la Administración puede suministrar copia de las resoluciones eliminando el nombre y apellidos del titular así como el nombre del Sindicato al que pertenece. Ello permitiría cumplir el objetivo de la transparencia sin vulnerar el derecho a la protección de datos. (FJ 5)
R/0050/2016, de 26 de abril[340]	El reclamante solicita a CRTVE información sobre la cantidad de dinero percibida por los presentadores de la emisión de las campanadas en 2015. CRTVE considera que la solicitud de acceso debe ser inadmitida por concurrir la causa de solicitudes manifiestamente repetitivas o que tengan un carácter abusivo no justificado con la finalidad de transparencia de la LTAIBG.	En el caso concreto, si bien no existen datos especialmente protegidos ni datos meramente identificativos relacionados con el órgano o entidad correspondiente, los datos solicitados se incardinan en la esfera íntima y personal de los titulares de los datos. El dinero percibido por los presentadores no se enmarca en una relación labora directa con CRTVE. Procede realizar la ponderación que exige el artículo 15.3 LTAIBG. (FJ 4) No existe un interés superior que justifique la divulgación de la información frente al perjuicio que puede derivarse para los interesados. La cesión de datos de terceros debe estar permitida en una norma con rango de ley o tener el consentimiento de los titulares, supuestos que no concurren en el caso particular. (FJ 5) Tampoco existe un interés público o privado superior que permita dar acceso a la información solicitada con el único fin de conocer el salario de los presentadores, no queda amparada por el objetivo de transparencia de la actuación pública en relación con otros derechos o intereses. Si se proporciona lo solicitado se traspasa la línea de la privacidad y el daño a dicha esfera es irreparable. (FJ 5)
R/0051/2016, de 4 de mayo	Denegación de acceso parcial de la solicitud del reclamante a la información sobre declaración de actividades a la toma de posesión, declaración de bienes a bienes a la toma	Coincide el CTBG con la Administración, que argumentó que una cosa es una eventual variación patrimonial de los Altos cargos y otra acceder a sus declaraciones patrimoniales, fuera de su esfera laboral o

[340] Ver en similar sentido: R/0290/2016

	de posesión y declaraciones anuales para los años 2012, 2013 y 2014 del Presidente del Gobierno y sus ministros. La Oficina de Conflictos de Intereses de la Secretaría de Estado de Administraciones Públicas del MINHAP concede parcialmente el acceso a la información, argumentando que las declaraciones anuales y declaraciones de bienes patrimoniales tienen carácter reservado según la Ley 3/2015 de 30 de marzo, reguladora del ejercicio del Alto cargo de la Administración General del Estado. Asimismo, acusa que ello supondría una vulneración al derecho a la protección de datos de los interesados.	profesional, que contienen datos de localización e identificación de los bienes inmuebles, así como a los datos del ISR de las personas físicas, que no sólo contienen información sobre os rendimientos del Alto cargo, sino que además afectan a datos especialmente protegidos como la orientación sexual (en el supuesto de matrimonio con una persona del mismo sexo), la ideología (si el alto cargo contribuye a organizaciones políticas), la religión (si el declarante opta por contribuir a la Iglesia Católica), la salud (del Alto cargo y de sus descendientes, si estos tienen una discapacidad) y los datos identificativos de su cónyuge y descendientes. (FJ 4) Concluye que en este caso existen datos de carácter personal que tienen consideración de especialmente protegidos y que se incardinan en la esfera íntima, personal y familiar de los titulares de los datos, por lo que no puede divulgarse esa información sin atender a los requisitos previstos en la norma. (FJ 4)
R/0075/2016, de 17 de mayo de 2016[341]	El reclamante solicita al MINHAP acceso a la información sobre la relación de abogados del Estado en activo que tienen autorización de la Oficina de Conflictos de Intereses del MINHAP para realizar actividades en el sector privado. Asimismo solicita se indique el puesto, actividades para las que tiene concedida la compatibilidad, fecha en que se concedió y la empresa privada en que realiza las funciones. El MINHAP hace entrega parcial de la información: no obstante, deniega los datos nominativos bajo el argumento de que hecha la ponderación que exige el artículo 15.3 de la LTAIBG, no procede conceder el acceso.	El CTBG reitera su criterio sobre el acceso a la información de las autorizaciones de compatibilidad de los empleados públicos. La finalidad perseguida con la divulgación de la información –el conocimiento público de que un determinado funcionario o empleado ha sido expresamente autorizado a realizar una actividad particular- solo se realiza en la práctica si se hace pública la identidad de éste, por lo que no puede presuponerse una limitación absoluta de la información por causa de la protección de datos. (FJ 4)
R/0091/2016, de 10 de junio de 2016[342]	El reclamante solicita un listado de los viajes del Ministro de Asuntos Exteriores con detalle de la fecha de ida, de vuelta, el destino, acompañantes, agenda completa de visita, reuniones, personas con quien se reunión, motivo de la reunión, contenido de las conversación, acuerdos, compromisos o convenios adoptados o firmados, a excepción de aquellos, que por limitaciones de la LTAIBG o seguridad nacional no puedan ser entregados.	El CTBG considera que las reuniones celebradas en el marco de la actividad profesional desarrollada por los responsables públicos puede afectar la esencia de la LTAIBG y que, por lo tanto, constituye información pública según el artículo 13. Por ende, es necesario definir y regular la necesidad de recoger la participación en reuniones afectadas por la Ley de Transparencia para formular además una obligación y un compromiso de rendición de cuentas. (FJ 4)

[341] Ver en términos similares: R/0067/2016 y R/0099/2016.

[342] En ese mismo sentido ver: R/0120/2016, R/0121/2016, R/0122/2016, R/0123/2016, R/0124/2016, R/0125/2016, R/0126/2016, R/0127/2016, R/0128/2016, R/0129/2016, R/0130/2016, R/0131/2016 R/0139/2016, R/0140/2016, R/0143/2016, R/0143/2016, R/0154/2016, R/0155/2016.

	El Ministerio de Asuntos Exteriores concede acceso a la información que está contenida en la página web, sin perjuicio de indicar que desde la entrada en vigencia de la LTAIBG se encuentra trabajando en ampliar las categorías de información que se muestran en el portal. El reclamante entiende que esto no satisface su solicitud.	Debe tenerse en cuenta el hecho de que entre la información solicitada se encuentren los datos de personas que hayan podido asistir a reuniones y que se encuentran protegidas por la LOPD. Al no haberse recabado inicialmente el consentimiento del titular de los datos para la cesión de la información, el acceso a la misma debe resolverse no sólo de acuerdo con el artículo 15 de la LTAIBG, sino también, con los criterios y disposiciones en materia de protección de datos. Inclusive en el hipotético supuesto de que se hubieran, voluntariamente, guardado datos relativos a reuniones, el acceso a los mismos debería analizarse de acuerdo a las reglas que regulan la relación y el equilibrio entre el derecho de acceso a la información y a la protección de datos. (FJ 4) Indica que no es posible utilizar los datos que se recogen en los registros de entrada en los edificios como elementos susceptibles de confirmar visitas de trabajo ya que dichos ficheros se rigen por la LOPD y la instrucción 1/1196 de la AEPD, que indica que los datos obtenidos no podrán ser utilizados ni cedidos para otros fines distintos a la seguridad y control, salvo con el consentimiento del interesado, y deberán ser destruidos cuando haya transcurrido el plazo de un mes a partir del momento en que fueron recabados. (FJ 4). Señala que el CTBG ha respaldado en varias ocasiones solicitudes de acceso a la información que se interesaban por conocer las reuniones mantenidas por los responsables públicos; no obstante señala que se entiende las dificultades que supone proporcionar información que no ha sido organizada, clasificada o sistematizada de tal forma que pueda ser proporcionada en los términos que se solicita. (FJ 6) Conscientes de esas dificultades, el CTBG considera delimitar cuanto antes lo que debe ser considerado una agenda para la transparencia, que se defina la información que debe incorporarse los eventuales límites y que se comprometa a los responsables públicos a proporcionar, de manera clara, sistemática y actualizada, información sobre la actividad que desarrollan en su desempeño público. Para estos efectos, el CTBG se encuentra trabajando con los actores implicados, en la definición de un modelo de agenda para la transparencia con la que se cumpla el mandato del legislador que reconoce a los ciudadanos el derecho de conocer cómo se toman las decisiones que les afectan, cómo se manejan los fondos públicos

		o bajo qué condiciones actúan las instituciones. Se desestima la reclamación. (FJ 6)
R/0165/2016, de 8 de julio de 2016	El reclamante solicita al Ministerio de Agricultura, Alimentación y Medio Ambiente, acceso en modalidad presencial a los méritos generales y específicos alegados y a sus correspondientes medios de acreditación aportados, de todos los candidatos que presentaron solicitud de participación para un determinado puesto. El Ministerio de Agricultura, Alimentación y Medio Ambiente considera que el concurso aún no se ha resuelto el concurso y que aplican los límites previstos en el artículo 18.1.a de la LTAIBG.	El acceso a los méritos aportados podrá limitarse en caso de que entre la información se encuentren datos especialmente protegidos de los previstos en el artículo 7 de la LOPD, para cuyo acceso será necesario el consentimiento del interesado o cuando, en virtud del tipo de datos que se aporten, deba realizarse una ponderación suficientemente justificada y proporcionada entre el derecho de acceder a la información y el derecho a la protección de datos. (FJ 6) Se estima por motivos formales la reclamación por incumplimiento de los plazos de respuesta (FJ 7)
R/0170/2016, de 14 de julio de 2016	El reclamante solicita al Ministerio de la Presidencia la relación de personas que ocupan o han ocupado un puesto de asesor con carácter eventual, no funcionarios y desempeñan esta función de asesoramiento o asistencia, identificando el servicio encomendado y las retribuciones anuales por ese concepto. El Ministerio de la Presidencia remite al reclamante a la web de transparencia y la categoría denominada Relaciones de Puesto de Trabajo. El reclamante acusa que la información del sitio web es incompleta y no incluye la información solicitada.	Aplicación del Criterio CI/001/2015 del CTBG y la AEPD. (FJ 6) Siendo que la solicitud se interesa por la identificación de los funcionarios de carácter eventual en los Gabinetes de los Ministros y los Secretarios de Estado, el CTBG considera que debe concederse el acceso a los nombres y apellidos de ese personal así como sus retribuciones. En el acceso deberán tenerse en cuenta las salvedades previstas en dicho criterio. (FJ 7)
R/0171/2016, de 13 de julio de 2016	Denegación de acceso parcial por parte del MAEC a la información sobre el número de pasaportes diplomáticos válidos, expedidos y caducados o que han perdido su validez en los años 2008 a 2015. Asimismo, solicita la relación de titulares de pasaportes con detalle de nombre y apellidos del titular, cargo del titular, fecha de expedición del pasaporte diplomático, fecha de renovación y fecha de pérdida de validez. El MAEC da acceso a un cuadro de pasaportes diplomáticos expedidos en los años de referencia así como los pasaportes caducados o que han perdido validez en esos años. En relación con la publicación exhaustiva de todas las personas que detentan un pasaporte diplomático, señala que aplicados los preceptos del artículo	Siendo que la cuestión de la reclamación se refiere al conocimiento de la identidad de titulares de pasaporte diplomático, el análisis debe realizarse teniendo en cuenta, entre otras, la aplicación del artículo 15 de la LTAIBG. (FJ 4) La identificación de quienes ocuparon los cargos mencionados en el artículo 3 del Real Decreto 1123/2008, de 4 de julio, sobre pasaportes diplomáticos, equivaldría al examen de cada uno de los expedientes sobre pasaportes concedidos de manera que se identificara el cargo con la persona que lo ocupaba en cada momento. Esto supone una elaboración expresa de la información, que está dentro de la exclusión de dar acceso según el artículo 18.1.c) de la LTAIBG. (FJ 4) Son titulares también del pasaporte diplomático los cónyuges de los cargos

	15.1 y 15.3, no procede hacer pública la relación de titulares de pasaportes diplomáticos.	anteriores, los hijos menores y otros miembros de la familia según determinadas circunstancias. Estas personas ostentan el pasaporte diplomático por sus lazos familiares con el titular. La previsión normativa en la que se fundamenta la concesión de ese pasaporte y la condición privada de esa categoría de titulares supone, a juicio del CTBG una vulneración del derecho a la protección de datos que no se ve justificada por lo previsto en la LTAIBG. (FJ 4) Se desestima la reclamación. (FJ 5)
R/0191/2016, de 22 de julio de 2016	El reclamante solicita al Instituto Nacional de la Seguridad Social (INSS) se facilite información sobre determinadas retribuciones del personal adscrito a la Dirección Provincial del INSS en Sevilla. El INSS únicamente facilita información sobre el Director Provincial. La Administración no responde en tiempo.	La Administración proporcionó al reclamante información únicamente sobre el Director Provisional del INSS en Sevilla, por lo que se trata de información incompleta. Falta, en caso de que hubiera puestos de dichas características información relativa a los puestos de nivel 29 y 28 –siempre que sean de libre designación- o equivalente, personal eventual de asesoramiento y especial de confianza, personal directivo y personal no directivo que ocupa puestos de nivel 30 de libre designación, vocales, asesores, asesores técnicos o equivalentes. Los conceptos sobre premios y cursos de todo el personal del INSS en Sevilla quedan al margen del Criterio interpretativo CI/001/2015 ya que no están reconocidas como derechos retributivos de los empleados públicos. (FJ 4)
R/0341/2016, de 20 de octubre de 2016	El reclamante solicita al MINHAP acceso a los nombres de los nueve altos cargos a los que la Oficina de Conflictos de Intereses ha incoado procedimiento sancionador. La Oficina de Conflictos de Intereses suministra únicamente información relativa a cinco funcionarios que han sido sancionados y cuya sanción ha sido publicada en el BOE.	De conformidad con lo dispuesto en el artículo 15.1 LTAIBG, únicamente debe suministrase los datos personales relativos a la comisión de una infracción administrativa sólo en aquellos casos en que conlleve la publicación de la sanción. (FJ 3 y4)
R/0250/2016, de 5 de septiembre de 2016	El reclamante solicita al Ministerio del Interior se dé acceso al número de funcionarios con prolongación o prórroga en servicio activo hasta los 70 años de edad, dependientes de la Secretaría de Instituciones Penitenciarias (SGIIPP), desglosados por cuerpos, puestos y centros de trabajo que hay actualmente. El Ministerio del Interior da información sobre el número de funcionarios sobre algunos centros penitenciarios; no obstante, siento que hay varios centros penitenciarios que únicamente cuentan con un funcionario, da un número global de	La información solicitada va más allá de información estrictamente relacionada con la organización, funcionamiento o actividad del órgano. (FJ 5) Informar sobre el Cuerpo al que pertenece o el puesto de trabajo que ocupa un funcionario en aquellos centros en los que él es el único destinado o no existe un número elevado de empleados en esa situación, permite identificar de manera inequívoca y sin esfuerzos desproporcionados a su titular, lo que puede incidir en su esfera personal. (FJ 5) La información facilitada cubre el interés alegado por el solicitante por lo que se desestima la reclamación. (FJ 6)

	estos (22 funcionarios en 22 centros penitenciarios).	
R/0258/2016, de 8 de septiembre de 2016	El reclamante solicita al Ministerio del Interior, qué personas habían sido nombradas comisionarios honorarios en la última legislatura. El Ministerio de Interior remite una resolución en la que indica que los Honorarios nombrados en la última legislatura son 148 personas pertenecientes a la Policía Nacional y 7 personas ajenas a la Policía Nacional.	La información a la que se refiere el solicitante en la reclamación (el nombre de las 7 personas nombradas Comisionarios Honorarios y que son ajenas al Cuerpo Nacional de Policía), debe señalarse que no son datos especialmente protegidos ni tampoco datos meramente identificativos relacionados con la organización, funcionamiento o actividad pública del órgano, pues se refieren a personas que no pertenecen al Cuerpo Nacional de Policía. (FJ 4) El perjuicio a la seguridad personal de los interesados que refiere el Ministerio del Interior, teniendo en cuenta que los méritos para el reconocimiento de Comisario Honorario se basan en la labor realizada a favor del cuerpo nacional de policía puede acreditarse en alguno de los casos afectados pero no en todos. En una búsqueda de internet puede encontrarse informaciones publicadas sobre personas reconocidas como Comisario Honorario y en los que no se ha considerado que dicha publicación afectase la seguridad. En todo caso, debe señalarse que la información solicitada tiene incidencia en el mecanismo de rendición de cuentas de la LTAIBG.(FJ 5) No cabe hacer consideraciones generales cuando se realiza la aplicación de los límites al derecho de acceso previstos en la LTAIBG. El Ministerio del Interior no ha realizado una adecuada ponderación en todos los casos y no ha procedido a la apertura de un trámite de alegaciones que hubiese permitido que los afectados alegasen lo que a su derecho consideran conveniente. Este trámite además de permitir obtener el consentimiento del interesado, permitiría analizar las circunstancias y ponderar adecuada y justificadamente, la incidencia de la solicitud de acceso en el derecho a la protección de datos. (FJ 6)
R/0267/2016, de 12 de septiembre de 2016	El reclamante solicita al Ministerio de Justicia información sobre la cantidad percibida, durante 2016, por un funcionario del grupo A2, destinado en el FOGASA de Teruel, que actuó como abogado sustituto. El Ministerio de Justicia deniega el acceso a la información bajo el argumento de que el funcionario no forma parte del RPT de la Abogacía	Aplicación del Criterio interpretativo CI/001/2015. El funcionario sobre el que se solicita la información no ocupa un puesto de especial confianza o alto nivel, puesto que se trata de un Nivel 26 que excepcionalmente ha ocupado el puesto de Abogado del Estado. Adicionalmente, debe tenerse en consideración que las condiciones para su nombramiento están específicamente

