SEMINARIO

"TRANSPARENCIA Y DERECHO DE ACCESO A LA INFORMACIÓN PÚBLICA DE LA ACTIVIDAD DE LOS TRIBUNALES CONSTITUCIONALES"

Cartagena de Indias (Colombia), 16 a 19 de julio de 2024

Ponencia V: El derecho fundamental a la protección de datos como límite al derecho de acceso a la información pública.

Dra. Anabelén Casares Marcos

Letrada del Tribunal Constitucional de España

I. La transformación digital en marcha.

1. El contexto social.

La fiebre informática que caracteriza a nuestra sociedad contemporánea, hiperconectada en el espacio virtual, conlleva un grave riesgo para algunos de los derechos fundamentales más importantes que reconocen el Tratado de Funcionamiento y la Carta de los Derechos Fundamentales de la Unión Europea, así como los textos constitucionales de sus Estados miembros, en particular, la Constitución española de 1978.

No en vano, la denominada *sociedad de la información* está marcada por una constante renovación como consecuencia de la auténtica revolución tecnológica experimentada al respecto desde la segunda mitad del siglo XX, que ha llevado, incluso, a debatir si debe considerarse la etiqueta superada y sustituida por la de sociedad del conocimiento[1]. Este último no consiste en el mero acceso e intercambio de información y datos, sino que supone partir de la información para estructurarla en representaciones integradas, relevantes, dirigidas a interpretar hechos y datos, dentro de un contexto y a través de esquemas y modelos, a fin de explicar, de prever. Se trata, en suma, de aprovechar la información inicial para una acción efectiva o reflexión ulterior[2]. En esta línea, la reciente Comunicación de la Comisión, *Configurar el futuro digital de Europa*, sostiene rotundamente que "las tecnologías digitales están cambiando profundamente nuestra vida cotidiana y nuestra forma de trabajar y hacer negocios, así como la manera en que viajamos, nos comunicamos y nos relacionamos. La comunicación digital, la interacción a través de las redes sociales, el comercio electrónico y las empresas digitales están modificando continuamente nuestro mundo. Generan un volumen cada vez mayor de datos que, si se ponen en común y se utilizan, pueden generar medios y niveles de

[1] Así, Toniatti, (1991: 141) considera decaída la expresión inicialmente citada a favor, en cambio, de la de "sociedad informática". Da noticia de la transformación y constante regeneración de la expresión, Bello Paredes (2005: 140).
[2] Vid. Castelfranchi (2007: 3).

creación de valor completamente nuevos. Se trata de una transformación tan fundamental como la causada por la revolución industrial."[3]

Ya en enero de 2013, el Consejo para la Agenda Global del Foro de Davos (GAC en sus siglas inglesas) afirmaba lapidariamente que internet era el sistema adaptativo complejo más grande y de más rápida evolución en la Historia de la Humanidad. Cuatro grandes cambios han marcado su evolución, contribuyendo a alumbrar y consolidar de manera simultánea el Derecho de internet. En primer lugar, el aumento del número y la diversidad de usuarios desde un pequeño grupo de científicos e investigadores a una base de usuarios más grande, más diversa y de menor sofisticación tecnológica. Difícilmente puede ser de otro modo cuando más 66% de la población mundial utiliza internet hoy en día[4]. Este crecimiento exponencial del número de usuarios ha acelerado su transformación en un medio absolutamente vital para todas las facetas y vertientes del mundo actual. A partir de aquí se explica también, lógicamente, el surgimiento y el propio desarrollo de las distintas ramas del Derecho de internet. Destaca, asimismo, en segundo lugar, el crecimiento en la diversidad y la intensidad de las aplicaciones empleadas, desde las que utilizan ancho de banda de baja intensidad a otras que precisan ahora, en cambio, anchos superiores para su uso. Se abre y promueve con ello el debate sobre la llamada calidad del servicio. Una tercera transformación ha venido marcada, a su vez, por el desarrollo de una mayor variedad de tecnologías para acceder a internet y por un vertiginoso incremento en el número y tipo de dispositivos conectados a la red. Por último, corolario lógico de cuanto antecede, cabe destacar también la importante eclosión en torno a internet de nuevos tipos de relaciones comerciales y de negocio mucho más complejas y diversas.

La innovación constante y el desarrollo imparable del sector continúan alumbrando, en todo caso, importantes novedades tecnológicas. Cabe citar así, sin ánimo exhaustivo, los retos abiertos por el *Internet of Things* (IoT), la *Augmented Reality* (AR), el *Cloud* o el *Edge Computing*, el despliegue de la 5G, la expansión del WiFi 6, la inversión en la analítica avanzada de datos, el aprendizaje automático de la *Artificial Intelligence* (AI) y el *Machine Learning*, el *Blockchain*, herramientas de *Conversational AI*, *Always-Connected-PCs* (ACPC) o la *Robotic Process Automation* (RPA). Su potencial prácticamente ilimitado para recopilar y tratar información, en especial, datos personales, supone, en este sentido, una amenaza inequívoca que pone en serios aprietos la capacidad del ciudadano del siglo XXI de controlar toda aquella información personal que se refiera a él o que de algún modo le afecte[5].