	General del Estado, sino que se encuentra adscrito a un plan extraordinario de actividad, así como que la información se refiere a retribuciones vinculadas a la productividad por objetivos o el rendimiento de un perceptor identificable.	reguladas y que debe contar con un informe favorable de sus responsables. Conocer la cuantía que ha cobrado un determinado funcionario en una fecha determinada y concreta no tiene como finalidad, a juicio del CTBG, poder controlar la acción pública ni conocer cómo se toman las decisiones en el Ministerio. Adicionalmente, las gratificaciones extraordinarias que ha percibido el funcionario van vinculadas al desempeño, concreto y objetivable de determinadas labores, por lo que excede la finalidad de la transparencia conceder el acceso a dicha información. (FJ 4)
R/0268/2016, de 13 de septiembre de 2016	El reclamante solicita al MINHAP acceso a la información sobre los expedientes de denegación de prolongación de permanencia de servicio activo de funcionarios de la Administración General del Estado. Solicita número de denegaciones fundamentadas por incumplimiento del procedimiento de la Resolución de 31 de diciembre de 1996, número de denegaciones motivadas por cuestiones de carácter personal o profesional, actitud inadecuada, así como número de denegaciones generadas por otros motivos con una breve descripción. El MINHAP facilita la cifra solicitada por el reclamante, pero no da acceso a los motivos de las denegaciones pues considera que es información que contiene datos de carácter personal.	Las motivaciones que pueden ser aducidas por la Administración como causa de denegación de una solicitud de prolongación del servicio activo, pueden basarse en circunstancias subjetivas aplicables a las circunstancias concretas del empleado público interesado. Ello no significa que pueda ser discrecional o carezca de control. (FJ 5) Conocer las razones que motivaron la denegación de las solicitudes de prolongación del servicio activo presentadas por dos empleados públicos, que, debido al conocimiento de la provincia en el que se encontraba su puesto de trabajo y teniendo en cuenta además que el número de funcionarios de la Administración General del Estado en los servicios periféricos es considerablemente inferior que en el caso de los servicios centrales, son identificables permitiría proporcional información de carácter personal, lo que supone una incidencia en su derecho a la protección de datos. (FJ 6)
R/0279/2016, de 16 de septiembre de 2016	El reclamante solicitó al Ministerio de Fomento acceso a los listados de productividad y gratificaciones correspondientes al año 2015, identificando la persona que los recibe, de las siguientes categorías: personal directivo, personal eventual, personal funcionario de libre designación y del resto del personal, se solicita el listado puesto a puesto sin identificación de la persona que lo ocupa.	Aplicación del Criterio Interpretativo conjunto CI/001/2015. Prima el interés público sobre los derechos a la intimidad o a la protección de datos en aquellos casos en que el acceso se refiere a información sobre la productividad percibida por cualquier empleado público que ocupa un puesto de especial confianza, un puesto de alto nivel en la jerarquía del órgano, organismo o entidad o un puesto que se provea mediante un procedimiento basado en la discrecionalidad. (FJ 7) Respeto del resto del personal funcionario que no ocupa tales puestos, la información que se solicita es la referida a puesto por puesto sin identificación de titulares, lo cual puede considerarse contradictorio, dado que comprobando esa información con la contenida en una Relación de Puestos de Trabajo, que posiblemente ya el interesado

		tiene en su poder, permite obtener fácilmente y sin esfuerzos desproporcionados una identificación final de cada funcionario perceptor, lo que sí vulneraría la normativa de protección de datos. Con el fin de encontrar un equilibrio entre esta información y los límites que impone el ordenamiento al acceso, si es posible incluir la denominación genérica de los puestos de trabajo y los niveles pero en ningún caso la identificación concreta del puesto ni la identificación personal de los perceptores. (FJ 8)
R/0296/2016, de 26 de septiembre de 2016.	El reclamante solicita al MAEC acceso a las actas de cada una de las sesiones de la Junta de la Carrera Diplomática celebradas desde septiembre de 2015 hasta la fecha más reciente disponible. El MAE deniega el acceso a la información, pues considera que de conformidad con el artículo 14.1.k) de la LTAIBG facilitar la misma afecta el proceso de toma de decisiones.	El acceso que solicita el reclamante puede incidir en datos especialmente protegidos, pues las actas pueden contener la valoración de determinados aspectos como infracciones administrativas de carácter sancionador. (FJ 4) Los datos contenidos en las actas constituyen un perfil laboral de cada uno de los funcionarios designados para asumir las tareas inherentes al puesto de trabajo por el que optan de manera que los datos no pueden ser disociados, pues se puede llegar a identificarlos de manera sencilla. (FJ 5)
R/0381/2016	El reclamante solicita al Ministerio de Industria, Energía y Turismo (MINETUR) acceso al expediente terminado relativo al reconocimiento de cualificación profesional para el ejercicio de Agente de la Propiedad Industrial, pruebas de acceso de las que formó parte. Entre la información solicitada se incluye la puntuación otorgada por cada miembro del tribunal a todos y cada uno de los candidatos por cada tema, pregunta, subpregunta, apartados o subapartados. El MINETUR le facilitó únicamente acceso a los datos que constan en su expediente.	Aplicación de Criterio Interpretativo CI/002/2015. No se está ante un supuesto de concurrencia competitiva. Debido a que en el caso concreto la puntación obtenida por los otros candidatos no tiene una incidencia directa en las posibilidades del interesado en el proceso de selección llevado a cabo, esta información no puede ser facilitada pues prevalece el derecho a la protección de datos. (FJ 4)
R/0397/2016, de 25 de noviembre de 2016	El reclamante solicita a la Fundación de Ferrocarriles Españoles (FFE) se dé acceso a los contrarios menores realizados por la institución, con las correspondientes facturas y la relación y contenido de todos los acuerdos marco suscritos entre la FFE y terceros. La FFE no da respuesta en tiempo.	Aplicación de Criterio Interpretativo CI/002/2015. La Fundación se encuentra dentro de los sujetos obligados por la LTAIBG a los principios de publicidad activa. Es decir, que está obligada a publicar sin necesidad de que nadie lo solicite, los contratos, convenios y acuerdos de los que forme parte. La propia norma legal obliga y respalda la publicación de los contratos menores. Debe entenderse que la cesión de estos datos está legamente amparada, conforme a lo dispuesto en el artículo 11 de la LOPD, pues está avalada la cesión por una norma con rango de ley. (FJ 5)
R/0369/2016, de 8 de	El reclamante solicita al Ministerio del Interior remita toda la información	Aplicación de Criterio Interpretativo CI/002/2015.

noviembre de 2016	relativa a expedientes sancionadores tramitados por la Administración General del Estado, en aplicación de la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana. Solicita la información desglosada por provincia y Comunidad Autónoma y que incluya los expedientes sancionadores tramitados desde julio de 2015 hasta la fecha más reciente. El Ministerio del Interior refiere al reclamante a varias páginas web en las que consta la información de criminalidad y seguridad ciudadana de los Anuarios Estadísticos.	El acceso al contenido de los expedientes sancionadores tramitados por la Administración General del Estado, en aplicación de la Ley Orgánica 04/2015 de 30 de marzo, de protección de la seguridad ciudadana, desglosados por provincia y Comunidad Autónoma, incide en los datos especialmente protegidos, tal y como se recoge en el Criterio precedente y no consta el consentimiento de los titulares de los datos ni norma que ampare esa cesión. (FJ 3)
R/0410/2016, de 15 de diciembre	El reclamante solicita al MINHAP acceso a las actas de las reuniones de la Comisión de Interpretación, Vigilancia, Estudio y Aplicación (CIVEA). El MINHAP deniega el acceso a la información, alegando entre otros, la existencia de datos especialmente protegidos y afectaciones al derecho a la protección de datos en caso de conceder el acceso a la información.	La Administración no aclara cuáles son los datos protegidos a los que se refiere. No obstante, del contenido de las órdenes del día que se publican en la página web se puede extraer que en las actas aparecen datos personales de trabajadores, acuerdos que afectan traslados específicos de trabajadores, suspensiones o creaciones de complementos singulares, modificaciones de encuadramientos específicos de determinados profesionales. (FJ 4) Aún y cuando el CTBG no ha podido comprobar cuáles son los datos protegidos a los que se refiere la Administración, los mismos no pueden ser facilitados salvo que medie consentimiento de los titulares. Siendo que no consta en el expediente dicho consentimiento, no puede proporcionarse esa información. (FJ 4) El resto de datos corresponden a supuestos específicos que afectan en exclusiva a determinados trabajadores de la Administración. Proporcionar esta información no contribuye en controlar el funcionamiento de la Administración, por lo que tampoco deben ser facilitados, ya que con la mera referencia a la adopción de un acuerdo y su contenido sobre ese aspecto se daría satisfacción al derecho de acceso. (FJ 4)
R/0421/2016, de 21 de diciembre	El reclamante solicitó al Ministerio de Defensa acceso a la información sobre qué personas civiles fueron invitadas por la Armada a la travesía del Buque-Escuela desde Marín a Cádiz. El Ministerio de Defensa facilitó información sobre el proceso de selección que lleva a cabo con el fin de determinar cuáles ciudadanos efectuarán el viaje en el Buque-Escuela. Considera que de conformidad	Aplica el Criterio CI/002/2015. No se puede proporcionar la identidad de las personas civiles sin que medie cuando menos autorización expresa por parte de las terceras personas afectadas. (FJ 4) Se requiere identificación de todos aquellos que no son militares, relacionados o no con la Armada y que iban embarcados en el Buque-Escuela Lo relevante en estos casos es conocer no la identidad de las personas

	con el artículo 15.3 de la LTAIBG, no procede dar información sobre la identificación, con nombres y apellidos de los pasajeros que hicieron el viaje.	concretas que iban en el embarque, puesto que se hace a título personal y lúdico, no oficial, sino qué criterio se sigue para seleccionarlas y ha sido puesto de manifiesto en las alegaciones. Procede la denegación de la información sobre la identidad de los civiles (FJ 4) Si bien conocer las personas que, previa solicitud voluntaria para participar en una travesía como la que trae causa de la solicitud, permite ejercer un control acerca del uso de bienes públicos, como sería en este caso el Buque-Escuela de la Armada, entiende el CTBG que dicha finalidad puede alcanzarse conociendo el número de participantes así como las condiciones en las que fueron seleccionados y los motivos para ello. Así, a nuestro juicio, se aporta transparencia al proceso, permitiendo su conocimiento por otros ciudadanos que eventualmente estuvieran interesados en participar en el mismo así como evitando un mal uso de los servicios públicos. (FJ 4)
R/0455/2016, de 17 de enero 2017	El reclamante solicita a la Subdelegación del Gobierno en Castellón acceso a la información relativa a las cantidades percibidas por concepto de productividad generadas por la participación del proceso electoral del 20 de diciembre de 2015 y 26 de junio de 2016. El reclamante no recibió la respuesta en tiempo.	Aplicación del Criterio interpretativo CI/001/2015. En el presente caso no se solicita identificación expresa de los empleados públicos que han recibido las gratificaciones extraordinarias por lo que se debe facilitar la cuantía global entregada por el organismo y el número de personas receptoras de las mismas. (FJ 4)
R/0541/2016, de 15 de marzo de 2017	El reclamante solicita a Corporación Radio Televisión Española (CRTVE) acceso a la información relativa a la retribución anual bruta percibida en 2015 y 2015 por el personal directivo de la corporación, según puesto en el organigrama. CRTVE inadmite la solicitud de información por entender que no se hizo a través de los cauces previstos por la ley, ya que se le dirigió la nota de forma directa y no a través del MINHAP.	El acceso a la información solicitada, relativa a retribuciones de personal directivo de una sociedad mercantil con participación 100% pública y financiada con cargo a los presupuestos generales del Estado, ha sido avalado tanto por criterios interpretativos, el CTBG, la AEPD y los Tribunales de Justicia, por lo que debe entregarse la información requerida. (FJ 10)

Recapitulación

El rol del CTBG en la interpretación de la excepción al acceso a la información pública supone sin duda alguna un aporte al tratamiento de la materia y otorga cierto grado de seguridad jurídica conforme vayan siendo reiteradas y cada vez más claras sus posiciones en temas que en alguno que otro caso han resultado recurrentes, como el relativo al acceso a los datos de la RPT de los organismos o entes que son sujetos pasivos de la LTAIBG.

En general, a nuestro criterio, el resultado en la aplicación de la LTAIBG ha sido positivo dentro del desbalanceado panorama en el que se encuentra el derecho de acceso a la información frente a la protección de datos personales. En la mayoría de casos en que la norma y la ponderación lo permite, se ha decantado hacia el acceso a la información pública, como es natural –lo contrario sucede en los casos que se verá más adelante que ha resuelto la AEPD, en los que naturalmente hay una predilección hacia el derecho a la protección de datos personales-.

Resulta relevante la uniformidad de criterio que hay en determinadas materias como por ejemplo, el acceso a las retribuciones de altos cargos, en las que se han emitido inclusive criterios de interpretación conjunta por parte de la AEPD y el CTBG. En estos casos la línea es clara respecto de cuál información es accesible y cuál se entrega previa disociación de datos personales y existe, en beneficio de la transparencia, una interpretación amplia del concepto de alto cargo que más que un concepto formalista el CTBG lo ha visto como un concepto material, de forma que alto cargo no es sólo el que defina la ley, sino el que desarrolle tales labores, aun cuando la estructura y la normativa le otorguen un nombre distinto.

También ha perfilado ya una línea clara respecto de la interpretación del concepto de datos meramente identificativos y ha señalado la necesaria vinculación de estos al funcionamiento o actividad del órgano al que pertenece la persona cuyos datos se pretende acceder.

En muchos casos, ha encontrado que la disociación de datos personales constituye un balance para concederé el derecho de acceso a la información sin necesidad de generar un perjuicio directo en el derecho a la protección de datos

personales. Si lo que se pretende es ejercer un control objetivo sobre la actuación de un órgano público, este parece ser un buen parámetro pues por un lado no se impide el ejercicio del derecho de acceso y por otro tampoco se vulnera el derecho a la protección de datos personales.

No obstante lo anterior, ello se complica cuando el control que se desea hacer en aras de la transparencia, la buena gestión pública y la rendición de cuentas depende de conocer el dato subjetivo, sea la persona, en una situación concreta, como ha ocurrido con el caso de las condecoraciones policiales, en las que si bien el CTBG tenía una posición de negar el acceso a la información sobre las personas que recibían dichos méritos, a nivel judicial se ha determinado que sí interesa para la consecución del objetivo que persigue la LTAIBG, conocer los nombres y apellidos de las personas a las que les fueron otorgados dichos méritos.

Si bien se coincide con la mayoría de sus posturas, cabe llamar la atención sobre algunos supuestos en los que el CTBG ha entendido que prevalece la protección de datos personales frente al acceso a la información o casos en los que ha tenido un cambio de criterio que resulta difícil de comprender.

Nos referimos a los supuestos en que ha negado el acceso a información sobre acompañantes de autoridades oficiales en vuelos del Grupo 45 de la Fuerza Aérea Española –en que se negó el acceso a los datos de los acompañantes-, información sobre pasaportes diplomáticos –en el que entendió que únicamente procedía el acceso a la información del funcionario público que ostenta el pasaporte diplomático pero no así respecto de sus familiares a los que se extiende el beneficio-, acceso a la declaración patrimonial de los altos cargos –por cuanto entiende que puede tener información sensible y de terceros que no son el alto cargo-, acceso a la información sobre el pago a personal que no tiene una relación laboral –pese a que el pago haya sido hecho con fondos públicos-, pues en todos ellos es clara la notoria relevancia pública que tiene la información, aún y cuando no pertenezca al titular de los datos. En un ejercicio de ponderación, perfectamente se pudo haber inclinado la balanza hacía el derecho de acceso a la información, pues aun tratándose de datos de terceros, un adecuado control y conocimiento de la función pública alcanza a esta información. Resulta innegable, por ejemplo, la trascendencia pública de conocer quién acompaña al

presidente de gobierno en los viajes que realiza en el Grupo 45 de la Fuerza Aérea, o las rentas patrimoniales de los altos cargos.

El segundo supuesto al que nos referimos es al imprevisible, cuando no difícil cambio de criterio del CTBG en relación con el tema de agenda pública y acceso a datos sobre reuniones de altos cargos, porque partió en sus inicios de una determinación clara en el camino de que ante la ausencia de una ley se debía entregar toda la información disponible y cambio su criterio al punto de indicar que hasta que no exista una ley que defina "agenda pública" y la información que debe contener esta, el ciudadano tendrá que darse por satisfecho con la información que las autoridades públicas digan que disponen y que ya ha sido publicada en los respectivos sitios web.

Capítulo X. La aplicación de los criterios de conciliación por parte de la Agencia Española de Protección de Datos

SUMARIO: 1. Cuestiones preliminares. 2. La aplicación de los criterios de conciliación por parte de la AEPD. 3. Informes jurídicos. A. Informe 0390/2013, sobre transmisión de datos identificativos del titular de una licencia municipal de obras a terceros. B. Informe 0178/2014, relacionado con la aplicación de la LTAIBG y su conciliación con la LOPD. C. Informe 0502/2014, sobre inclusión de firmas manuscritas en documentos escaneados. Informe 12155/2016, relativo al acceso a la información sobre personas que ocupan cada plaza de la RPT. D. Informe 0160/2016, sobre aplicación de la LOPD a tratamiento posterior de datos obtenidos por medio de solicitudes de acceso a la información. 4. Resolución de denuncias. A. Datos especialmente protegidos. B. Publicidad activa de ayudas y beneficios públicos. C. Publicidad activa del DNI. D. Publicaciones de datos consignados en actas o sesiones por parte de los Ayuntamientos. E. Retribuciones. F. Libertad de Expresión. G. Divulgación en Internet de identidad de trabajadores en procesos de licitación.

1. Cuestiones preliminares

La labor de la AEPD en lo que se refiere al a interpretación, aplicación y vigencia de la LOPD y el derecho a la protección de datos personales ha sido esencial y ha contribuido a una sólida garantía de este derecho.

El modelo que el legislador español ha optado seguir para la tutela de la transparencia y el derecho de acceso a la información, ha sido confiado en principio al CTBG, pero tiene un punto de encuentro con las facultades y competencias de la AEPD cuando se trata de la interpretación y aplicación de la LTAIBG a información que contiene datos de carácter personal, más específicamente.

En este Capítulo, pretende exponerse el abordaje que ha hecho la AEPD de las obligaciones de transparencia y acceso a la información después de promulgada la LTAIBG. Para ello, se han tomado en consideración las resoluciones e informes jurídicos publicados a abril de 2017 en la página web de la AEPD bajo el descriptor "Ley 19/2013", consultables en la página de la AEPD[343].

2. La aplicación de los criterios de conciliación por parte de la AEPD

No hay duda que la mayoría de disposiciones de la LTAIBG corresponde su aplicación y control al CTBG. No obstante, el panorama no resulta del todo claro cuando se trata de la aplicación de la normativa de protección de datos, pues dada la escogencia

[343] Disponible en: www.agpd.es

del legislador español[344], ha quedado en la práctica un sistema dual con competencias tanto de la AEPD como del CTBG en lo que se refiere a la interpretación de la relación entre transparencia y protección de datos personales.

Por un lado, si se examina desde la óptica del CTBG, en el tanto el artículo 15 que contiene la excepción a la publicidad y el acceso a los documentos en razón de la protección de datos personales, su aplicación y correcta interpretación sería resorte de su competencia. No obstante, si analizamos que la cesión de datos que se lleve a cabo en virtud del ejercicio de derechos conferidos en la LTAIBG requiere necesariamente la aplicación de la LOPD y sus principios, también tiene amplia competencia para conocer de su aplicación la AEPD, la cual como se verá aplica de forma estricta, como corresponde, los principios y derechos de la LOPD[345].

Bajo esta óptica, han sido ya un número considerable los casos por medio de los cuales la AEPD se ha encargado de dilucidar el conflicto entre transparencia y protección de datos personales[346], así como varias las oportunidades en las cuales ha emitido informes

[344] GUICHOT REINA explica con claridad este panorama: "en los países donde existe el modelo de doble agencia implantado en España (como Portugal, Italia o Francia, por no alejarnos de nuestro "vecindario"), las relaciones entre ambas han estado tradicionalmente marcadas por cierta tensión, y en ocasiones, por disparidad de criterios. En este sentido, la previsión podría saludarse como positiva. Ahora bien, a nuestro juicio (y no por casualidad) la propuesta viene de la AEPD. Y es que no debe olvidarse que, en coherencia con lo dispuesto en el apartado primero, es la normativa sobre acceso la que rige la publicidad activa o pasiva de información que contiene datos de terceros y en ese sentido, siendo deseable una interpretación armónica de ambos bloques normativos, dicha interpretación ha sido precisamente la efectuada por el legislador en el artículo 15 LTBG y su interpretación, como la del resto del articulado de dicha LTB, es de la competencia de las autoridades de transparencia". En: Guichot Reina, E. (2014). Los límites a la transparencia y el acceso a la información… *op. cit.* pp. 97-142.

[345] Sobre este particular, MATIA PORTILLA realiza una crítica importante a la interpretación de la AEPD. Si bien no compartimos el criterio expuesto, vale la pena hacer cita de la misma. Sin perjuicio de las observaciones apuntadas sobre la dificultad de tener dos autoridades interpretando desde paradigmas distintos una misma relación, no compartimos la crítica por cuanto la interpretación que el autor refiere como "hipertrofiada" o excesiva del derecho a la protección de datos personales es la que corresponde hacer a la AEPD en plena vigencia y garantía del derecho de acceso a la información, labor que le ha sido encomendada por el legislador y que ha jugado un papel determinante en la cultura de la protección de dato de carácter personal en España. Matia Portilla refiere que: "la regulación maximalista del derecho a la protección de datos que contiene la LOPD se ha visto intensificada, y esta es la segunda razón que explica la perturbación que la irrupción de este nuevo derecho ha producido en nuestro ordenamiento jurídico, por una doctrina especializada y una Autoridad específicamente establecida para vigilar la aplicación de esa norma que han tenido, en general, a propugnar, en el caso de la primera, y a llevar a cabo, en el caso de la Agencia Española de Protección de Datos, una interpretación extraordinariamente rigorista de las garantías contempladas en dicha ley para la defensa del derecho a la autodeterminación informativa, cuando no abiertamente extensiva del contenido de este". Ver en: Matia Portilla, E. (2017). Derecho a la información de los representantes políticos, protección de datos y transparencia. *Revista Jurídica de Castilla y León. Revista jurídica de Castilla y León, núm.* 42, mayo 2017. Recuperado de: http://www.jcyl.es/web/jcyl/AdministracionPublica/es/Plantilla100/1131978346397/_/_/_.

[346] En su Memoria Anual del año 2015, la AEPD anuncia que: "el más que significativo incremento de las cuestiones planteadas en torno a la conciliación de las normas de protección de datos con el principio de transparencia y el acceso a la información pública, en atención a lo establecido esencialmente, en el artículo 15 de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.

jurídicos que interpretan y definen el alcance de las obligaciones de la LTAIBG a la luz de los principios y derechos que inspiran la protección de datos de carácter personal y su principal referente normativo en el ordenamiento jurídico español (LOPD).

Las ocasiones en las que se ha pronunciado, han sido en su mayoría en el ejercicio del procedimiento de tutela de derechos previsto en el artículo 18 de la LOPD, que dispone que las actuaciones que sean contrarias a lo establecido en la LOPD, pueden ser objeto de reclamación ante la AEPD. Asimismo, ha emitido criterios haciendo uso de las facultades conferidas en el artículo que le permite emitir informes jurídicos.

3. Informes jurídicos

A. Informe 0390/2013 sobre transmisión de datos identificativos del titular de una licencia municipal de obras a terceros

En este informe, la AEPD resuelve de una consulta planteada en relación a la transmisión de los datos identificativos del titular de una licencia municipal de obras a terceros que se lo solicitan con amparo en la necesidad de conocer dichos datos para el ejercicio de acciones civiles contra tales titulares.

La AEPD considera que si bien la LTAIBG, aprobada después de entrada la consulta ante la Agencia, no había entrado en ese momento en vigor, si corresponde tomar en cuenta los criterios que establece para interpretar la ya derogada Ley 30/1992 que resultaba de aplicación en el momento de plantearse la consulta y cuyo precepto 37 que permitía el acceso a la información ha venido a ser sustituido por la LTAIBG (artículo 12 sobre el derecho de acceso a la información pública) y la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (artículo 13 sobre derechos de las personas en sus relaciones con las Administraciones Públicas). Bajo este entendido, apunta que el artículo 15.3 de la LTAIBG establece dentro de sus criterios que cabrá considerar prevalente el derecho del solicitante cuando la solicitud tenga por objeto el poder ejercer un derecho en juicio, lo que sucede en el caso de la consulta en

Como ya se indicó en la Memoria de 2014 se produjo un número significativo de estas consultas en el último trimestre de 2015, habiéndose confirmado esa tendencia, al incrementarse en 2015 en un 169%, pasando de representar un 2.5% a un 7.2% del total de consultas. A ello debe añadirse la elaboración conjunta por la Agencia y el Consejo de Transparencia y Buen Gobierno de criterios interpretativos relacionados con el artículo 15.". Disponible en: http://www.agpd.es/portalwebAGPD/LaAgencia/informacion_institucional/memorias-ides-idphp.php

que el solicitante desea tener acceso a los datos identificativos del titular de una licencia municipal con el fin de ejercer acciones legales.

En ese sentido, la AEPD considera que la cesión que deriva del derecho de acceso a la información pública –registros de licencias municipales de obras-, se encuentra amparado por lo dispuesto en la LOPD en conexión con el derogado artículo 37 de la Ley 30/1992, interpretada esta última norma al tenor de lo dispuesto en la LTAIBG.

B. Informe 0178/2014 relacionado con la aplicación de la LTAIBG y su conciliación con la LOPD

Por medio de este informe, la AEPD atiende varias consultas relacionadas con la publicación de los datos de beneficiarios de ayudas a personas con discapacidad, sin que se especifique el tipo de discapacidad,

Sobre el primer particular, la publicación de la condición de discapacidad de las personas que reciban alguna subvención o beneficio, de conformidad con lo que establece el artículo 8.1.c) de la LTAIBG, la AEPD estima que se trata de datos relacionados a la salud de una persona, según el artículo 7 de la LOPD. Siendo que aplica lo dispuesto en el artículo 5.3 y artículo 15 de la LTAIBG, así como las reglas del artículo 7 de la LOPD, lo procedente es que la publicación –ya sea en un tablón de anuncios o sitio web- se lleve a cabo previa disociación de los datos personales relacionados con las subvenciones de forma que no sea identificable el beneficiario. Añade, que para estos casos, el dato especialmente protegido no es el tipo de discapacidad, sino la existencia de la misma por lo que en todo caso debe procederse con la disociación.

C. Informe 0502/2014 sobre inclusión de firmas manuscritas en documentos escaneados

La Dirección General de Coordinación de Competencias con las Comunidades Autónomas y con las Entidades Locales del Ministerio de Hacienda y Administraciones Públicas, planteó una consulta ante la AEPD con el fin de conocer si de conformidad con la LOPD y la LTAIBG, resulta apegado al ordenamiento jurídico la publicación en el portal de transparencia, de los datos relacionados con firmas manuscritas que aparecen digitalizadas en documentos escaneados sobre convenios de colaboración o encomiendas de gestión firmadas por las entidades públicas, sociedades mercantiles, fundaciones y personas físicas.

La AEPD precisa que de conformidad la definición de datos de carácter personal tanto de la LOPD como de la Directiva 95/46, no queda duda que identificados los firmantes de los convenios o encomiendas de gestión, su firma queda vinculada a los mismos y por ende posee condición de dato de carácter personal.

Menciona que de conformidad con la regla de ponderación contenida en el artículo 15.3 de la LTAIBG, que exige tener en consideración el principio de proporcionalidad en el tratamiento de los datos personales contenido en el artículo 4.1 de la LOPD, la inclusión del dato de la firma escaneada en el portal de transparencia resultaría ajustada a lo dispuesto tanto en la LOPD como en la LTAIBG, en el tanto resulte adecuada, pertinente y no excesiva para la consecución de la obligación contenida en el artículo 8.1.b) de la LTAIBG.

Hecha la ponderación señalada, concluye que la inclusión en un documento escaneado de la firma manuscrita de los intervinientes no añade información adicional que coadyuve a la consecución del objetivo de la transparencia y podría implicar el conocimiento por parte de los consultantes, de información que genere un riesgo a la actividad pública, al ser de conocimiento público la grafía de la firma manuscrita de quienes intervienen en el convenio o encomienda. Asimismo, concluye que el artículo 8.1.b) no otorga cobertura a la inclusión de las firmas escaneadas de los intervinientes, por lo que dicho dato debe ser excluido de los documentos publicados en el portal de transparencia.

D. Informe 12155/2016 relativo al acceso a la información sobre personas que ocupan cada plaza de la RPT

En el Informe jurídico 12155/2016, la AEPD conoció de la consulta de un Delegado sindical miembro del Comité Intercentros relativo a la solicitud de acceso a un listado con nombres y apellidos del personal perteneciente al Consejo de Administración del Patrimonio Nacional, con el fin de conocer las personas que ocupan las plazas de la RPT[347].

El Informe comienza por reconocer que si bien la AEPD se ha pronunciado en ocasiones anteriores sobre este tema, en el sentido de que la normativa vigente –Ley

[347] Sobre este mismo tema, la AEPD se pronunció en el informe 012084/2016 en el que se consultaba la adecuación a la LOPD de las obligaciones de publicidad activa contempladas en la Ley 12/2014, de 16 de diciembre, de transparencia y participación ciudadana de la Región de Murcia.

30/1984 y Ley 7/2007-, no permitía una cesión masiva de la RPT incluyendo nombres y apellidos de todo el personal a los representantes de los trabajadores salvo casos específicos como por ejemplo, el ejercicio de una función de control, lo cierto es con la entrada en vigencia de la LTBG, entran en juego otra serie de consideraciones.

Partiendo de las disposiciones contenidas en la LTAIBG, en especial del artículo 15.2, la AEPD entiende que los datos de la RPT que deben figurar en el mismo, son aquellos que se refieran únicamente a datos meramente identificativos relacionados con la organización, funcionamiento o actividad pública del órgano, como por ejemplo, el nombre y apellido de las personas que ocupan los puestos.

Siendo que esto datos –nombre y apellidos- se encuentran cubiertos dentro del concepto de "datos meramente identificativos", la regla general se inclina a otorgar el acceso a los mismos frente al derecho a la protección de datos personales, salvo que, en el caso concreto, estos últimos prevalezcan. Para tales efectos, considera la AEPD que previo a conceder el acceso, debe notificarse de forma individualizada a todos los empleados a los que se refiera la información, otorgándose el plazo de 15 días previsto en el artículo 19.3 de la LTAIBG, para que estos puedan formular las alegaciones que estimen oportunas y así determinar la prevalencia o no de otros intereses o derechos protegidos distinto al de la publicad y el acceso.

Si bien a su criterio existe un principio general favorable al acceso, ello no exime que en cada caso concreto deban ponderarse las circunstancias específicas a fin de ponderar si prevalece el derecho de acceso o el derecho a la protección de dato. Esta es la única forma de poder garantizar que no se lesionan datos personales u otros intereses jurídicos como la seguridad, tal y como sucedería en el caso de víctimas de violencia de género, testigos protegidos o menores de edad.

Asimismo, hace referencia a los criterios interpretativos conjuntos emitidos junto con el CTBG en los cuales se abordó el tema del acceso a los datos sobre la RPT así como el informe de 4 de agosto de 2015, en el que concluyó que la LTAIBG no habilita el acceso indiscriminado a la totalidad de la información, sino que es modulado por los criterios tanto del CTBG y la AEPD, de modo que habrá de tenerse en cuenta, en cada caso, la categorización sobre la clase y nivel del puesto, los intereses que pueden entrar en juego, entre otros.

E. Informe 0160/2016 sobre aplicación de la LOPD a tratamiento posterior de datos obtenidos por medio de solicitudes de acceso a la información

En el Informe 0160/2016, la AEPD resuelve una consulta remitida por parte del CTBG, en la que en esencia el consultante, pregunta sobre la licitud a la luz de lo dispuesto en el artículo 15.5 de la LTAIBG, de la cesión de los datos que ha obtenido mediante el ejercicio del derecho de acceso a la información a los alumnos que reciben sus cursos. Indica que en ningún caso, ha disociado la información de forma previa a la difusión a sus estudiantes.

En primer lugar, la AEPD apunta que de conformidad con lo dispuesto en el artículo 15.5 de la LTAIBG, la LOPD resulta aplicable a cualquier tratamiento posterior de datos. De conformidad con lo anterior, a quien ejercita el derecho de acceso a la información pública le será aplicable el artículo 4 de la LOPD así como que deberá contar con la adecuada legitimación para llevar acabo el tratamiento y la cesión, conforme a lo dispuesto en los artículos 6 y 11 de la LOPD. Asimismo, deberá implantar las medidas de seguridad adecuadas y respetar el deber de secreto, conforme a lo establecido en los artículos 9 y 10 de la LOPD. Igualmente pesa la obligación de atender solicitudes de ejercicio de los derechos de acceso, rectificación, cancelación y oposición establecidos en la normativa de protección de datos.

Ni la LOPD ni la LTAIBG, contemplan supuestos que exceptúen la aplicación del artículo 15.5 de la LTAIBG, por lo que la difusión que se vaya a hacer de la información queda sometida en su totalidad a la LOPD. Entiende que una interpretación de la LTAIBG que pretenda justificar la inaplicación de las normas de protección de datos, especialmente los principios de calidad y legitimación, en aquellos casos en que se hubieran obtenido de forma lícita los datos de carácter personal, lesionaría de forma grave este derecho y frustraría el nivel elevado de protección que justamente persiguen sus normas.