La protección jurídica de los datos personales se ha revelado, en consecuencia, como una cuestión fundamental en nuestros días, hasta llegar a erigirse en uno de los temas más significativos y, por ende, polémicos relacionados con la articulación y el funcionamiento concreto de los instrumentos de tutela de los derechos y libertades ciudadanas[6]. Más aún si se considera que a las dificultades planteadas por el continuo

[3] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, *Configurar el futuro digital de Europa*, de 19 de febrero de 2020, COM (2020) 67 final, p. 1.

[4] De los más de 8 mil millones de personas que componen la población mundial, 5,35 mil millones empleaban internet al cierre del informe *Digital 2024 Global Overview Report. The essential guide to the world's connected behaviours*, publicado por We Are Social y Meltwater.

[5] Conde Ortiz (2005: 19 y ss.) hace hincapié, en este sentido, en la fácil vulnerabilidad de la intimidad con las nuevas tecnologías.

[6] Vid. Toniatti, (1991: 139).

avance tecnológico, se une, por otra parte, la futilidad de buena parte de las soluciones que pudieran articularse de forma autónoma y sin conexión a otras respuestas ensayadas con éxito en el ámbito internacional, por cuanto no cabe duda alguna que la globalidad de los ataques experimentados al efecto por los ciudadanos "no saben de fronteras"[7]. Son, en cualquier caso, agresiones explicables, esperables, incluso, hasta cierto punto, en el contexto socioeconómico vigente, en el que la información se erige claramente y de forma cada vez más global en instrumento de poder, en valor de cambio, desatando un voluminoso y difícilmente controlable tráfico de datos[8].

La sociedad contemporánea se ha acostumbrado, por lo demás, a convivir con este riesgo informático como elemento de conflictividad en mudanza y agravamiento constante a causa de la imparable innovación tecnológica. Trasiego que pone a prueba los principios, instrumentos y técnicas jurídicas habituales para reclamar, en cambio, una atenta y profunda reflexión en busca de nuevas soluciones normativas que permitan no sólo sancionar *a posteriori* los posibles incumplimientos en la materia, sino una prevención realmente efectiva de la vulneración de derechos y libertades esenciales de los ciudadanos.

A este respecto, el reconocimiento del derecho a la protección de los datos personales como derecho fundamental ha resultado polémico, no solo en el ordenamiento jurídico español, sino también en el ámbito internacional, planteando "apasionantes debates doctrinales" que han contribuido a perfilar con mayor nitidez conceptos esenciales y, en principio, tan cercanos como, entre otros, los de intimidad y privacidad, desembocando, en última instancia, en la articulación y confirmación de un auténtico derecho a la autodeterminación informativa por parte de los ciudadanos[9].

2. El reconocimiento del derecho a la protección de datos y a la consiguiente autodeterminación informativa.

Por lo que se refiere al Derecho español, la cuestión fue regulada por vez primera entre nosotros por Ley Orgánica 5/1992, de 29 de octubre, reguladora del tratamiento automatizado de los datos de carácter personal (en adelante, LORTAD). Su exposición de motivos subraya, a estos efectos, cómo "el progresivo desarrollo de las técnicas de recolección y almacenamiento de datos y de acceso a los mismos ha expuesto a la privacidad […] a una amenaza potencial antes desconocida", haciendo hincapié en la radical diferencia entre privacidad e intimidad.

Sostiene, a estos efectos, que "aquélla es más amplia que ésta, pues en tanto la intimidad protege la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona -el domicilio donde realiza su vida cotidiana, las comunicaciones en las que expresa sus sentimientos, por ejemplo-, la privacidad constituye un conjunto, más amplio, más global, de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado. Y si la intimidad, en sentido estricto, está suficientemente protegida por las previsiones de los tres primeros párrafos del art. 18 de la Constitución

[7] Así lo recuerda Piñar Mañas (2008a: 40).
[8] Una auténtica "fiebre informativa", tal y como subraya Betancor Rodríguez (1994: 181). Se refiere, asimismo, al peligro "que surge del valor económico de esta información", Murillo de la Cueva (2009: 58).
[9] Así lo refiere Agúndez Lería (2010: 938 y ss.).

y por las leyes que los desarrollan, la privacidad puede resultar menoscabada por la utilización de las tecnologías informáticas de tan reciente desarrollo."[10]

Ha tenido ocasión de pronunciarse a este respecto el Tribunal Constitucional, quien subraya la naturaleza como derecho fundamental, al amparo del art. 18.4 de la Constitución[11], del denominado derecho de protección de datos. De construcción y definición eminentemente jurisprudencial, toma la privacidad como referencia esencial o punto de partida fundamental para su construcción[12].

La Sentencia 254/1993, de 20 de julio, fue la primera en abordar un asunto relacionado con la existencia de datos personales en poder de las Administraciones públicas, radicando su importancia en reconocer que, si bien estamos ante un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad del art. 18.1 CE, es también "un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos" (FJ 6). El Tribunal Constitucional confirma así de manera inequívoca la configuración constitucional de la, en principio, garantía normativa del uso de la informática como un verdadero derecho fundamental: el derecho a la protección de datos personales o *habeas data,* si bien su incardinación constitucional no la establecería aún en el art. 18.4, sino en el art. 18.1 CE.