Concluye, que en el caso concreto de la consulta, el uso que se haga de los datos obtenidos como consecuencia de una solicitud de acceso a la información, indudablemente está sometido a lo dispuesto en la LOPD en virtud del artículo 15.5 de la LOPD, lo que implica que debe contar con legitimación suficiente para poder llevar a cabo el tratamiento de los datos. Asimismo, estima la AEPD que la comunicación de las resoluciones a los alumnos sin previa disociación de los datos personales supone una cesión contraria al derecho a la protección de datos personales, resultando dichos datos

innecesarios y excesivos para la labor didáctica o divulgativa que podría justificar que se transmita una copia de las resoluciones o información obtenida.

4. Resolución de reclamaciones

A. Datos especialmente protegidos

En similar sentido, la AEPD en resolución R/02316/2016 conoció de un caso en el que se acusaba la publicación en un sitio web de la baremación para la concesión de plaza escolar de un menor, incluyendo el dato de minusvalía del padre aportado. Si bien la Consejería de Educación, Cultura y Deportes de la Junta de Comunidades de Castilla La Mancha aduce a su favor que la publicación de tales datos es en cumplimiento de las exigencias derivadas de la LTAIBG, lo cierto es que hacer referencia a la discapacidad de una persona dentro del entorno familiar del menor, en un sitio web en el que se publican los resultados de la concesión de la plaza escolar, con acceso irrestricto, constituye un tratamiento de información sensible que no está permitido por la LOPD. Por último, indica que la finalidad perseguida con la publicación se puede cumplir facilitando el acceso de un usuario y contraseña a todos los participantes del concurso, o bien, cualquier otro sistema siempre que este sea de acceso limitado.

También, la AEPD estimó por medio de la R/00270/2016 una denuncia interpuesta contra el Gobierno de Canarias, por haber publicado las listas de ampliación y constitución para docentes en la especialidad de medios audiovisuales, indicando la condición de minusválido del denunciante. A su criterio, la publicación en la página web de los datos personales de los solicitantes relativos a la situación de baremo, en la que se indica su condición de minusválido, contiene información sensible de las personas admitidas o excluidas, debiéndose haber ponderado la prevalencia del derecho de la protección de datos sobre la publicidad activa, de forma que se evitara la publicación del dato referido a la minusvalía de los participantes.

Asimismo, en la R/002575/2016, la AEPD consideró que hacer referencia a la situación de baja médica de un funcionario policial, en una noticia que tiene por objeto hacer de conocimiento que la policía local del Ayuntamiento de Teror amplio su horario de servicio 24 horas, no constituye el ejercicio del derecho de acceso a la información ni una obligación de publicidad activa, por lo que no puede alegarse que la divulgación de dicho dato se hizo en cumplimiento de los dispuesto en el artículo 1 de la LTAIBG.

B. Publicidad activa de ayudas y beneficios públicos

En la R/02702/2016, la AEPD conoció de una denuncia presentada contra *la Conselleria de Cultura, Educación e Ordenación Universitaria,* por haber colocado en un tablón de anuncios en la entrada del colegio, visible desde la vía pública, la fotografía y datos personales de su hija. Asimismo, los datos fueron publicados con acceso irrestricto en el sitio web del centro educativo. La *Conselleria* alega en su defensa que los datos publicados –nombre y apellidos de la alumna, así como los libros que recibe del fondo solidario-, forma parte de las bases de la convocatoria que regula el fondo solidario de libros de textos y además, que en aplicación de la LTAIBG corresponde la publicación de dichos datos.

En el presente caso, la AEPD estima que si bien se prestó el consentimiento para el tratamiento de los datos al haber aceptado las bases de la convocatoria y el centro docente actuó en cumplimiento de la normativa, debe considerarse que la difusión de concesión de ayudas públicas y subvenciones que exige la ley debe hacerse tomando en cuenta la LOPD. En ese sentido, deben adoptarse medidas legales que tengan en cuenta ambos derechos y satisfagan el fin de la publicidad perseguido, como por ejemplo, la limitación del acceso a la web únicamente a los participantes de la convocatoria, mediante la identificación con clave y usuario, y la eliminación de la publicación del anuncio en la vía pública.

Por resolución R/02242/2016, entro en el conocimiento de una denuncia presentada contra el Ayuntamiento de Madrid, por haber publicado en la página web los datos personales de un beneficiario de una beca, con indicación de que se aportaba copia de una sentencia que le reconoce como víctima de violencia de género y una orden de alejamiento emitida por un juzgado penal. El Ayuntamiento alega que la publicación se hace con base en la norma reguladora del procedimiento, que establece que se debe publicar la concesión de la beca, así como en el artículo 8 de la LTAIBG que obliga a la publicación de las subvenciones concedidas. En este caso, la AEPD estima la reclamación por considerar que el Ayuntamiento debió haber valorado los motivos que alegó la interesada y no publicar los datos personales, esto según lo dispuesto en el informe jurídico 0414/2015 de la AEPD. En idénticos términos se pronunció en la R/02183/2016.

C. Publicidad activa del DNI

Por medio de resolución R/00417/2017, la AEPD, resolvió un caso en el que el denunciante reclamaba haber solicitado el ejercicio de oposición frente al Ayuntamiento de Madrid para que se procediera con el borrado de su nombre y DNI de determinados contratos públicos en los que aparecía como apoderada o representante de BANKIA. El Ayuntamiento de Madrid contesta la audiencia conferida, manifestando que dichos contratos están afectos a la publicidad activa que exige el artículo 8 de la LTAIBG; no obstante, siguiendo los criterios interpretativos del CTBG y la AEPD, procederá al borrado de los datos del DNI de las personas jurídicas en convenios y contrarios, previo la adopción de medidas técnicas necesarias, en el tanto es información que excede la esfera pública de los firmantes.

Si bien la AEPD inadmite la reclamación presentada, confirma y ratifica que se debe proceder al borrado de los datos del DNI del reclamante al ser este un dato que excede la esfera pública.

D. Publicaciones de datos consignados en actas o sesiones por parte de los Ayuntamientos

Por medio de la R/00692/2017, la AEPD conoció de una denuncia interpuesta contra el Ayuntamiento de Las Regueras, en la que una persona reclamaba que en el sitio web del Ayuntamiento constaba publicada un acta de la Junta de Gobierno Local, en la que constan sus datos personales, en concreto, nombre y apellidos así como domicilio, con ocasión de una gestión ante dicho Ayuntamiento. Ante la denuncia interpuesta, el Ayuntamiento denunciado manifestó que de los artículos 5 y 15 de la LTAIBG, en el caso de la publicidad activa, únicamente corresponde la no publicación y disociación de datos especialmente protegidos.

Por otra parte estimó que el Ayuntamiento realizó un tratamiento de datos del denunciante en la página web sin que hubiese existido habilitación legal para tales efectos, ya que al no ser públicas las sesiones por ley, tampoco pueden ser públicos los datos en ellas discutidos. Asimismo, considera que una simple petición de reposición de mobiliario urbano, no justifica bajo la pretendida transparencia, la exposición de los datos del denunciante. Tampoco se acreditó que se cuente con el consentimiento del afectado para la publicación de sus datos.

Asimismo, en la R/00475/2016 entendió que la publicación en un tablón de anuncios en una página web y en el tablón de anuncios del Ayuntamiento, de un acta de la sesión ordinaria del Pleno en determinada fecha, en la que se publican los datos personales del denunciante en relación con el impago de varios impuestos municipales, es contrario a la LOPD. Esto por cuanto a pesar de que el Ayuntamiento acusa estar amparado por la LTAIBG, la publicación de la totalidad de las actas resulta excesiva. Si bien el Real Decreto 2568/1986 faculta a las corporaciones a dar publicidad resumida del contenido de las sesiones plenarias y acuerdos del pleno, así como Comisiones de Gobierno y resoluciones del Alcalde, en el presente caso, en que se publica ni resumida ni anonimizada la totalidad del acta, tanto en el tablón de anuncios como en la página web, a la vista de cualquiera, sobrepasa los límites de la ley y resulta contrario a la LOPD.[348]

No obstante, en la R/00697/2015, desestimó una denuncia incoada contra el Ayuntamiento de La Rinconada, por haber publicado en el sitio web un acuerdo adoptado por el Pleno del Ayuntamiento, que a su vez ratificaba un acuerdo de pago de justiprecio a un ciudadano. En este particular, la AEPD estimó que la información incluida en el acta del Pleno publicada en el sitio web sí reviste un interés para el conocimiento de la actuación pública en un proceso de expropiación que concluyó en determinadas actuaciones jurisdiccionales y en las que se generó un amplio debate por el desacuerdo con el afectado.

E. Retribuciones

Por su parte, la AEPD conoció en el ámbito de sus competencias, por medio de la R/02765/2016, de una denuncia contra el Ayuntamiento de Calpe por motivo de la publicación en su sitio web de un documento en el que consta el presupuesto del Ayuntamiento y aparece toda la plantilla de la Policía Municipal con nombres y apellidos así como su asignación económica.

En este caso, la AEPD consideró que siendo que no se trata del ejercicio del derecho de acceso a la información ni de una obligación de publicidad activa, sino que la intención del Ayuntamiento era, por voluntad propia, exponer la memoria presupuestaria, pudieron haberse consignado los datos de forma global y disociada y no cono

[348] En un sentido similar pueden observarse la R/02162/2015 y R/02253/2015.

identificación del puesto y la persona que lo ocupa, que además en el caso concreto no refleja la realidad pues no se contemplaron trienios, productividad o antigüedad. Atendiendo a los artículos 4.1 y 2 de la LOPD, considera que para cumplir con la finalidad de la transparencia perseguida, no resultaba necesario identificar al titular del puesto, pues a efectos presupuestarios ello no tiene relevancia, sino que únicamente el dato de forma global.

Asimismo, expone que los principios de nivel de idoneidad, proporcionalidad y calidad en el tratamiento de los datos se incrementen si se incluye a los ocupantes de los puestos, ya que el conocimiento de dichos datos no guarda relación con cifras económicas consolidadas y conceptos de contabilidad, pudiendo suministrarse sin necesidad de hacer referencia a nombres y apellidos de los ocupantes, por ejemplo, mediante el desglose sin datos personales.

Por último, considera que no exista norma que habilite la exposición de los datos de los ocupantes de los puestos de la plantilla contenido en la memoria anual del presupuesto no concurre algún supuesto de transparencia que permita la publicación de los datos de los ocupantes de los puestos detallados en la memoria anual de presupuesto. Tampoco se contaba con el consentimiento de los trabajadores y empleados para la publicación de estos datos.

En otra resolución, la R/00401/2016, estimó una denuncia contra la Consejería de Hacienda y Administraciones Públicas del Gobierno de Aragón, que publicó en el Boletín Oficial de Aragón la RPT de todos sus trabajadores. A criterio de la AEPD, la publicación de la RPT de todos los funcionarios resulta excesiva y no está prevista en la Ley 8/2015, de Transparencia de la Actividad Pública y Participación Ciudadana de Aragón, que no contempla la publicación de datos personales de los empleados públicos ni "ocupantes" que cubren puestos de trabajo. Por lo tanto, considera la AEPD que debieron ponderarse ambos derechos y evitarse la publicación de los datos identificativos relativos al nombre, apellidos, DNI o número de registro del personal.

La AEPD en su resolución de archivo de actuaciones del expediente E/07173/2015, conoció de una reclamación presentada por el Jefe de Administración de la Federación Gallega de Vela, quien entendía que era improcedente la publicación de su sueldo en el sitio web de la Federación, por cuanto su puesto no debe soportar las obligaciones de publicidad activa que contiene la LTAIBG. Siguiendo una línea similar

a la expuesta por el CTBG, la AEPD considera que si bien dentro de la circular de la Xunta de Galicia a la Federación Gallega de Vela, en la que especifica los puestos sobre los que deben publicarse las retribuciones anuales de los máximos responsables federativos (presidente, secretario, gerente, tesorero, director, técnico), no consta el de jefe administrativo, este puesto es asimilable en funciones al de gerente, por lo que sí es procedente la publicación de los datos relativos a las retribuciones.

Asimismo, estimó una denuncia presentada contra la Consejería de Presidencia de la Comunidad Autónoma de la Región de Murcia, que publicó en el portal de transparencia, la RPT en la que constan 8.000 empleados públicos de la administración general y los organismos autónomos que incluían datos más allá de los considerados como datos meramente identificativos. La Consejería argumenta que es con ocasión del cumplimiento de las obligaciones impuestas por la LTAIBG así como que se está en consonancia con los criterios conjuntos que han emitido la AEPD y el CTBG.

La AEPD estima la denuncia por considerar contrario a la LOPD, haber difundido sin consentimiento ni amparo legal, datos personales de los empleados públicos que exceden lo previsto para la consecución del fin que persigue el objetivo de la transparencia. En ese sentido, considera que exceden a los datos identificativos que deben ser publicados, datos como la titulación académica, formación específica, complementos salariales, así como varias observaciones relacionadas con capacitación y formación del empleado público. También, resulta excesivo publicar datos como por ejemplo, si se posee permiso de conducir, nivel de inglés, acreditaciones técnicas, entre otras. Todos los anteriores, datos que no resultan amparados por el artículo 6.1 de la LOPD.

F. Libertad de expresión

La AEPD conoció en su resolución de archivo de actuaciones del expediente E/04059/2016, de una denuncia presentada por una persona que acusa que el Partido Popular de Monachil, Granada, publicó en su página web, un Decreto de la Alcaldía en la que aparecen su nombre y apellidos en relación con un adelanto de nómina. Señala que estos datos han sido publicados sin su consentimiento.

En esta ocasión estimó que en el caso concreto se está ante el ejercicio de la libertad de expresión e información que realiza un partido político, con el fin de conformar una opinión política y pública sobre una actuación que afecta a un

representante político y a una supuesta situación de privilegio denunciada. Por esta razón, consideran improcedente la imposición de una sanción por infracción a la LOPD.

G. Divulgación en Internet de identidad de trabajadores en procesos de licitación

El Concello de Vigo publicó en su sitio web, los pliegos técnicos presentados con ocasión del concurso para la contratación de servicios para piscinas y gimnasios, los cuales incluyen un anexo en la que se incluye la relación de trabajadores, con los nombres y apellidos, DNI, antigüedad, categoría y jornada de cada uno de ellos. Por motivo de esta publicación, una persona presentó una denuncia, por considerar que ello vulnera su derecho a la protección de datos personales.

Por R/02526/2015, la AEPD resolvió la denuncia y estimó, en primer lugar, que no resultaba necesario que se realizara la publicación del pliego de condiciones de forma abierta en Internet, de forma que se pusiera en conocimiento de terceros que no poseen ningún interés legítimo, datos personales de los trabajadores como por ejemplo, nombre y apellidos, DNI, antigüedad, categoría y jornada de cada uno de ellos. A su criterio, la invocación de la LTAIBG y el principio de transparencia como justificación para la difusión de los datos no resulta procedente, ya que no hay relevancia pública que justifique la publicidad y acceso universal a la identidad de los trabajadores asociada a su perfil profesional, siendo que la exigencia de la transparencia se hubiera visto satisfecha con la publicación en la web pero únicamente con acceso restringido para los licitadores, ya hubiera sido en el trámite o tras la adjudicación.

5. Tabla de casos resueltos

A continuación se presenta una tabla con la totalidad de los casos analizados para este trabajo junto con una descripción y la resolución que dio el AEPD a los mismos.