Representan un punto de inflexión fundamental al efecto las Sentencias constitucionales 290 y 292, ambas de 30 de noviembre del año 2000. Certifican un cambio de rumbo favorable a la consideración sin ambages del derecho a la protección de datos como verdadero derecho fundamental autónomo e independiente anclado en el art. 18.4 CE[13]. Afirma así la Sentencia 292/2000, de 30 de noviembre, que con la inclusión en el texto constitucional del art. 18.4, "el constituyente puso de relieve que era consciente de los riesgos que podría entrañar el uso de la informática", encomendando al legislador la salvaguardia tanto de ciertos derechos fundamentales como del pleno ejercicio de los derechos de la persona; e incorporando, en definitiva un instituto de garantía "como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona", que es también, "en sí mismo, un derecho o libertad fundamental"[14].

Y así, frente a la función del derecho fundamental a la intimidad del art. 18.1 de la Constitución, que no es otra que la de "proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del

[10] Se refiere, en concreto, al "camino de sombras" que va de la intimidad a la afirmación de la privacidad, del Castillo Vázquez (2007: 213 y ss.).

[11] El párrafo cuarto del citado art. 18 de la Constitución remite a la ley la limitación del "uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos". Sancho López (2019: 756) subraya cómo "el precepto se configuró en origen de forma tímida o residual", si bien "la función de adecuación del Derecho a la realidad social ha permitido una interpretación extensiva de su contenido, dando lugar al reconocimiento al derecho fundamental de protección de datos personales y al olvido digital, de manera sucesiva y complementaria, gracias a su apertura hermenéutica".

[12] Resulta esencial, a estos efectos, la concreción del concepto de dato personal *stricto sensu*, por cuanto condicionará de manera indudable el ámbito de aplicación del citado derecho. Vid., en este sentido, Agúndez Lería (2010: 941 y ss.) y Aparicio Salom (2002: 49 y ss.).

[13] Subrayan, asimismo, el valor de estas Sentencias y de la jurisprudencia del Tribunal Constitucional en la materia, Guichot (2005: 68 y ss.) y Piñar Mañas (2008a: 29 y ss.). Asimismo, sobre las posibles alternativas y consecuencias de la interpretación constitucional, Martínez Martínez (2004: 324 y ss.).

[14] FJ 4, con cita y reiteración expresa de la doctrina contenida en la anterior Sentencia del Tribunal Constitucional 254/1993, de 20 de julio, FJ 6.

conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad", el "derecho fundamental a la protección de datos" persigue, en cambio, "garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado". Se trata de una garantía que impone, en todo caso, 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"[15]. En definitiva, el objeto de ambos derechos resulta dispar.

El objeto de protección del derecho fundamental a la protección de datos es más amplio que el del derecho a la intimidad, pues "no se reduce sólo a los datos íntimos de la persona", sino que comprende "cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal". En definitiva, "los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo"[16].

Pero no sólo eso. Su distinto alcance otorga a su titular posibilidades también diversas para su adecuado ejercicio en cada caso. Así, la singularidad del derecho a la protección de datos deriva, además, de que confiere a su titular un "haz de facultades consistentes en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que no se contienen en el derecho fundamental a la intimidad, y que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer". Entre ellos, en concreto, "el derecho a que se requiera el previo 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 a acceder, rectificar y cancelar dichos datos. En definitiva, el poder de disposición sobre los datos personales."[17] De ahí que el derecho a la protección de datos haya sido apodado también como derecho a la autodeterminación informativa, por cuanto su contenido nuclear se dirige, en realidad, a garantizar la subsistencia de un poder de control por parte del ciudadano sobre sus datos personales, facultándole "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"[18].

[15] FJ 6.

[16] FJ 6.

[17] Recoge esta sustancial diferenciación entre los derechos fundamentales a la intimidad y a la protección de datos de los apartados 1 y 4 del art. 18 de la Constitución, el FJ 6 de la Sentencia. En consonancia, por otra parte, con la doctrina que había comenzado a abrirse paso respecto a la "libertad informática" con la Sentencia del Tribunal Constitucional 254/1993, de 20 de julio, FJ 7.

[18] FJ 7. Así lo subrayan, entre otros muchos, Tornos Mas (2008: 33) y Troncoso Reigada (2009: 94), para quien el derecho a la autodeterminación informativa no es sino el "derecho que tienen las personas a decidir por sí mismas cuándo y dentro de qué límites procede revelar datos referentes a su propia vida". La bibliografía sobre la construcción del derecho a la protección de datos o a la autodeterminación informática, su contenido esencial y las garantías para su efectividad resulta prácticamente inabarcable; vid., por todos, Canales Gil (2007: 13 y ss.), Conde Ortiz (2005: 27 y ss.), del Castillo Vázquez (2007: 133 y ss.), Fernández

El problema, como se ha subrayado ya, excede de las fronteras de cada Estado concreto para plantearse de forma global, en consonancia con el carácter universal y la ausencia de fronteras propia de internet y de las innovaciones tecnológicas alumbradas a partir de la red. No es de extrañar, por tanto, la atención dispensada a la materia por la Unión Europea, cuya regulación ha permitido asegurar un mínimo estándar de protección de los datos personales común a todos los países miembros[19]. Este propósito se ha visto reforzado tras el desplazamiento de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, por el Reglamento de la Unión Europea 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril, 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 (en adelante, RGPD)[20]. El nuevo Reglamento General de Protección de Datos pospone su aplicación hasta dos años más tarde, en concreto, hasta el 25 de mayo de 2018, si bien cabe reseñar desde su aprobación que la decidida apuesta de la Unión Europea por el alcance general, la obligatoriedad y aplicación directa de los Reglamentos europeos en todos sus elementos a todos los Estados miembros, así como la vigencia e implicaciones prácticas del principio de lealtad comunitaria, impusieron a los Estados la prohibición de adoptar medidas que pudieran resultar contrarias a la efectividad del Reglamento adoptado.

En todo caso, a diferencia de las construcciones jurisprudenciales nacionales del derecho a la protección de los datos personales que han debido inferir su vigencia y anclar su naturaleza constitucional en el reconocimiento previo y más amplio de un derecho a la intimidad y/o a la privacidad del ciudadano, el ordenamiento jurídico de la Unión Europea cuenta en la actualidad con cimientos taxativos más sólidos al respecto. Y así, el art. 8 de la Carta de los Derechos Fundamentales de la Unión Europea reconoce de forma expresa el derecho de toda persona "a la protección de los datos de carácter personal que la conciernan", sancionando, por lo demás, la obligación de tratarlos "de 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". De forma correlativa, "toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación", quedando sujeto el respeto de estas normas "al control de una autoridad independiente".

Se eleva así a la Carta de los Derechos Fundamentales de la Unión Europea la anterior exigencia comunitaria, plasmada en el art. 28 de la Directiva 1995/46/CE, dirigida a que los Estados miembros crearan "una o más autoridades públicas" encargadas de vigilar, con total independencia, la aplicación en su territorio de las disposiciones adoptadas por la Unión Europea en la materia. Una tendencia apreciable en el ámbito comparado y, en particular, en el ordenamiento jurídico español[21], que se había anticipado

Salmerón (2003: 51 y ss.), Guerrero Picó (2006: 27 y ss.), Guichot (2005: 61 y ss.), Herrán Ortiz (1998), Martínez Martínez (2004: 252 y ss.), Murillo de la Cueva y Piñar Mañas (2009), Piñar Mañas (2008b: 17 y ss.) y Serrano Pérez (2003: 123 y ss.).

[19] "Básicamente idéntico", en opinión de Muñoz Machado (2000: 181 y ss.), para quien no basta, sin embargo, con la regulación europea, debiendo mundializarse los estándares de protección de los datos personales "porque global es también la red por la que circulan".

[20] Con el fin, en expresión de Minero Alejandre (2014: 133), "de superar las incoherencias y debilidades que la aplicación de una norma del siglo pasado suponía para los problemas surgidos del avance de las nuevas tecnologías". Vid. al respecto, por todos, Davara Rodríguez (2016), Martínez Rojas (2016: 59 y ss.), Pérez Cambero (2016) y, muy especialmente, con mayor profundidad, la obra colectiva dirigida por Piñar Mañas y coordinada por Álvarez Caro y Recio Gayo (2016).

[21] Sobre las diversas soluciones articuladas al respecto en el ámbito internacional en relación a su esquema organizativo e institucional, vid., por todos, Toniatti (1991: 148 y ss.).

ya a esta posibilidad organizativa, alumbrando en 1992 la Agencia de Protección de Datos, regulada en el Título VI de la LORTAD, como Administración independiente[22]. Una configuración que permanece inalterada, como no podía ser de otra manera a la vista de los requerimientos comunitarios, tras la sustitución de la LORTAD por la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (en adelante, LOPD), y de esta última, a su vez, por Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPD-GDD), que mantienen las líneas esenciales de su regulación si bien bajo el rótulo actual de Agencia Española de Protección de Datos (en adelante, AEPD)[23].

Ahora bien, también el Tratado de Funcionamiento de la Unión Europea reconoce de forma expresa en su art. 16 el derecho a la protección de los datos de carácter personal, disponiendo que "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 Estados miembros 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", sometiendo, asimismo, el respeto de dichas normas "al control de autoridades independientes"[24].

El espectacular desarrollo tecnológico propiciado por la implantación y la propia evolución de internet aboca a los poderes públicos y, en concreto, a los reguladores, a una actividad frenética, marcada por el propio vértigo que imprime a la aprobación y la modificación del régimen jurídico aplicable al ámbito electrónico la velocidad de los cambios habidos sucesivamente en el sector, no solo en relación con el advenimiento de tecnologías desconocidas hasta el momento y de nuevos tipos de aplicaciones y herramientas para potenciales usuarios, que amplían considerablemente el número y la diversidad de los ciudadanos que interactúan con la red, sino también por la expansión progresiva pero imparable, en términos tanto cuantitativos como cualitativos, de las relaciones sociales, comerciales y de cualquier otro tipo que se traban en la red. Así las cosas, las respuestas articuladas desde el Derecho se caracterizan por ser recientes, por su extraordinaria mutabilidad y marcada especialización pese a su vocación multidisciplinar y expansiva y, ante todo, por cierta vocación de globalidad acorde, por lo demás, con la propia naturaleza y funcionamiento de internet. El caldo de cultivo para la amenaza a nuestra seguridad tecnológica y, en concreto, a la garantía de nuestra información personal, es, como se comprende, óptimo. Nuestros datos quedan expuestos a potenciales

[22] Independencia ineludible, en opinión de Rallo Lombarte (2002: 131), por cuanto estas Autoridades deben preservar los derechos de los ciudadanos "frente a las agresiones procedentes tanto de lo privado como de lo público". En concreto, sobre su ineludible articulación como Administración independiente y las manifestaciones y garantías de su independencia que recoge nuestro ordenamiento jurídico, vid. Casares Marcos (2012: 263 y ss.).