Resolución	Objeto	Fundamentos jurídicos
R/00697/2015, de 7 de abril	El Ayuntamiento de La Rinconada publicó en su sitio web, un acuerdo adoptado por el Pleno del Ayuntamiento sobre la ratificación de un acuerdo de pago de justiprecio de julio de 2014. El reclamante solicitó el ejercicio de su derecho de cancelación de dichos datos, en el tanto considera que supone un perjuicio a su derecho a la protección de datos personales.	La AEPD considera que la información incluida en la publicación en el sitio web del Ayuntamiento reviste un interés para el conocimiento de la actuación pública en un proceso de expropiación que desembocó en diversas actuaciones jurisdiccionales y en un amplio debate político. Asimismo, considera que la publicación no refleja datos obsoletos, pues aún en 2017 continúan haciéndose efectivos los pagos de dicho acuerdo. (FJ 9)

R/02526/2015, de 2 de octubre	El reclamante denuncia ante la AEPD que el Concello de Vigo publicó en su página web, el concurso para la contratación de servicios para piscinas e instalaciones del Instituto Municipal de Deportes de Vigo. Indica que en los pliegos técnicos y administrativos publicados, se incluye una lista de trabajadores con el siguiente detalle: nombre y apellidos, DNI, antigüedad, categoría y jornada.	La AEPD considera en este caso que el principio de transparencia, como justificación para la difusión de los datos personales de los trabajadores no puede ser tenido en consideración. La identidad de los trabajadores, asociada su perfil profesional, no resultaba de relevancia pública en ese momento del concurso. De tal manera que no se justificaba el acceso universal a dicha información a través de una publicación en la web. (FJ 6) El objetivo de la trasparencia en el caso concreto, pudo conseguirse a través de la publicación de dichos datos de forma que fuera únicamente accesible a los licitadores de forma restringida o tras la adjudicación. Es decir, que el Concello pudo haber ofrecido la misma información, para esa finalidad sin necesidad de publicar los datos de los trabajadores a través de su sitio web. (FJ 6)
R700270/2016, de 3 de marzo	La denunciante alega ante la EPD que la Consejería de Educación del Gobierno de Canarias, publicó listas de ampliación y constitución para docentes en la especialidad de medios audiovisuales indicando su condición de "minusválidos".	En este caso, la AEPD consideró que la publicación en una página web de la Consejería de los datos personales de los solicitantes relativos a su situación en un baremo en el que se hacía constar su condición de minusválido, constituye un tratamiento de información sensible sobre aquellas personas que se presentan al concurso, sean admitidos o excluidos, por lo que debería haberse ponderado la prevalencia del derecho a la protección de datos y la publicidad activa, evitando la publicación sobre el dato que refiere a la condición de minusvalía. (FJ 6)
R/00475/2016, de 7 de marzo[349]	El reclamante acusa ante la AEPD que el Ayuntamiento de Los Alcázares llevó a cabo una publicación de un acta de una sesión ordinaria del Pleno, en la que se publican sus datos personales en relación con varios impuestos municipales impagados.	La AEPD consideró en el caso concreto que el Ayuntamiento denunciado no dio una publicidad resumida de las actas del Pleno como le autoriza la ley, sino que publicó de forma total las actas en las que figuran los datos del denunciante en relación con varios impuestos municipales impagados. La publicidad no resumida ni anonimizada de esta información, sobrepasó los límites del Tablón de Anuncios del Ayuntamiento o de los boletines informativos de la entidad, ya que se publicó en la página web a la vista de cualquier persona. (FJ 6)
R/01585/2016, de 28 de julio de 2016	La AEPD conoce de 56 denuncias contra la Consejería de Presidencia de la Comunidad Autónoma de la Región de Murcia, que publicó en el portal de transparencia, la RPT en la que constan los datos de 8.000 empleados de la Administración General y los organismos públicos.	En el caso concreto, la AEPD considera que la Consejería denunciada procedió a difundir sin consentimiento ni amparo legal de los empleados públicos de la Comunidad Autónoma, datos que exceden los meramente identificativos y necesarios para la finalidad que justificaba la publicación, como por ejemplo, datos relativos a la titulación académica, formación específica,

[349] En similar sentido pueden observarse la: R/02162/2015 y la R/02253/2015

		complementos salariales, capacitaciones, entre otras. El tratamiento no resulta amparado por lo dispuesto en el artículo 6.1 de la LOPD. (FJ 8)
R/02242/2016[350]	La reclamante denuncia ante la AEPD que el Ayuntamiento de Madrid publicó en su página web sus datos personales en relación con una beca que le fue concedida, con la indicación de que aportó una sentencia que le reconoce como víctima de violencia de género y una orden de alejamiento emitida por un juzgado penal.	De conformidad con lo dispuesto en el informe jurídico 0414/2015 de la AEPD, estima que debieron valorarse los motivos que expuso la interesada en el ejercicio de sus derechos y no publicar los datos personales en relación con su situación de víctima de violencia de género. (FJ 7).
E/04059/2016, de 8 de septiembre	El denunciante alega ante la AEPD que el Partido Popular de la localidad de Monachil publicó en la red social Facebook, un decreto de la Alcaldía en que aparecen sus datos personales relacionados con un adelanto sin nómina. Aduce que el tratamiento de datos se llevó a cabo sin su consentimiento.	La AEPD resuelve que en este caso se está ante el ejercicio de la libertad de expresión e información realizado por un partido político en aras de conformar una opinión política y pública sobre una actuación que afecta a un representante político y a una supuesta situación de privilegios que se ha denunciado. (FJ 6)
R/00401/2016, de 14 de marzo	En esta reclamación, se acusa ante la AEPD que la Consejería de Hacienda y Administraciones Públicas del Gobierno de Aragón, publicó en su Boletín Oficial, la RPT de todos sus trabajadores. Los datos publicados comprenden: nombre, apellidos, NIF y RPT asociados a denominación del puesto, grupo, características y tareas encomendadas, titulación académica, información específica, complementos salariales, observaciones, entre otros.	La publicación en la página web de la Consejería de los datos personales indicados, se deduce información excesiva y no prevista en la Ley 8/2015, de Transparencia de la Actividad Pública y Participación Ciudadana de Aragón, que no contempla la publicación de los datos personales de los empleados públicos ni de los ocupantes que cubren los puestos de trabajo. En ese sentido, debió haberse ponderado la prevalencia del derecho a la protección de datos y la publicidad activa, evitando la publicación referida a los datos, pues no existe habilitación legal para tales efectos. (FJ 6)
E/07173/2015, de 3 de octubre de 2016	El reclamante, quien es Jefe de Administración de la Federación Gallega de Vela, denuncia que su sueldo ha sido publicado en el sitio web de la Federación con el fin de dar cumplimiento a la Ley de Transparencia, pese a que entiende que el puesto que desempeña no soporta la obligación de publicidad activa. Asimismo, denuncia que el tratamiento de datos se ha llevado a cabo sin su consentimiento.	Indica la AEPD que el criterio de publicación de los datos se basa en las obligaciones contenidas, entre otras, en la LTAIBG y la Ley 3/2012, de 2 de abril, del Deporte de Galicia. En el caso concreto, si bien la denominación de "jefe de administración" no aparece de forma expresa dentro de los puestos sobre los que debe publicarse la información retributiva presidente, secretario, gerente, tesorero, director, técnico), lo cierto es que el puesto es asimilable en funciones al puesto de gerente, por lo que procede la publicación de la información. (FJ 3)
R/02575/2016, de 17 de octubre	El denunciante acusa que en la página web del Ayuntamiento de Teror se publicó una noticia sobre la policía local, en la que aparece su nombre y apellidos asociado al dato de que se encuentra de baja médica, lo que	La APED estima que el interés público de la noticia está en la ampliación del servicio pero resulta invasivo en relación con la publicidad activa que pretende la noticia, revelar los datos sobre la condición de baja médica del denunciante. (FJ 2)

[350] En idénticos términos: R/02183/2016.

	considera vulnera el derecho a la protección de datos personales.	La publicación de estos datos no resulta adecuada, pertinente, ni necesaria para la finalidad perseguida, que era la de informar de la apertura del servicio de policía local a 24 horas, siendo colateral y no necesario informar para tales efectos el nombre y apellidos del denunciante, así como que estaba de baja médica. (FJ 2)
R/02316/2016, de 13 de octubre	La denunciante alega ante la AEPD que la Consejería de Educación, Cultura y Deportes de la Junta de Comunidades de Castilla - La Mancha publicó en su página web, la baremación para la concesión de la plaza escolar de su hijo, incluyendo en la información el dato de minusvalía del padre aportado para la baremación.	A juicio de la AEPD, la publicación en la página web de la Consejería de los datos personales de los solicitantes relativos a la situación en un baremo en el que se hace constar la condición de discapacidad de uno de los miembros del entorno familiar, corresponde a un tratamiento de información sensible que no es acorde con la protección de datos personales. (FJ 6) La Consejería de Educación debería prever un sistema en el que todos los participantes puedan acceder a la información, puesto que se trata de concurrencia competitiva, pero dicha información no puede ser accesible a terceros no autorizados ni puede ser captada por los buscadores de Internet. (FJ 5)
R/02702/2016, de 3 de febrero de 2017	La reclamante denuncia ante la AEPD la publicación de datos de un menor en un tablón de anuncios del colegio al que asiste, ubicado en vía pública. Los datos publicados corresponden a la lista definitiva de admitidos al fondo solidario de libros de texto.	Estima la AEPD que la difusión de concesión de ayudas públicas y subvenciones que requiere la normativa debe satisfacerse con medidas que conjuguen tanto la publicidad en la gestión de fondos públicos con la protección de datos personales, como por ejemplo, la limitación del acceso a la web únicamente a los participantes de la convocatoria por medio de un acceso restringido, o bien, la eliminación de la publicación del tablón de anuncios de la vía pública. (FJ 5)
R700417/2017, de 22 de febrero	El reclamante ejerció su derecho de oposición ante el Ayuntamiento de Madrid para que se procediera con el borrado de su nombre y DNI en contratos públicos en los que aparecía como apoderado o representante de Bankia.	Pese a que el Ayuntamiento denegó de forma motivada el ejercicio del derecho de oposición en el transcurso de la tramitación de la denuncia ante la AEPD, manifestó que procedería a cumplir con el borrado del dato del DNI de conformidad con los criterios establecidos por la AEPD y el CTBG que entienden que dichos datos resultan excesivos de conformidad con la finalidad que persigue la LTAIBG. (FJ 8)
R/00692/2017, de 14 de marzo	El denunciante acusa ante la AEPD que el Ayuntamiento de Las Regueras publicó la totalidad de un acta en la que constan sus datos personales (nombre, apellidos, domicilio) con ocasión de una gestión de reposición de mobiliario inmueble que realizó ante dicho Ayuntamiento.	En función de la publicidad activa, el ayuntamiento puede publicar de forma resumida el contenido de las sesiones y acuerdos del Pleno y las Comisiones pero sin incluir más datos de los adecuados y pertinentes en relación con la finalidad pretendida. En el caso concreto en el que lo discutido en el acta de la sesión era una mera propuesta o solicitud de reposición de mobiliario, resulta excesivo la publicación de los datos personales y las circunstancias particulares del solicitante. (FJ 6)

R702765/2016,, de 4 de noviembre de 2016	Un representante sindical presenta una denuncia contra el Ayuntamiento de Calpe, por haber publicado en su sitio web, un documento en el que aparece toda la planilla de la Policía Municipal con nombres apellidos y su correspondiente asignación económica.	El Ayuntamiento no logró demostrar que contara con el consentimiento de los trabajadores y empleados para la publicación de sus datos personales. Si lo pretendido era exponer la memoria presupuestaria, pudo haber hecho la publicación de los datos consignando los mismos de forma global y disociada. Asimismo, la información publicada no refleja datos exactos, pues no se contemplaron datos como los trienios, productividad o antigüedad. (FJ 5)

Recapitulación

Como ya se explicó en un apartado anterior, en el caso español, el legislador decidió atribuir la competencia de la aplicación de la LTAIBG al CTBG. Esto conduce a que exista en la actualidad un sistema de interpretación de la relación entre transparencia, acceso a la información y protección de datos personales.

Por un lado, la LTAIBG confiere la interpretación de la LTAIBG –lo que incluye el artículo 15 al CTBG, mientras que por otra parte, la AEPD continúa teniendo plenas competencias para el conocimiento de casos e interpretación de la LOPD en el ámbito de sus facultades, creando un ambiente que no resulta del todo armónico que no logra ser superado con la facultad de emitir criterios de interpretación conjunta que les fue conferido por la LTAIBG, porque al menos hasta ahora, estos han sido limitados y lo cierto del caso es que ambas agencias, a la fecha, se encuentran resolviendo por su lado una gama de temas mucho más amplios de los que han tenido oportunidad de pronunciarse en los escasos criterios conjuntos que han emitido.

La tensión, aunque no reconocida abiertamente por ninguna de las dos instituciones, no ha tardado en aflorar y es natural, pues es totalmente entendible que el órgano encargado de interpretar el acceso a la información y la transparencia, sea más proclive a este derecho, y que la agencia encomendada a la protección de los datos personales, que además tiene ya una sólida historia de la consolidación del derecho, se muestre más conservadora en sus posturas.

Ha significado también, como lo ha reconocido la propia AEPD, un replanteamiento al abordaje que había hecho hasta el momento de la relación entre transparencia, acceso a la información y protección de datos personales. Ejemplo de

ello es que ha tenido que cambiar su postura previa a la LTAIBG que consideraba que para poder acceder a datos personales que constaban en información pública se requería el consentimiento informado del interesado, a reconocer que la LTAIBG constituye un título habilitante para la cesión de datos personales, según lo que establece la LOPD en materia de transmisión de datos a terceros.

En comparación con las resoluciones y criterios expuestos del CTBG, si bien no hay contradicciones, al menos evidentes por ahora, si ha sido tajante la línea en la aplicación de los principios y derechos de la protección de datos personales –línea rígida propia de la materia-, que dejan poco espacio desde la interpretación que hace la AEPD, a la ponderación a la que también llama la LTAIBG cuando se pretenda el acceso a datos personales que constan en información pública.

Evidencia de lo anterior es la interpretación a rajatabla que ha hecho del artículo 15.5 de la LTAIBG, indicando que ni la LOPD ni dicha ley establecen una excepción a la aplicación de la normativa de protección de datos en los tratamientos posteriores que se haga de la información obtenida a través del ejercicio del derecho de acceso a la información.

Surge entonces así la duda de, cómo se compatibilizará la transparencia y el ejercicio del derecho del acceso a la información y el fin que se persigue, que es que los ciudadanos tengan cada vez mayor conocimiento de la administración pública y sus gestiones y puedan exigir el rendimiento de cuentas, cuando la información a la que se puede acceder no podrá ser después sometida a un debate público?

Sin demérito de los avances que ha supuesto, sólo la aplicación en la práctica de la LTAIBG por parte del CTBG y la AEPD tendrán la capacidad de indicar, si con todos los elementos que hay en juego, incluido el artículo 15.5 y la interpretación hecha por la AEPD a instancia del CTBG, se está ante un panorama lampedusiano en el que se ha cambiado todo para que nada cambie.

Conclusiones

Ha transcurrido ya un tiempo considerable desde que se comenzara a hablar en los textos jurídicos internacionales del derecho a la intimidad (CEDH) y que los tribunales internacionales (TEDH) así como los diferentes actores políticos y sociales entraran en cuenta de que la protección de datos personales requería de un tratamiento jurídico específico, que quedó cristalizó por primera vez, en la década de los ochenta, en el Convenio 108 del Consejo de Europa.

Años más tarde y con miras en estos y otros antecedentes que fueron surgiendo en el ámbito doméstico de los Estados miembros de la UE, se planteó dentro del marco comunitario, la necesidad de regular la libre circulación de datos de carácter personal, de forma que no constituyera un obstáculo para el mercado y la libre circulación de los mismos, pero que tampoco supusiera un menoscabo para las libertades y derechos de las personas. Con este afán de libre circulación y no obstaculización del mercado se aprobó la Directiva 95/46, que poco tiempo después, sería reconocido como un derecho fundamental en la CDFUE y que ha alcanzado las dimensiones que conocemos hoy en día, al punto, como ya lo ha señalado algún autor, de que el tema de protección de datos ha llegado a ocupar un sitio importante dentro de la política de la UE y del Consejo de Europa.

La Directiva 95/46 fue aprobada en un contexto histórico y social en el que poco se vislumbraban los alcances que rápidamente adquiriría el uso de las nuevas tecnologías y el Internet en prácticamente cualquier espacio de nuestra vida cotidiana. Bajo este panorama, no es de extrañar que con relativa frecuencia el derecho a la protección de datos, ya positivivzado en dicha Directiva, corriera el riesgo de perder vigencia por no tener la capacidad de adaptación y de respuesta a los cada vez más cambiantes escenarios en los que se planteaba su efectividad –reto que hoy en día, ante la velocidad de los avances tecnológico, subsiste-.

La manera de mantener este derecho con vigencia y contenido frente a los vertiginosos avances de la tecnología y los retos que representa para la privacidad de las personas y especialmente sus datos personales, el TJUE se dio a la tarea de interpretar el derecho en una variedad de escenarios, logrando así que este tuviera la capacidad de dar una protección y tutela a los datos de carácter personal en la sociedad de la información. Es importante destacar, que esta labor en el ámbito del Consejo de Europa estuvo

encomendada también al TEDH, que con su jurisprudencia e interpretación del artículo 8 del CEDH, colaboró también en el perfilamiento del derecho a la protección de datos personales en el ámbito comunitario por parte del TJUE.

La labor que ha desarrollado el TJUE durante las poco menos de dos décadas al día de hoy, ha alcanzado a pronunciarse sobre temas como si los datos biométricos se encuentran comprendidos dentro del concepto de dato de carácter personal, pese a que la Directiva no los menciona específicamente, a casos que han generado gran impacto mediático, político y judicial, como lo es el pronunciamiento del caso Google sobre el derecho al olvido frente a motores de búsqueda en Internet, o el caso Schrems, en el que se resolvió sobre los flujos internacionales de datos a países terceros y las garantías de un nivel de protección adecuado en dichos países. Todos estos años de interpretación, le han permitido crear una sólida doctrina sobre el derecho a la protección de datos personales, que ha terminado siendo incorporada a la nueva regulación de protección de datos personales en la UE: el RGPD.

Desde la aprobación de la Directiva 95/46 hasta el RGPD, el cambio que ha supuesto la tecnología en lo que se refiere al tratamiento de nuestros datos personales ha dado un giro radical; no obstante, fue hasta casi dos décadas después que llegó la actualización del marco normativo comunitario, tras un largo proceso de consultas y respectivos consensos que dio inicio desde antes de 2012.

El RGPD consciente de la dimensión que ha cobrado el tratamiento de los datos de carácter personal en el mundo globalizado y ante la sensación de los ciudadanos de tener cada vez menos control sobre los mismos, ha tratado de crear un marco normativo que le devuelva a los ciudadanos ese poder de control y disposición de sus datos e información personal. Pero más importante aún, el RGPD pretende cambiar el enfoque reactivo por parte de los responsables y encargados del tratamiento de los datos personales –paradigma bajo el que nos encontramos actualmente con la Directiva 95/46 y las normas nacionales que la trasponen-, por un enfoque proactivo –RGPD-.