[23] Nominada inicialmente por la LORTAD "Agencia de Protección de Datos", mantiene esta denominación de forma ininterrumpida hasta que el art. 79 de la Ley 62/2003, de 30 de diciembre, dispone su nueva denominación como "Agencia Española de Protección de Datos".

[24] Debe tomarse en consideración que el propio art. 16 establece que las normas adoptadas al efecto se entenderán sin perjuicio de aquellas específicas sobre la política exterior y de seguridad común previstas en el art. 39 del Tratado de la Unión Europea. Del mismo modo, las declaraciones anejas al acta final de la Conferencia Intergubernamental que adopta el Tratado de Lisboa, en concreto, números 20 y 21, se refieren a este art. 16 para establecer reservas y salvaguardas específicas en relación con la protección de datos de carácter personal y su libre circulación en cuanto puedan tener repercusión directa en la seguridad nacional y en relación con la naturaleza específica de los ámbitos de la cooperación judicial en materia penal y de la cooperación policial.

ciberataques de origen sumamente diverso, ubicuos, de bajo coste y fácil realización, de gran efectividad e impacto pese al escaso riesgo que entraña su ejecución material.

En este contexto se ha abierto paso, a título de ejemplo, el debate social y jurídico (*ubi societas, ibi ius*) en torno a un posible "derecho al olvido", que brota precisamente a partir del denominado "efecto eterno" de la información en internet, fruto de la "memoria total" de la red[25]. Si antaño los viejos maestros del periodismo afirmaban que el papel del periódico de hoy envuelve el pescado de mañana[26], actualmente el derecho a la intimidad en su vertiente particular como derecho a ser dejado en paz ha evolucionado hacia lo que se ha dado en denominar un nuevo derecho al olvido, apuntalado, en todo caso, por el derecho que asiste al ciudadano de proteger sus datos personales y, en su ejercicio, determinarse informativamente, decidiendo y modulando la imagen pública y la reputación que se tiene de él[27].

Brota de esta forma en el espectro electrónico un nuevo derecho al olvido digital, de creación eminentemente jurisprudencial[28], que encarnaría, en definitiva, una variante de los derechos de acceso, rectificación, cancelación y oposición en que se descompone inicialmente la libertad o el derecho a autodeterminarse informativamente. Así lo concibe tempranamente la AEPD que mantiene en varias de sus resoluciones que "ningún ciudadano que no goce de la condición de personaje público ni sea objeto de hecho noticiable de relevancia pública tiene que resignarse a soportar que sus datos de carácter personal circulen por la red sin poder reaccionar ni corregir la inclusión legítima de los mismos en un sistema de comunicación universal como internet"[29]. La pretensión del solicitante de que internet "olvide" cierta información personal que se refiera a él puede resultar, por tanto, no solo factible sino legítima, abocando a una delicada tarea de ponderación entre intereses enfrentados y derechos subyacentes a cada caso particular.

De nuevo el casuismo como punto de partida y destino de cualquier debate jurídico mínimamente difícil. El Derecho no es sino el intento de objetivar y encasillar en

[25] Chéliz Inglés (2016: 256) se refiere, en este sentido, a la "perennidad" de la información contenida en internet y a su memoria "infalible".

[26] En alusión a la famosa frase de Walter Lippman, "tus grandes exclusivas de hoy envuelven el pescado de mañana".

[27] Así lo recuerda y destaca, en particular, Martínez Otero (2015: 106). Vid., asimismo, Casino Rubio (2012: 201 y ss.).

[28] Así, por todos, Minero Alejandre (2014: 129 y ss.) y Seligrat González (2015). Podría definirse de entrada como el derecho que tienen las personas físicas cuyos datos han accedido a los motores de búsqueda de páginas web en internet, a que tales datos sean desindexados y a que desaparezcan, en consecuencia, de los resultados de estos buscadores de tal modo que ya no resulte viable seguir encontrando informaciones antiguas y/o desactualizadas que, tras un período de tiempo de existencia en la red, se entiende justificado que desaparezcan a solicitud del propio sujeto afectado. Es oportuno recordar que la exigencia de cancelación o borrado de datos o informaciones perjudiciales del pasado no es una cuestión novedosa en nuestro ordenamiento jurídico, que contempla figuras como la cancelación de antecedentes penales o la anonimización de las sentencias judiciales y otras resoluciones administrativas antes de ser publicadas, con la pretensión de garantizar al sujeto su derecho a la intimidad, a la reinserción, al libre desarrollo de su personalidad, etc., si bien la eclosión de las nuevas tecnologías informáticas en red ha recrudecido el debate y propiciado su expansión a nuevos supuestos. Caso paradigmático de esta nueva reivindicación por borrar un contenido legal pero ya carente de actualidad e interés es del señor Costeja, considerado auténtico *leading case* en materia de derecho al olvido y resuelto por la pionera Sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014. Vid., con mayor profundidad, sobre el derecho al olvido en internet y la autodeterminación informativa personal en el ordenamiento jurídico español, Casares Marcos (2020: 401 y ss.).

[29] Así, entre otros, en los expedientes de tutela de derechos TD/01335/2008, TD/00627/2009 y TD/00061/2012.

tipos predefinidos la complejidad, diversidad e impredecibilidad de los comportamientos humanos a la luz de las circunstancias y de las valoraciones sociales vigentes en cada contexto y momento. Una misión aún más compleja ante las connotaciones del mundo digital, en continua evolución y con un claro efecto megáfono respecto a cualquier información que alcanza la red, en la que se sabe cúando se ingresa pero no si se podrá salir[30]. A falta de nuevas herramientas o soluciones jurídicas que permitan automatizar la respuesta a los conflictos así planteados, el principio de proporcionalidad se erige, sin duda, en herramienta esencial al respecto para constatar si el ejercicio efectivo de la facultad de oposición al tratamiento de la información personal es susceptible de quebrar de algún modo la legitimidad de una medida que, si bien resulta restrictiva del derecho fundamental, se encuentra amparada, pese a todo, por los juicios de idoneidad, en cuanto "susceptible de conseguir el objetivo propuesto", necesidad, porque "no exista otra medida más moderada para la consecución de tal propósito con igual eficacia" y equilibrio, "por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto"[31].

Sostiene expresamente la Sentencia del Tribunal Constitucional 17/2013, de 31 de enero, que "el derecho a la protección de datos no es ilimitado y aunque la Constitución no le imponga expresamente límites específicos, ni remita a los poderes públicos para su determinación como ha hecho con otros derechos fundamentales, no cabe duda de que han de encontrarlos en los restantes derechos fundamentales y bienes jurídicos constitucionalmente protegidos, pues así lo exige el principio de unidad de la Constitución"[32].

Nos situamos, en suma, ante un derecho de última generación en plena configuración en su vertiente tecnológica, vinculada a la revolución digital[33], sin que su mayor proyección actual a consecuencia de la omnipresencia de internet, de la consolidación y expansión del comercio electrónico, de las redes sociales y de la divulgación universal e instantánea de todo tipo de información obste para reconocer que se trata, en realidad, de una problemática anterior a la propia sociedad de la información[34]. Cabe citar así, por ejemplo, la Sentencia del Tribunal Constitucional Federal alemán de 5

[30] La libertad con que los datos circulan por el ciberespacio, entre bases de datos, servidores y copias periódicas de páginas web, ha dado lugar al que Troncoso Reigada (2008: 320) ha bautizado como el "efecto Hotel California": *you may enter, but you may never leave*.

[31] Vid., por todas, la Sentencia del Tribunal Constitucional 207/1996, de 16 de diciembre, FJ 4. Destaca asimismo, entre otras muchas, la ponderación efectuada en estos mismos términos por la Sentencia del Tribunal Supremo 210/2016, de 5 de abril (rec. 3269/2014), en relación con una solicitud en 2009 a Google Spain de la cancelación del tratamiento de los datos personales de un ciudadano con relación a un indulto que le fue concedido en 1999 por un delito cometido en 1981.

[32] FJ 4. En cuanto a sus posibles límites, sostiene la STC 292/2000, de 30 de noviembre, FJ 9, que han de ser establecidos por una norma con rango legal, *ex* art. 18.4 CE, y han de ser los estrictamente indispensables en una sociedad democrática. Con apoyo en la jurisprudencia del TEDH, las limitaciones previstas en la ley ha de ser accesibles a los individuos, previsibles en sus consecuencias, y que respondan a una imperiosa necesidad social. Entre estas últimas se encuentran, en particular, la seguridad del Estado [art. 105.b) CE], la persecución y castigo de delitos o la distribución equitativa del sostenimiento del gasto público y las actividades de control en materia tributaria (art. 31 CE), como bienes y finalidades constitucionales legítimas capaces de restringir los derechos del art. 18.1 y 4 CE.

[33] Motivo que explica para Sancho López (2019: 759) las "disparidades jurisprudenciales o cambios de criterio" en algunas cuestiones concretas.

[34] Así lo subrayan, por ejemplo, Moura Vicente (2019-2020: 225 y ss.) y Sancho López (2018: 194 y ss.), quien refiere cómo "la doctrina existente en esta materia" habrá de adaptarse "a los nuevos marcos sociales y tiempos de la técnica". Ya Díez-Picazo (1979: 114) reclamaba la necesidad de consentimiento expreso para publicar la biografía de una persona o investigar su vida anterior, apoderarse de sus datos o archivarlos.

de junio de 1973[35], que, invocando el principio de proporcionalidad, avala con fundamento en el derecho al libre desarrollo de la personalidad, consagrado en el art. 2.1 de la Ley Fundamental alemana, la prohibición de emisión de un documental de televisión que evocaba tiempo después la condena criminal de un participante, al que se identificaba personalmente, en el conocido como asesinato de soldados de Lehbach, al ser susceptible de causar un perjuicio nuevo o adicional al autor del hecho, poniendo en peligro su resocialización y reinserción en la sociedad. Sin que las más que notables divergencias entre el modo europeo y el americano de concebir el derecho a la privacidad y las libertades esenciales de prensa, información o expresión hayan privado al ordenamiento jurídico estadounidense de debates similares[36]. En efecto, aun anterior en el tiempo es la famosa sentencia estadounidense *Sidis v. F.-R. Publishing Corp*, de 22 de julio de 1940[37], en la que se deja abierta la puerta a una eventual limitación de la libertad de información cuando los datos que se pretendan revelar a través de la prensa resulten de una naturaleza tan íntima y de tan injustificable divulgación desde la perspectiva de su titular como para vulnerar y violentar la noción colectiva de decencia (*the community's notions of decency*)[38].