El enfoque proactivo que contempla el RGPD, pretende que el cumplimiento de la normativa de protección de datos no se acredite únicamente cuando existen situaciones que causan compromiso en el tratamiento de los datos, sino que desde que se comienzan a tratar los mismos, el responsable o encargado de tratamiento de los datos, esté en la obligación de adoptar todas las medidas necesarias para garantizar el tratamiento

adecuado y seguro de los mismos, condición que deberá ser capaz de acreditar en cualquier momento y no sólo cuando se encuentre en una situación en la que se cuestione la licitud o lealtad del tratamiento, por ejemplo.

Por medio de este enfoque, se pretende dar o al menos poder responder con mediana rapidez a los cambios constantes que nos traen los avances tecnológicos, pues sin que ello suponga una suplantación de la normativa jurídica, el responsable o encargado del tratamiento de datos personales debe estar la capacidad, en todo momento, de poder asegurar el cumplimiento de la normativa de protección de datos personales en cualquier situación o contexto.

Es decir, que si un responsable trata hoy día los datos personales de una manera que no supone un riesgo, pero el día de mañana, existe un avance tecnológico que permite mejorar la eficiencia en el tratamiento de estos datos, el responsable no debe esperar que se emitan las regulaciones necesarias para garantizar el cumplimiento de la normativa de protección de datos en ese nuevo contexto, sino que proactivamente debe adecuar protocolos, estructuras, etc., de manera que la vigencia de la normativa de protección de datos se garantice en ese nuevo panorama.

Junto con este cambio principal, existen otra serie de cambios importantes a nivel normativo y en los contenidos esenciales del derecho a la protección de datos personales, como lo son los nuevos requisitos para entender que se ha dado un consentimiento para el tratamiento de los datos, o los derechos reconocidos en el RGPD, que han sumado al catálogo ya existente, el derecho al olvido o el derecho a la portabilidad de los datos personales, entre otros.

No obstante lo anterior, el RGPD ha venido a realizar un aporte mínimo en lo que se refiere a la relación entre transparencia, acceso a la información y protección de datos personales, pues únicamente ha incluido una disposición muy breve en la que indica que cuando se pretenda el acceso a un documento público que contenga datos de carácter personal, deberán atenderse y tomarse en consideración los principios que rigen el derecho de acceso a la información pública. Esta disposición ya estaba contenida en al Directiva 95/46 dentro de sus considerandos y lo que ha hecho el RGPD ha sido incorporarla al articulado de la nueva normativa.

Sin perjuicio de esta breve inclusión en el texto normativo que no arroja muchas más luces de las que existen actualmente, las Administraciones Públicas verán afectadas

sus relaciones con los ciudadanos, en tanto el RGPD aplica, sin distinción alguna, a cualquier responsable o encargado de tratamiento de datos personales, lo que incluye como corresponde, a las Administraciones Públicas.

Esto incide directamente, sin duda alguna, en la relación entre transparencia, acceso a la información pública y protección de datos, así como las soluciones y conciliaciones que desde el TJUE en el ordenamiento comunitario y la LTAIBG y su interpretación por parte del CTBG y la AEPD se ha dado al tema.

A nivel comunitario, el TJUE ha llegado a conciliar este conflicto de derechos partiendo de que no se puede atribuir una primacía absoluta a ninguno de ellos -ni a la transparencia y el derecho de acceso a la información, ni a la protección de datos personales-, por lo que resulta necesario garantizar la plena vigencia de ambos. Sólo a través de una ponderación se puede decidir cuál de los derechos debe prevalecer en cada caso concreto, lo que a su criterio, y de conformidad con la normativa comunitaria vigente, pasa por la necesaria acreditación y justificación de la necesidad en el acceso.

El TJUE tiene una línea jurisprudencial sólida en la que ha reconocido que la ponderación, que es el mecanismo de solución que ha encontrado más adecuado para este conflicto de derechos, únicamente se puede llevar a cabo cuando se haya acreditado la necesidad en el acceso, pues sólo de esta forma se puede atribuir un peso al derecho de acceso a la información que permita ponerlo en una balanza frente al derecho a la protección de datos de carácter personal.

Esta posición adoptada el TJUE desde su primer sentencia –caso Bavarian Lager- y que ha repetido en todos los casos en que ha resuelto el conflicto entre transparencia, acceso a la información protección de datos personales ha sido ampliamente criticada. Por una parte, desde esa primera ocasión el SEPD y el Defensor del Pueblo Europeo vienen avisando que el derecho a la protección de datos de carácter personal no puede ser interpretado de forma que constituya un impedimento al acceso a la información, o bien, que permita entenderse que concede el derecho al anonimato en la gestión y participación de la actividad pública. La doctrina reprocha que se exija demostrar la necesidad en el acceso para poder llevar a cabo la ponderación, así como que en la práctica generalmente prevalece el derecho a la protección de datos personales.

Bajo la óptica del TJUE, la ponderación como mecanismo de solución en estos casos, requiere necesariamente que se acredite, o al menos alegue la necesidad en el

acceso, para que quien debe decidir cuál derecho prevalece, tenga en cuenta los elementos de juicio necesarios para poder llevar a cabo la ponderación de forma correcta.

Ahora bien, pese a la sólida jurisprudencia que tiene el TJUE en esta materia, es importante hacer mención a que estas decisiones en la medida en que se interprete el RGPD van a ser redefinidas. Asimismo, no puede obviarse que desde 2008 se está tramitando una propuesta de reforma al Reglamento 1049/2001 sobre acceso a la información pública, en la que justamente una de las cuestiones más debatidas es el alcance que debe contener una excepción al acceso a la información pública en razón de la protección de los datos de carácter personal, que sin duda, una vez aprobado, también dará una nueva dimensión a la interpretación y solución que ha dado hasta ahora en sus casos el TJUE.

Por su parte, en el ordenamiento comunitario español, si bien la solución que ha pretendido dar el legislador a esta problemática incorpora la ponderación en algunos casos, se ha establecido un mecanismo distinto a través de la LTAIBG, que ha venido a suponer un cambio radical en el ordenamiento jurídico español que no contaba, hasta ese entonces, con un verdadero derecho de acceso a la información pública.

A pesar de que la LTAIBG constituye un avance importante, debe tenerse en consideración que prefirió mantener el derecho de acceso a la información pública como un derecho de configuración legal, lo que claramente lo coloca de forma automática en una situación muy desventajosa frente al derecho a la protección de datos personales, que sí tiene reconocido vía jurisprudencia del TC, ese carácter iusfundamental.

A criterio de la doctrina mayoritaria, esta situación ha hecho que la LTAIBG se encuentre desde un primer momento desfasada, responda a un paradigma meramente administrativista y vaya muy por detrás de las legislaciones modernas y la jurisprudencia tanto del TEDH como de la Corte IDH, que le han reconocido al derecho al acceso a la información pública, un carácter de derecho fundamental por su evidente conexidad e integración en el derecho a la libertad de expresión y el derecho a recibir y difundir informaciones.

Los serios inconvenientes que podía suponer una desigualdad de este tipo no tardaron en salir a la luz y el ejemplo más claro de ello es el informe de la AEPD y el dictamen del Consejo de Estado, en el que fueron ampliamente enfáticos en que bajo ningún supuesto se podía pretender introducir limitaciones al derecho a la protección de

datos personales, contenido en una ley orgánica, por medio del derecho de acceso a la información pública, que, regulado en una ley ordinaria, es incapaz de afectar o limitar, el derecho a la protección de datos personales.

La LTAIBG, si bien recurre a la ponderación de derechos cuando se pretenda el acceso a información que contiene datos de carácter personal, creo una categorización a través del establecimiento de criterios normativos para poder llevar a cabo la conciliación entre transparencia, acceso a la información pública y protección de datos personales.

De forma que el artículo 15 de la LTAIBG, que contiene la excepción al acceso a la información en función de los datos personales prohíbe el tratamiento de datos especialmente protegidos y datos que se refieran a sanciones penales o infracciones administrativas, salvo que concurra alguno de los supuestos que permitan su tratamiento, como lo es el consentimiento del interesado, que exista una norma legal que lo autorice, o, que el titular de los datos los haya hecho manifiestamente públicos. Esto se encuentra en plena consonancia con lo dispuesto por la LOPD en relación con la categoría de datos especialmente protegidos.

La segunda categoría, viene a estar constituida por datos meramente identificativos que estén relacionados, con la organización, actividad y funcionamiento del órgano público. En relación de estos datos opera una presunción bajo la cual procede la entrega de la información, salvo que se demuestre que a través de la transmisión de tales datos se causa un perjuicio a algún derecho constitucionalmente reconocido y protegido.

La tercer categoría, son todos aquellos datos personales que figuren en la información pública y que no se encuentren comprendidos en las dos categorías ya mencionadas. Para determinar si procede o no el acceso a la información que los contiene, corresponde al órgano al que se dirige la solicitud hacer la ponderación respectiva. Esta solución, termina siendo en términos generales, similar a la que da el TJUE a través de su jurisprudencia.

Si bien la LTAIBG incorpora unos criterios objetivos que pretenden dar seguridad jurídica en la ponderación que se lleve a cabo (art. 15.3 de la LTAIBG), lo cierto es que los mismos son orientativos y no son los únicos que se pueden tener en consideración. En la práctica, en las resoluciones analizadas, en aquellos casos en que se ha recurrido a esta

ponderación, los mismos no han sido factores de peso o determinantes a la hora de resolver el acceso a la información que contiene los datos personales.

Es también importante rescatar que el artículo 15 de la LTAIBG confiere una potestad conjunta a la AEPD y al CTBG para que emitan criterios de interpretación conjunta de esta excepción de protección de los datos personales, que de igual forma permita dar una seguridad jurídica en su aplicación. Esta disposición actualmente ha dado lugar a la emisión de criterios de interpretación de la excepción en temas relevantes como el acceso a la información sobre relaciones de puestos de trabajo y retribuciones de funcionarios públicos, entre otros.

Por último, el artículo 15 de la LTAIBG, relativo a la excepción de datos de carácter personal, contiene dos cláusulas de cierre correspondientes a la disociación de datos personales y la obligatoria aplicación de la LOPD en los tratamientos posteriores de los datos personales que hayan sido obtenidos a través de las solicitudes de acceso a la información. Esta última cláusula ha sido una de las disposiciones más controversiales, pues puede llegar a hacer nugatorio el derecho de acceso a la información, si por ejemplo, para la difusión posterior de la información para contribuir a un debate público, se llevará a requerir del consentimiento del interesado o tendrá en último lugar que discutirse ante la AEPD la licitud del tratamiento de los datos para tales efectos y la procedencia de su difusión o transmisión.

En el plano práctico, la interpretación de este artículo la están llevando a cabo tanto el CTBG desde las atribuciones que le confirió la LTAIBG, pero también la AEPD desde el ámbito de sus competencias. Si bien a la fecha no existen posiciones contradictorias entre una agencia y la otra, si es fácilmente constatable la interpretación de cada una de ellas más proclive al derecho que les ha sido encomendado según corresponde: el CTBG es más proclive a tutelar el derecho de acceso a la información, mientras que la AEPD protege con mayor recelo el derecho a la protección de datos personales.

De forma general, tanto en el plano comunitario como en el ordenamiento jurídico doméstico, la solución entre transparencia, acceso a la información pública y protección de datos personales está en un continuo perfeccionamiento, así como los criterios y soluciones que se puedan dar a la misma.

Es innegable que el RGPD y su aplicación a partir de 2018 repercutirán en todos los aspectos en que corresponda atender la normativa de protección de datos personales, como lo puede resultar el acceso a la información pública que contenga datos de esta naturaleza. Será sólo con la aplicación de esta normativa y con la interpretación que den del ordenamiento comunitario los Estados miembros y posteriormente el TJUE que se podrá determinar la incidencia y especial repercusión del RGPD en la relación de la que nos hemos ocupado en este trabajo.

Tampoco debe perderse de vista la eventual aprobación de un nuevo reglamento en materia de acceso a la información pública en el ámbito comunitario, que eventualmente vendrá también a modular el conflicto que suscita el acceso a la información pública que contiene datos de carácter personal.

En el caso español, la solución que la LTAIBG se verá también modulada en razón de que avance la regulación a nivel comunitario y también conforme se vaya aplicando la LTAIBG por parte del CTBG, la AEPD y los tribunales, pues en el corto tiempo de vigencia que lleva, sacar conclusiones sobre la efectividad de la misma, especialmente cuando contiene disposiciones cuestionables como la de la aplicación de la LOPD a cualquier tratamiento posterior de los datos obtenidos a través de una solicitud de acceso, puede ser aventurado.

Bibliografía

AEPD (2017). La importancia de la información por capas en el Reglamento General de Protección de Datos. Recuperado de: http://www.agpd.es/blog/la-importancia-de-la-informacion-por-capas-en-el-reglamento-general-de-proteccion-de-datos-ides-idPhp.php

AEPD (2017). Qué es un delegado de protección de datos. Recuperado de: http://www.agpd.es/blog/que-es-un-delegado-de-proteccion-de-datos-ides-idPhp.php

AEPD (s.f.). El impacto del Reglamento General de Protección de Datos sobre la Actividad de las Administraciones Públicas. Recuperado de: http://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/Impacto_RGPD_en_AAPP.pdf

Adamski, D. (2014). Access to documents, accountability and the rule of law – do private watchdogs matter? *European Law Journal*. Vol. 20, núm. 4, julio 2014. pp. 520-543.

Aguado Renedo, C. (2010). La protección de los datos personales ante el Tribunal Constitucional español. *Revista Mexicana de Derecho Constitucional*, núm. 23, julio-diciembre 2010. pp. 3-25.

Albuquerque, L. (2007). Los ficheros de solvencia patrimonial y crédito: breves comentarios a su régimen jurídico. *Anuario de la Facultad de Derecho*, Vol. XXV, 2007. pp. 179-194.

Alhadeff et al (2012). The Accountability Principle in Data Protection Regulation: Origin, Development and Future Decisions. En D. Guagnin et al (Eds.), Managing Privacy Trough Accountability. Recuperado de: http://www.palgrave.com/us/book/9780230369320.

Álvarez Caro, M. (2016). El derecho a la supresión o al olvido. En J.L. Piñar Mañas (Dir.), *Reglamento General de Protección de Datos: hacia un nuevo modelo europeo de privacidad*. Madrid: Editorial Reus. pp. 241-256.

Arenas Ramiro, M. (2016). Transparencia, acceso a la información pública y democracia: elementos inseparables. *Transparencia y Sociedad*, núm. 4, 2016. pp. 113-131.

Arroyo Jiménez, L. (2009). Ponderación, proporcionalidad y Derecho administrativo. *Indret*: *Revista para el Análisis del Derecho,* núm. 2/2009. Recuperado de: www.indret.com

Atienza Rodríguez, M. (2010). A vueltas con la ponderación. *Anales de la Cátedra Francisco Suárez,* núm. 44. (2010). pp. 43-59.

Asduara Varela, B. (2016). El consentimiento. En J.L. Piñar Mañas (Dir.), *Reglamento General de Protección de Datos: hacia un nuevo modelo europeo de privacidad*. Madrid: Editorial Reus. pp. 151-167.

Augustyn, M.; Monda, C. (2011). Transparency and access to documents in the EU: ten years from the adoption of Regulation 1049/2001. *EIPAScope,* 2011 (1). pp. 17-20

Ballester Martínez, B. (2011). La forja jurisprudencial del principio de transparencia. *Teoría y Realidad Constitucional,* núm. 28, 2011. pp. 383-406.

Bazzocchi, V. (2011). The European Charter of Fundamental Rights and the Area of Freedom, Security and Justice. En G. Di Federico (Ed.), The EU Charter of Fundamental Rights: from declaration to binding instrument. Bruselas: Springer. pp. 177-197.

Blanke-H. (2012). The protection of fundamental rights in Europe. En H. Blanke; S. Magiameli (Eds.), The European Union after Lisbon: constitutional basis, economic order and external action. Bruselas: Springer. pp. 159-232.

Blume, P. (2014).The myths pertaining to the proposed General Data Protection Regulation. *International Data Privacy Law*, 2014. Vol. 4, núm. 4. pp. 269-273.

Boehm, F. (2012). Information Sharing and Data Protection in the Area of Freedom, Security and Justice. Towards Harmonized Data Protection Principles for Information Exchange at EU-level. Brusleas: Springer. p. 168.

Burgar Arquimbau, J. M. (2014). Aproximación a la protección de datos de carácter personal en el marco de Ley de transparencia, acceso a la información pública y buen gobierno. Revista Digital CEMCI, núm. 23, de abril a septiembre de 2014. Recuperado de: http://revista.cemci.org/numero-23/pdf/revista-cemci-numero-23.pdf

Buttarelli, G. (2016). One giant leap for digital rights. Recuperado de: https://edps.europa.eu/press-publications/press-news/blog/one-giant-leap-digital-rights_fr

(2016). The EU GDPR as a clarion call for a new global digital gold standard. *International Data Privacy Law*, 2016, Vol. 6, núm. 2. pp. 77-78.

Casas Baamonde, M. E. (2015). El derecho a la protección de datos de carácter personal en la jurisprudencia del Tribunal Constitucional. En AEPD, 20 años de protección de datos en España. Madrid: Agencia Española de Protección de Datos. pp. 91-126.