Planteado el dilema en las coordenadas socioeconómicas y, ante todo, tecnológicas actuales, no cabe duda que exige de una profunda reflexión y reinterpretación a la luz del doble efecto que internet y, en particular, los motores de búsqueda en la red ejercen sobre la información que en ella se vierte. No en vano se combinan en su seno, de un lado, la teoría del megáfono, en cuanto al efecto multiplicador propiciado por los motores de búsqueda en la red, y, de otro, la denominada teoría del mosaico[39], a que alude la Sentencia del Tribunal Supremo 179/2011, de 18 de marzo (rec. 703/2008), al desestimar el recurso de casación interpuesto contra Sentencia del Juzgado de Primera Instancia núm. 54 de Madrid, de 23 de abril de 2007, en la que se hace hincapié en que "existe el concepto de derecho a la intimidad denominado teoría del mosaico, que aparece como protección de la intimidad del individuo frente a las nuevas tecnologías. […] las esferas hasta ahora indicadas, de públicas y privadas son relativas, ya que existen datos que son irrelevantes desde el punto de vista del derecho a la intimidad, pero que unidos a otros, pueden servir para configurar una idea completa de cualquier individuo."[40]

De ahí, por tanto, que pese a que el asunto se enuncie en los términos tradicionales de confrontación entre derechos constitucionales y, en definitiva, de necesaria ponderación a la luz de cada caso particular para comprobar y determinar la prevalencia de uno u otro en función del bien jurídico o constitucional más digno de protección en

[35] 1 BvR 536/72.

[36] En todo caso, la diversa perspectiva desde la que se plantea el debate se debe, indudablemente, a la distinta concepción que existe de la privacidad en Estados Unidos y en Europa, así como al conflicto más amplio entre los diversos conceptos nacionales sobre la relevancia relativa de las sucesivas generaciones de derechos humanos. Sin entrar en profundidad en la materia cabe citar al efecto Abril y Pizarro Moreno (2014), Sidhu (2014) y Moura Vicente (2019-2020), quien refiere cómo se trata de un "problema recurrente en la historia de internet".

[37] US Court of Appeals for the Second Circuit – 113 F. 2d 806 (2d Cir. 1940), de 22 de julio de 1940.

[38] Siempre que no se trate, sin embargo, de un personaje público (*public character*), como era el caso, ya que entonces la veracidad de sus infortunios y fragilidades justificaría el interés y el debate públicos. Salvador Coderch (1987: 98) reflexiona a partir de esta sentencia sobre los confines que impiden a la memoria colectiva entrometerse en la intimidad personal.

[39] Aluden a esta combinación Manzanero Jiménez y Pérez García-Ferrería (2015: 256).

[40] Juicio ordinario núm. 1074/2006, fundamento de derecho tercero.

cada supuesto, sean muchas las cuestiones no solo complejas sino especialmente arduas y engorrosas planteadas al respecto.

¿Con qué alcance se debe configurar el derecho a la protección de datos en internet? ¿Es posible conjugar los derechos comunicativos, en concreto, las libertades de información y expresión, con la intimidad de las personas? ¿Qué responsabilidad cabe imputar en cada caso a los diferentes prestadores de servicios en la red? ¿Deben los motores de búsqueda en internet responder de aquellos contenidos que analizan, indexan y ofrecen a los internautas? ¿Puede borrarse el pasado de una persona de internet? Es más, ¿debe hacerse? ¿A qué precio? ¿Al de restringir la libertad de expresión o el derecho a la información de sus usuarios? ¿No se abre con ello la puerta a un control de contenidos en la red que linda con la censura? ¿Qué responsabilidad y capacidad de decisión debemos reconocer a los buscadores de internet sobre los contenidos que indexan? ¿Pueden actuar ciegamente o deben, por el contrario, incorporar criterios de oportunidad en su indexación, retirando, por ejemplo, de sus listas de resultados aquellos enlaces de contenido especialmente ofensivo? ¿Dónde situar el límite concreto que hace decaer la idoneidad y, por ende, la legitimidad del tratamiento de los datos personales hasta el punto de obligar a suprimir un enlace? ¿Quién está legitimado para solicitar o, en su caso, oponerse a dicha retirada? Son interrogantes que pueden multiplicarse, sin duda, de forma indefinida y que inciden también, de forma muy señalada, sobre la transparencia y, en especial, sobre el derecho de acceso a la información pública, en tanto, conviene recordarlo, su plasmación y regulación normativa no suele exigir la concurrencia de causa justificativa o la motivación explícita de la petición al solicitante, que, una vez obtenida la información, será libre, en principio, para decidir sobre su uso y, si así lo decide, transmitirla, darla a conocer o informar sobre ella.