Canals Ametller, D. (2016). El acceso público a datos en un contexto de transparencia y buena regulación. En Dolores Canals Ametller (Ed.), Datos. Protección, Transparencia y Buena Regulación. Recuperado de: www.documentauniversitaria.com.

Cavoukian, A. (2009). Privacy by desing. Recuperado de: https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf.

(2010). *Implementation and mapping of fair information practices.* Recuperado de: https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-implement-7found-principles.pdf

(2015). Evolving FIPPs: *Proactive Approaches to Privacy,* Not Privacy Paternalism. En S. Gutwirth, R. Leenes y P. de Hert (Eds.), *Reforming European Data Protection Law. Law, Governance and Technology Series (20)*. Bruselas: Springer. pp.293-310.

Ciriani, S. (2015). The Economic Impact of the European Reform of Data Protection. *Digiworld Economic Journal*, núm. 97, 1st, Q. 2015. pp. 41-58.

Colombo, G. (2008). Sulle regole. Milano: Feltrinelli.

Cotino Hueso, L. (2016). Transparencia y derecho de acceso a los documentos en la Constitución europea y en la realidad de su ejercicio. En La Constitución Europea: actas del III Congreso Nacional de Constitucionalista de España. Tirant lo Blanc. pp.285-308.

(2014). La nueva ley de transparencia y acceso a la información. *Anuario de la Facultad de Derecho, Universidad de Alcalá*, núm. VII (2014). pp. 241-256.

De Hert, P.; Papakonstantinou, V. (2016). The new General Data Protection Regulation: still a sound system for the protection of individuals?. *Computer Law and Security Review*, Vol. 32, núm. 2. pp. 179-194.

De la Nuez Cascado, E. (2012). El proyecto de Ley de Transparencia, Acceso a la Información Pública y Buen Gobierno ¿Una ley gatopardesca? Recuperado de: http://hayderecho.com/2012/09/24/el-proyecto-de-ley-de-transparencia-acceso-a-la-informacion-publica-y-buen-gobierno-una-ley-gatopardesca/

De la Quadra-Salccedo y Fernández del Castillo, T. (2015). La primera ley española de protección de datos (LORTAD) y el proceso de su elaboración. En AEPD, 20 años de protección de datos en España. Madrid: Agencia Española de Protección de Datos. pp. 27-39.

De Vries, S. et al (2013). The protection of fundamental rights in the EU after Lisbon. Oxford: Hart Publishing.

Del Castillo Vásquez, I.C. (2007). Transparencia, acceso a la documentación administrativa y protección de datos de carácter personal. *Foro, Nueva época*, núm. 6/2007. pp. 231-254.

Duaso Caldés, R. (2016). Los principios de protección de datos desde el diseño y protección de datos por defecto. En J.L. Piñar Mañas (Dir.), *Reglamento General de Protección de Datos: hacia un nuevo modelo europeo de privacidad*. Madrid: Editorial Reus. pp. 295-320.

Fernández Pérez, A. (2016). La protección de los derechos fundamentales de los menores en internet desde la perspectiva europea. *Revista Ius et Praxis*, año 22, núm. 1, 2016. pp. 377-416.

Fernández Ramos, S. (2013). El acceso a la información en el proyecto de Ley de transparencia, acceso a la información pública y buen gobierno. *Monografías de la Revista Aragonesa de Administración Pública*, núm. XIV. pp. 233-298.

Fernández Vivas, Y. (2016). Debatiendo: La influencia de la Sentencia de la Corte Interamericana de Derechos Humanos "Claude Reyes contra Chile" en la jurisprudencia del Tribunal Europeo de Derechos Humanos. *Eunomía. Revista en Cultura de la Legalidad*, núm 9, octubre 2015-marzo 2016. pp. 321-333.

García Macho, R. (2012). La transparencia en el sector público. En A. Blasco Esteve, *El Derecho público de la crisis económica. Transparencia y sector público. Hacia un nuevo derecho administrativo. Actas del VI Congreso de la Asociación Española de Derecho Administrativo*. Madrid: INAP. Recuperado de: http://www.marcialpons.es/libros/el-derecho-publico-de-la-crisis-economica-transparencia-y-sector-publico-hacia-un-nuevo-derecho-administrativo/9788473514194/.

García Muñoz, O. (2017). La protección de los datos de carácter personal. En VV.AA, Los límites al Derecho de Acceso a la Información Pública. Madrid: INAP. Recuperado de: https://www.libreriavirtuali.com/inicio/Los-l%C3%ADmites-al-derecho-de-acceso-a-la-informaci%C3%B3n-p%C3%BAblica-p83707115.

Gianfrancesco, E. (2012). The Charter of Fundamental Rights of the Union as a source of law. En H. Blanke; S. Magiameli (Eds.), The European Union after Lisbon: constitutional basis, economic order and external action. Bruselas: Springer. pp. 295-310.

Gil Antón, A.M. (2013). El derecho a la propia imagen del menor en internet. Madrid: Dykinson.

(2015). El menor y la tutela de su entorno virtual a la luz de la reforma del Código Penal LO 1/2015. *Revista de Derecho UNED*, núm. 16. pp. 275-319.

Goig Martínez, J.M. (2015). Transparencia y corrupción. La percepción social ante comportamientos corruptos. *Revista de Derecho UNED*, núm. 17, 2015. pp. 73-107.

Gómez Sánchez, Y. (2008). La protección de los datos genéticos: el derecho a la autodeterminación informativa. *DS: Derecho y salud*, núm. 16. pp. 59-78.

Gómez-Juárez Sidera, I. ((2015). Hacia un nuevo derecho de protección de datos para las personas especialmente vulnerables en la sociedad digital del Siglo XXI: los niños y las personas mayores. *Revista CESCO de Derecho de Consumo*, núm. 14/2015. pp. 217-240.

González Fuster, G. (2009). TEDH – Sentencia de 04.12.2008, S. y Marper c. Reino Unido, 30562/04 y 30566/04 – Artículo 8 CEDH – Vida privada – Injerencia en una sociedad democrática – Los límites del tratamiento de datos biométricos de personas no condenadas. *Revista de Derecho Comunitario Europeo*, núm. 33, Madrid, mayo/agosto (2009). pp. 619-633.

González Pascual, M. (2014). El TJUE como garante de los derechos en la UE a la luz de la sentencia Digital Rights Ireland. *Revista de Derecho Comunitario Europeo*, núm. 49, Madrid, septiembre/diciembre (2014). pp. 943-971.

Guasch Portas, V.; Soler Fuensanta, J.R. (2015). El interés legítimo en la protección de datos. *Revista de Derecho UNED*, núm. 16. pp. 417-438.

Guerrero Picó, M.C. (2005). El derecho fundamental a la protección de datos de carácter personal en la Constitución Europea. *ReDCE*, núm. 4, julio-diciembre de 2005. pp. 293-332

Guichot Reina, E. (2003). El nuevo derecho europeo de acceso a la información pública. *Revista de Administraciones Públicas*, núm. 160, Enero-abril 2003. pp. 283-315

(2007). Derecho a la privacidad, transparencia y eficacia administrativa: un difícil y necesario equilibrio. *Revista catalana de dret públic*, núm. 35, 2007. pp.43-74.

(2010). Comunicación de datos por las Administraciones Públicas a Sujetos Privados. En A. Troncoso Reigada (Dir.) Comentario a la Ley Orgánica de Protección de Datos de Carácter personal. Pamplona: Aranzadi. pp. 1024-1056

(2011). Transparencia y acceso a la información pública en España: análisis y propuestas legislativas. Documento de trabajo 170/2011. Recuperado de: http://www.fundacionalternativas.org/

(2011). Las relaciones entre transparencia y privacidad en el Derecho comunitario ante la reforma de la normativa sobre acceso a los documentos públicos. *Revista Española de Derecho Europeo*, núm. 37, Enero-Marzo, 2011. pp. 37-69.

(2011). Transparencia versus protección de datos. Ponencia impartida en el VI Congreso Anual de la Asociación Española de Profesores de Derecho Administrativo. Palma de Mallorca, 12 de febrero 2011.

(2012). El proyecto de Ley de Transparencia y acceso a la información pública y el margen de actuación de las Comunidades Autónomas. *Revista Andaluza de Administración Pública*, núm. 84, Sevilla, septiembre-diciembre (2012). pp. 89-134.

(2014). La nueva Ley de Transparencia, un reto para la gestión de las organizaciones públicas. *Revista Vasca de Gestión de Personas y Organizaciones Públicas*, núm. 6/2014. pp. 94-107

(2014). Límites a la transparencia y el acceso a la información. En E. Guichot Reina (Coord.). Transparencia, Acceso a la Información Pública y Buen Gobierno. Estudio de la Ley 19/2013, de 9 de diciembre. Madrid: Tecnos. pp. 97-142.

Hempel, L.; Lammerant, H. (2015). En S. Gutwirth, R. Leenes y P. de Hert (Eds.) *Reforming European Data Protection Law. Law, Governance and Technology Series (20)*. Bruselas: Springer. pp. 125-146.

Hernández Corchete, J.A. (2016). Transparencia en la información al interesado del tratamiento de sus datos personales y en el ejercicio de sus derechos. En Piñar Mañas, J.L. (Dir.) *Reglamento General de Protección de Datos: hacia un nuevo modelo europeo de privacidad*. Madrid: Editorial Reus. pp. 205-226.

Hijmans, H. (2016). The European Union as guardian of internet privacy: the story of art 16 TFUE. Law, Governance and Technology Series (Vol. 31). Bruselas: Springer.

Jiménez Asensio, R. (____). El Proyecto de Ley de Transparencia, Acceso a la Información y buen Gobierno: su posible impacto sobre los Gobiernos Locales. Recuperado de: https://www.gobiernolocal.org/historicoBoletines/nueva_web/RJA.pdf

Kiss, A.; Szoke, G.L. (2015). Evolution or Revolution? Steps Forward to a new Generation of Data Protecion. En S. Gutwirth, R. Leenes y P. de Hert (Eds.), *Reforming*

European Data Protection Law. Law, Governance and Technology Series (20). Bruselas: Springer. pp. 311-332.

Komanovics, A. (2010). Transparent Europe? The Council of Europe Convention on Access to Official Documents. *Boletín JADO,* Bilbao, año VIII, núm. 19, mayo, 2010. pp. 141-170.

Korenhonf et al (2015) Timing the right to be forgotten, a study into "time" as a factor in deciding about retention or erasure of data. En S. Gutwirth, R. Leenes y P. de Hert (Eds.), *Reforming European Data Protection Law. Law, Governance and Technology Series (20)*. Bruselas: Springer. pp.171-201.

Lynskey, O. (2014). Deconstructing data protection: the 'added-value' or a right to data protection in the EU legal order. *The International and Comparative Law Quarterly*, 63(3). pp. 569-597.

Lucas Murillo de la Cueva, P. (1999). La construcción del derecho a la autodeterminación informativa. *Revista de Estudios Políticos (Nueva época),* núm. 104. Abril-Junio 1999. pp. 35-60.

(2007). Perspectivas del derecho a la autodeterminación informativa. *Monográfico "III Congreso Internet, Derecho y Política (IDP). Nuevas Perspectivas"*, *IDP*, núm. 5 (2007). pp. 18-32.

(2008). El derecho a la autodeterminación informativa y la protección de datos personales. *Azpilcueta*, núm. 20, 2008. pp. 43-58.

(2009). La protección de los datos de carácter personal en el horizonte de 2010. *Anuario Facultad de Derecho – Universidad de Alcalá*, (2009). pp. 131-142.

(2010). El objeto de la Ley Orgánica de Protección de Datos de Carácter Personal. En A. Troncoso Reigada (Dir.), Comentario a la Ley Orgánica de Protección de Datos de Carácter personal. Pamplona: Aranzadi. pp. 75-96.

Martínez Capdevila, C. (2005). La transparencia en la Unión Europea. *Cuadernos de derecho público*, núm. 26 (septiembre -diciembre 2005). pp. 169-193.

Martín Delgado, I. (2016). La reclamación ante el Consejo de Transparencia y Buen Gobierno. Un instrumento necesario, útil y ¿eficaz? En F. López Ramón (Coord.), Las vías administrativas de recurso a debate: Actas del XI Congreso de la Asociación Española de Profesores de Derecho Administrativo, Zaragoza, 5 y 6 de febrero de 2016. Madrid: INAP pp. 291-328.

Martínez Martínez, R. (2007). El derecho fundamental a la protección de datos: perspectivas. *Monográfico "III Congreso Internet, Derecho y Política (IDP). Nuevas perspectivas". Revista de Internet Derecho y Política, n*úm. 5 (2007). pp. 47-61.

Matia Portilla, E. (2017). Derecho a la información de los representantes políticos, protección de datos y transparencia. *Revista Jurídica de Castilla y León. Revista jurídica de Castilla y León, núm.* 42, mayo 2017. Recuperado de: http://www.jcyl.es/web/jcyl/AdministracionPublica/es/Plantilla100/1131978346397/_/_/_

Meseguer Yebra, J. (2014). El procedimiento administrativo para el ejercicio del derecho al acceso a la información pública. *Revista Jurídica de Castilla y León. Revista jurídica de Castilla y León,* núm. 33, mayo 2014. Recuperado de: http://www.jcyl.es/web/jcyl/AdministracionPublica/es/Plantilla100Detalle/1215245063566/_/1284319275652/Redaccion

McDonagh, M. (2012). Balancing disclosure of information and the right to respect for private life in Europe. *Journal of Internet Law*. September, 2012. pp. 3- 17

Minero Alejandre, G. (2017). Presente y futuro de la protección de datos personales. Análisis normativo y jurisprudencial desde una perspectiva nacional y europea. *Anuario Jurídico y Económico Escurialense,* L (2017). pp. 13-58.

Moretón Toquero, A. (2014). Los límites del derecho de acceso a la información pública. *Revista jurídica de Castilla y León, núm.* 33, mayo 2014. Recuperado de: http://www.jcyl.es/web/jcyl/AdministracionPublica/es/Plantilla100Detalle/1215245063566/_/1284319275652/Redaccion

Nieto Garrido, E. (2014). Transparencia y acceso a los documentos *versus* el derecho a la protección de datos de carácter personal en la reciente jurisprudencia de TJUE. En Piñar

Mañas, J. L. (Dir.), *Transparencia, acceso a la información y protección de datos*. Madrid: Editorial Reus. pp. 63-96.

Olmedo Palacios, M. (2014). La Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información y buen gobierno. Diario La Ley, (8327).

Ordóñez Solís, D. (2011). Privacidad y protección judicial de los datos personales. Barcelona: Bosch.

Pavón Pérez, J.A. (2002). La protección de datos personales en el Consejo de Europa: el Protocolo Adicional al Convenio 108 relativo a las autoridades de control y a los flujos transfronterizos de datos personales. *Anuario de la Facultad de Derecho*, núm. 19-20, 2001-2002, pp. 235-252.

Pauner Chulvi, C. (2015). La libertad de información como límite al derecho a la protección de datos personales: la excepción periodística. *Teoría y Realidad Constitucional*, núm. 36, 2015. pp. 377-395.

Pazos Castro, R. (2015). EL mal llamado "derecho al olvido" en la era de Internet. *Boletín del Ministerio de Justicia*, año LXIX, núm. 2183, noviembre de 2015.

Pecsteen, E. (2015). Public Access to documents: effective rear guard to a transparent EU? Recuperado de: https://europeanlawblog.eu/2015/12/30/public-access-to-documents-effective-rear-guard-to-a-transparent-eu/

Pérez Carrillo, E. (2000). La transparencia en el funcionamiento de la Unión Europea: el acceso público a los documentos de sus instituciones y órganos. *Revista Vasca de Administración Pública*, núm. 56, enero-abril, 2000. pp. 349-387.

Pérez Luño, A.E. (2009). La protección de los datos personales del menor en Internet. *Anuario Facultad de Derecho, Universidad de Alcalá*, 2009. pp. 143-175.

Piñar Real, A. (2016). Tratamiento de datos de menores de edad. En J.L. Piñar Mañas (Dir.), *Reglamento General de Protección de Datos: hacia un nuevo modelo europeo de privacidad*. Madrid: Editorial Reus. pp. 187-203.

Piñar Mañas, J.L. (2009). Seguridad, transparencia y protección de datos: el futuro de un necesario e incierto equilibrio. Madrid: Fundación Alternativas.

(2014). Transparencia y protección de datos. Una referencia a la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información y buen gobierno. En J.L. Piñar Mañas (Dir.), Transparencia, acceso a la información y protección de datos. Madrid: Editorial Reus. pp. 45.-57.

(2014). Transparencia y derecho de acceso a la información pública. Algunas reflexiones en torno al derecho de acceso en la Ley 19/2013, de transparencia, acceso a la información y buen gobierno. *Revista catalana de dret públic*, núm 40 (diciembre 2014). pp. 1-19.

Pollicino, O.; Bassini, M. (2013). Diritto all'oblio: I piu recenti spunti riconstruttivi nella dimensione comparada ed europea. En F. Pizzetti (Coord.) Il caso del diritto all'oblio. ____: Giappichelli. pp. 186-228.

Poullet, Y. (2011). Internet et Sciences Humaines ou "Comment comprendre l'invisible? *Revue des Questions Scientifiques*, 2011, 184(4). pp. 377-398.

Prado Falcón, J. (2008). La protección de datos personales. En M.E. Casas Baamonde y M. Rodríguez-Piñero y Bravo-Ferrer (Dir.) Comentarios a la Constitución Española. Madrid: Fundación Wolters Kluwer. pp. 456-459.

Prieto Gutiérrez, J. M. (2004). Objeto y naturaleza jurídica del derecho fundamental a la protección de datos personales. *Boletín del Ministerio de Justicia.* Año 58, núm. 1973, 2004. pp. 3317-3337.

Robinson, N. et al (2009). Review of the European Data Protection Directive. Recuperado de:
http://www.rand.org/content/dam/rand/pubs/technical_reports/2009/RAND_TR710.pdf

Rallo Lombarte, A. (2009). La protección de datos en España. Análisis de actualidad. *Anuario Facultad de Derecho – Universidad de Alcalá* (2009). pp. 15-30.

(2012). Hacia un nuevo sistema europeo de protección de datos: las claves de la reforma. *UNED. Revista de Derecho Político,* núm. 85, septiembre-diciembre 2012. pp. 13-56.

Rams Ramos, L. (2016). Tratamiento y acceso público a documentos oficiales. En J.L. Piñar Mañas (Dir.), *Reglamento General de Protección de Datos: hacia un nuevo modelo europeo de privacidad*. Madrid: Editorial Reus. pp. 601-619.

Razquin Lizarraga, M.M. (2015). El derecho de acceso a la información pública. Teoría y práctica, en especial, para las entidades locales. Oñati: Instituto Vasco de Administración Pública.

Rodríguez Álvarez, J.L. (2016). Transparencia y protección de datos personales: criterios legales de conciliación. En D. Canals Ametler (Ed.), *Datos. Protección, Transparencia y Buena Regulación.* Recuperado de: www.documentauniversitaria.com

Rodríguez Boente, S.E. (2003). Ponderación y "reglas" de derechos fundamentales: dos enemigos conciliables. *Dereito,* Vol. 12, núm. 2. pp. 137-160.

Rodríguez de Santiago, J.M. (2000). La ponderación de bienes e intereses en el derecho administrativo. Madrid: Marcial Pons.

Rodríguez-Izquierdo Serrano, M. (2015). El Tribunal de Justicia y los derechos en la sociedad de la información: privacidad y protección de datos frente a las libertades informativas. *ReDCE,* núm. 24. Julio-Diciembre de 2015. Recuperado de: http://www.ugr.es/~redce/REDCE24/articulos/10_RODRIGUEZ_IZQUIERDO.htm#uno

Rollnert Liern, G. (2014). El derecho de acceso a la información pública como derecho fundamental: una valoración del debate doctrinal a propósito de la Ley de transparencia. Teoría y Realidad Constitucional. UNED, núm. 34, 2014. pp. 349-368.

(2014). La justiciabilidad del derecho de acceso a la información pública ante el Tribunal Constitucional. XII Congreso de la Asociación de Constitucionalistas de España, "Participación, representación y democracia", Salamanca, 3 y4 de abril de 2014.

Ruiz Miguel, C. (1994). En torno a la protección de los datos personales automatizados. *Revista de estudios políticos,* núm. 84, pp. 273-264.

(2003). El derecho a la protección de los datos personales en la Carta de Derechos Fundamentales de la Unión Europea: análisis crítico. *Revista de*

Derecho Comunitario Europeo, Año 7, núm. 14, enero-abril 2003. pp. 7-43

Sánchez de Diego Fernández de la Riva, M. (2014) Transparencia y acceso a la información desde una perspectiva constitucional. *Iurisprudentia Elegans: Revista de Derecho Político e Historia Constitucional*, núm. 1, 2014. pp. 30-55.

(2014). El "día después" de la Ley de Transparencia. *Revista jurídica de Castilla y León,* núm. 33, Mayo de 2014. Recuperado de:http://www.jcyl.es/web/jcyl/AdministracionPublica/es/Plantilla100Detalle/1215245063566/_/1284319275652/Redaccion

Sánchez Morón, M. (2011). Derecho administrativo: parte general. Madrid: Tecnos

Sendín García, M.A. (2014). El Consejo de Transparencia y Buen Gobierno. *Revista jurídica de Castilla y León,* núm. 33. Mayo de 2014. Recuperado de:http://www.jcyl.es/web/jcyl/AdministracionPublica/es/Plantilla100Detalle/1215245063566/_/1284319275652/Redaccion

SEPD (2005). Public access to documents and data protection, Background Paper Series N° 1. Recuperado de: https://edps.europa.eu/

(2011). Public access to documents containing personal data after the Bavarian Lager ruling. Recuperado de: https://edps.europa.eu/

(2015). Opinion 3/2015: Europe's big opportunity. EDPS recommendations on the EU's options for data protection reform. Recuperado de: https://edps.europa.eu/

Serrano Pérez, M.M. (2003). El derecho fundamental a la protección de datos. Derecho español y comparado. Madrid: Thomson Civitas.

(2005). El derecho fundamental a la protección de datos. Su contenido esencial. *Nuevas Políticas Públicas: Anuario multidisciplinar para la modernización de las Administraciones Púbicas*, núm. 1, 2005. pp. 245-265.

Sommermann, K. (2010). La exigencia de una administración transparente en la perspectiva de los principios de democracia y del Estado de Derecho. En R. García Macho

(Ed.), Derecho administrativo de la información y administración transparente. Madrid: Marcial Pons. pp. 11-26.

Subiza Pérez, I.; Arias Pou, M. (2009). La protección de datos y sus mundos. Pamplona: DAPP Publicaciones Jurídicas.

Tejedor Bielsa, J. C. (2014). A la búsqueda del equilibrio entre transparencia administrativa y protección de datos. Primeros desarrollos en el ámbito municipal. *Gestión y Análisis de Políticas Públicas. Nueva Época, núm. 12 julio-diciembre 2014.* Recuperado de: https://revistasonline.inap.es/index.php?journal=GAPP&page=article&op=view&path%5B%5D=10205&path%5B%5D=10687

Trepte, S. et al. (2015). Do people know about privacy and data protection strategies? Towards the "online privacy literacy scale" (OPLIS). En S. Gutwirth, R. Leenes y P. de Hert (Eds.), *Reforming European Data Protection Law. Law, Governance and Technology Series (20)*. Bruselas: Springer. pp. 333-365.

Troncoso Reigada, A. (2016). Los límites al acceso a la información: la protección de datos personales. *Revista Iberoamericana de Derecho Informático (Segunda Época)*, *Fundación Iberoamericana de Asociaciones de Derecho e Informática*, año 1, núm. 1, 2016. pp. 45-53.

Tzanou, M. (2013). Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right. *International Data Privacy Law*, 2013, Vol. 3, núm. 2. pp. 88-99.

Uría Gavilán, E. (2016) Derechos fundamentales versus vigilancia masiva. *Revista de Derecho Comunitario Europeo*, 53. pp. 261-282.

Villaverde Menéndez, I. (2004). La resolución de conflictos entre derechos fundamentales. El principio de proporcionalidad. En F. Bastida Frejiedo (Ed.) Teoría general de los derechos fundamentales en la Constitución española de 1978. Madrid: Tecnos. pp. 175-187.

(2006). La jurisprudencia del Tribunal Constitucional sobre el derecho fundamental a la protección de datos de carácter personal. En A. Farriols

i Solá (Coord.), La protección de datos de carácter personal en los centros de trabajo. Madrid: Cinca: Fundación Francisco Largo Caballero. pp. 48-63.

Voss, W. G. (2017). European Union data privacy law reform: General data protection regulation, privacy shield, and the right to delisting. *The Business Lawyer, 72*(1). pp. 221-233. Recuperado de: https://search.proquest.com/docview/1861788438?accountid=14478

WP 29 (2012). Opinion 3/2012 on developments in biometric technologies. Recuperado de: ec.europa.eu/justice/data-protection/.../opinion.../wp193_en.pdf

- **Documentos de las instituciones comunitarias:**

Conclusiones de la Presidencia, Consejo Europeo de Edimburgo de 11-12 de diciembre de 1992 (EC 12-1992)

Comunicación de 5 de marzo de 1993, *Mayor transparencia en el trabajo de la Comisión*, DOCE C 63/8

Comunicación al Consejo, al Parlamento Europeo y al Comité Económico y Social, de 8 de junio de 1993, *Acceso a los ciudadanos a los documentos de la instituciones*, DOCE C156/5

Comunicación al Consejo, al Parlamento y al Comité Económico y Social, *Transparencia en la comunidad.* COM (1993) 258 final

Conclusiones de la Presidencia, Consejo Europeo de Copenhague de 21-22 de junio de 1993 (Doc. SN 180/93

Conclusiones de la Presidencia, Consejo Europeo de Cardiff de 15 y 16 de junio de 1998, apartado 28-31. (Doc. SN 150/1/98 REV 1)

Conclusiones de la Presidencia, Consejo Europeo de Köln de 3 y 4 de junio de 1999 (Doc. 9064/99)

Resolución del Parlamento Europeo sobre el Informe Especial al Parlamento Europeo como continuación del proyecto de recomendación remitido a la Comisión Europea en la

reclamación 713/98/IJH (redactado de conformidad con el apartado 7 del artículo 3 del Estatuto del Defensor del Pueblo Europeo) (C5-0463/2001 – 2001/2194(COS)), de 11 de diciembre de 2001

Recomendación 509/1968 de 31 de enero, de la Asamblea del Consejo de Europa

- **Sentencias TEDH**

STEDH de 26 de marzo de 1987, caso Leander c. Suecia (rec. núm. 9248/81)

STEDH de 25 de febrero de 1997, caso Z. c. Finlandia (rec. núm. 9/1996)

STEDH de 4 de diciembre de 2008, caso S. y Marper c. Reino Unido (rec. núm. 30562/04 y 30566/04)

STEDH de 14 de abril de 2009, caso Táraság a Szabadságjogokért c. Hungría

STEDH de 26 de mayo de 2009, caso Kenedi c. Hungría

STEDH de 2 de septiembre de 2010, caso Uzun c. Alemania (rec. núm. 35623/05)

STEDH de 25 de junio de 2013, caso Youth Initiative for Human Rights c. Serbia

STEDH de 12 de enero de 2016, caso Szabó y Vissy c. Hungría (rec. núm. 37138/14)

STEDH de 08 de noviembre de 2016, caso Magyan Helsinki Bizottság c. Hungría

- **Sentencias Corte IDH**

Caso Claude Reyes y otros vs. Chile. Sentencia de 19 de septiembre de 2016

- **Sentencias TJUE**

STPI (Sala Cuarta) de 7 de febrero de 2002, asunto T-211/00 (caso Kuijer/Consejo)

STJCE de 20 de mayo de 2003, asuntos C-465/00, C-128/01 y C-139/01 (caso Österreichischer Rundfunk y otros)

STJCE de 6 de noviembre de 2003, asunto C-101/01 (caso Lindqvist)

STPI (Sala Quinta) de 23 de noviembre de 2004, asunto T-84/03 (caso Turco/Consejo)

STPI (Sala Quinta ampliada) de 30 de noviembre de 2004, asunto T-168/02 (caso IFAW Internationaler Tierschtz-Fonds/Comisión

STGUE (Sala Segunda), de 30 de mayo de 2006, asunto T-198/03, (caso Bank Austria Creditanstalt/Comisión)

STPI (Sala Tercera) de 6 de julio de 2006, asuntos T-391/03 y T-70/04 (caso Franchet y Byk/Comisión)

STGUE (Sala Segunda) de 12 de septiembre de 2007, asunto T-259/03 (caso Nikolaou/Comisión)

STJCE (Gran Sala) de 29 de enero de 2008, asunto C-275/06, (caso Promusicae)

STJCE (Gran Sala) de 16 de diciembre de 2008, asunto C-524/06 (caso Huber)

STJCE (Gran Sala) de 16 de diciembre de 2008, asunto C-73/07 (caso Satakunnan Markkinapörssi y Satamedia)

STJUE (Gran Sala) de 29 de junio de 2010, asunto C-28/08 P (caso Comisión/Bavarian Lager)

STJUE (Sala Tercera) de 7 de mayo de 2009, asunto C-553/07 (caso Rijkeboer)

STJUE (Gran Sala) de 9 de marzo de 2010, asunto C-518/07 (caso Comisión/Alemania)

STJUE (Gran Sala) de 09 de noviembre de 2010, asuntos C-92/09 y C-93/09 (caso Volker und Markus Schecke y Eifert)

STGUE (Sala Octava) de 07 de julio de 2011, asunto T-161/04 (caso Valero Jordana/Comisión)

STGUE (Sala Segunda) de 23 de noviembre de 2011, asunto T-82/09 (caso Dennekamp/Parlamento)

STJUE (Sala Tercera) de 24 de noviembre de 2011, C-468/10 y C-469/10 (caso ASNEF)

STJUE (Sala Tercera) de 24 de noviembre de 2011, asunto C-70/10 (caso Scarlet)

STJUE (Gran Sala) de 8 de abril de 2014, asunto C-288/12 (caso Comisión/Hungría)

STJUE (Gran Sala) de 16 de octubre de 2012, asunto C-614/10 (caso Comisión/Austria)

STJUE (Sala Tercera) de 19 de abril de 2012, asunto C-461/10 (caso Bonnier)

[1] STJUE (Sala Tercera) de 22 de noviembre de 2012, asunto C-119/12 (caso Probst)

STJUE (Sala Tercera) de 30 de mayo de 2013, asunto C-342/12, (caso Worten)

STJUE (Sala Cuarta) de 17 de octubre de 2013, asunto C-291/12 (caso Schwartz)

STJUE (Sala Octava) de 12 de diciembre de 2013, asunto C-486/12 (caso X)

STJUE (Gran Sala) de 8 de abril de 2014, asuntos C-293/12 y C-594/12 (caso Digital Rights Ireland y Seitlinger y otros)

STJUE (Gran Sala) de 13 de mayo de 2014, asunto C-131/12 (caso Google)

STJUE (Sala Tercera) de 17 de julio de 2014, asunto C-141/12 (caso YS y otros)

STJUE (Sala Cuarta) de 11 de diciembre de 2014, asunto C-212/13 (caso Rynes)

STGUE (Sala Quinta) de 11 de junio de 2015, asunto T-496/13 (caso McCullough/CEDEFOP)

STGUE (Sala Quinta) de 15 de julio de 2015, asunto T-115/13 (caso Dennekamp/Parlamento)

STJUE (Sala Segunda) de 16 de julio de 2015, asunto C-615/14 P (caso ClientEarth y PAN Europe/EFSA)

STJUE (Sala Tercera) de 1 de octubre de 2015, asunto C-201/14, (caso Bara)

STJUE (Sala Tercera) de 1 de octubre de 2015, C-230/14 (caso Weltimmo)

STJUE (Gran Sala) de 6 de octubre de 2015, asunto C-362/14 (caso Schrems)

STJUE (Sala Segunda) de 19 de octubre de 2016, asunto C-582/14 (caso Breyer)

STJUE (Gran Sala) de 21 de diciembre de 2016, asuntos C-203/15 y C-698/15 (caso Tele2Sverige)

- **Sentencias del TC**

STC 161/1988, de 20 de septiembre

STC 254/1993, de 18 de agosto

STC 143/1994, de 9 de mayo

STC 11/1998, de 13 de enero

STC 144/1999, de 22 de julio

STC 202/1999, de 8 de noviembre

STC 290/2000, de 4 de enero

STC 292/2000, de 4 de enero

- **STS**

STS 4291/2012, de 19 de junio

STS 3886/2012, de 29 de mayo

- **SAN**

SAN, de 17 de abril de 2017

- **Sentencias del Juzgado Central Contencioso-Administrativo de Madrid**

Sentencia 162/2016, de 2 de diciembre

Sentencia 138/2016, de 17 de octubre

- **Informes de la AEPD**

Informe 0390/2013, sobre transmisión de datos identificativos del titular de una licencia municipal de obras a terceros

Informe 0178/2014, relacionado con la aplicación de la LTAIBG y su conciliación con la LOPD

Informe 0502/2014, sobre inclusión de firmas manuscritas en documentos escaneados

Informe 12155/2016, sobre acceso a la información sobre personas que ocupan cada plaza de la RPT

Informe 0160/2016, sobre aplicación de la LOPD a tratamientos posteriores de datos

- **Informes conjuntos de la AEPD y el CTBG**

Informe conjunto de 1/2015 de 23 de marzo

Criterio Interpretativo CI/001/2014, de 24 de junio, sobre RPT, y retribuciones de empleados o funcionarios

Criterio Interpretativo CI/002/2015, de 24 de junio, sobre aplicación de los límites al derecho de acceso a la información

Criterio Interpretativo CI/004/2015, de 23 de julio, sobre publicidad activa de los datos del DNI y de la firma manuscrita

Criterio Interpretativo CI/002/2016, de 5 de julio, sobre información relativa a las agendas de los responsables públicos

- **Sitios web consultados:**

Agencia Española de Protección de Datos: http://www.consejodetransparencia.es/

Consejo de Transparencia y Buen Gobierno: http://www.consejodetransparencia.es

Corte Interamericana de Derechos Humanos: www.corteidh.or.cr/

Grupo de Trabajo del Artículo 29: http://ec.europa.eu/

Supervisor Europeo de Protección de Datos: https://edps.europa.eu/

Tribunal de Justicia de la Unión Europea: https://curia.europa.eu/

Tribunal Europeo de Derechos Humanos: http://www.echr.coe.int/