3. Desafíos planteados a la protección de datos por la transformación digital de la Administración.

En España la aprobación de las Leyes 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, desató, en su momento, una honda preocupación, que no ha amainado, acerca de sus implicaciones concretas tanto para los operadores jurídicos, públicos y privados, como para los ciudadanos en general. No en vano, derogó a su entrada en vigor la longeva y asentada Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, iniciando una nueva etapa en relación con la organización y el funcionamiento del sector público español, marcada, fundamentalmente, por la separación en dos textos normativos diversos de la regulación de las vertientes *ad extra* y *ad intra* de nuestras Administraciones públicas.

Destaca, a tal efecto, la preocupación del legislador, cuando no su auténtica obsesión, por continuar profundizando en la expansión e implantación definitiva de la Administración electrónica, vocación que la Ley 19/2013 había hecho suya poco tiempo antes[41]. La reforma incorpora, en tal sentido, importantes innovaciones, escudándose en la necesidad de mejorar el funcionamiento interno de nuestra Administración pública y, en particular, en los principios de eficacia y eficiencia, para implantar un nuevo modelo administrativo que suscita, sin duda, cuestiones y objeciones que precisan respuesta,

[41] Meseguer Yebra e Ibáñez Pascual (2017: 25) refieren cómo el texto se encuentra sembrado, a tal efecto, "de continuas llamadas a los factores tecnológicos de la transparencia".

sobre todo desde la perspectiva de los derechos y garantías de los ciudadanos, en general, y, de forma específica, desde su derecho concreto a la protección de sus datos personales, en particular.

Los nuevos textos legales comparten tres rasgos esenciales, descansando sobre ellos a modo de auténticos pilares de la reforma[42]. En primer lugar, su insistencia en la necesidad de mejorar el funcionamiento interno de la Administración pública en aras de lograr la eficiencia y economía administrativas tan reivindicadas por el Informe de la Comisión para la Reforma de las Administraciones Públicas (CORA), presentado al Consejo de Ministros celebrado el 21 de junio de 2013[43]. Cabe subrayar, a tal efecto, la atención dispensada por las nuevas leyes de 2015 a la simplificación y electronificación de la Administración pública y de sus trámites, previsiones sin duda idóneas para sustanciar un considerable ahorro económico en su funcionamiento interno, si bien a costa de postergar en ocasiones en su enunciado normativo las relaciones entre el ciudadano y la Administración pública, subordinadas ahora, en gran medida, a la satisfacción de aquellos objetivos prioritarios[44].

En segundo lugar, su escaso alcance innovador, en cuanto ambas leyes se limitan, en esencia, a refundir la normativa preexistente con algunos amplios desarrollos de normas jurídicas vigentes al momento de su aprobación, por ejemplo, en materia de convenios y relaciones interadministrativas. En tal sentido, las leyes de 2015 comprenden, más bien, pequeñas reformas, puntualizaciones y aclaraciones, así como algunos desarrollos, que se insertan, sin discusión alguna, en un planteamiento claramente continuista respecto a la normativa vigente al momento de su alumbramiento como anteproyectos, posterior tramitación y ulterior aprobación parlamentaria.

Y, por último, su abrumadora inquietud por la Administración electrónica, por imponer, en definitiva, su despliegue y funcionamiento efectivo, fácilmente constatable a la vista del número de referencias expresas al fenómeno electrónico que salpican su enunciado final[45]. El legislador continúa profundizando de esta manera en el concepto de Administración electrónica, incorporando importantes innovaciones al respecto[46], si bien el paso que persigue y alienta, en última instancia, desde una cultura administrativa en

[42] Así lo destaca el análisis propuesto por Santamaría Pastor (2015).

[43] No en vano, al disertar sobre las razones de la reforma de la Administración pública en España el Informe de la Comisión para la Reforma de las Administraciones Públicas (CORA), elaborado -conviene recordarlo- en un momento de honda preocupación por la austeridad presupuestaria a consecuencia de las devastadoras consecuencias de la crisis financiera desatada poco antes, sostiene, p. 35, que "existe una conciencia generalizada de que la Administración debe adaptarse a las demandas de la sociedad del siglo XXI. En los últimos treinta años la mayoría de los países de la OCDE han puesto en marcha medidas de reforma de la Administración pública. Algunas de las adoptadas han estado enmarcadas en planes globales mientras que otras son muy específicas y se concentran en aspectos concretos. En general, todas ellas tienen su origen en la necesidad de contener el crecimiento del gasto en el seno de un proceso de consolidación fiscal, pero son cada vez más lo casos en los que las reformas persiguen una verdadera transformación de la Administración, mejorando su eficacia, su calidad y eficiencia, para adaptarse mejor a las necesidades de los ciudadanos. El tema no es baladí. La gestión de lo público es importante. La Administración equivale, en términos de gasto público en la Unión Europea, a mitad de la economía. Si una de las variables estratégicas para el desarrollo económico es el aumento de la competitividad, una organización que equivale a cerca del 50% del PIB debe ser competitiva."

[44] Vid. Casares Marcos (2016).

[45] Y sobre las que cabe ver, con mayor profundidad, Casares Marcos (2016: 61 y ss.), así como la doctrina allí citada.

[46] Hace especial hincapié en ello, por todos, Quintana Daimiel (2015).

papel a una nueva completamente electrónica, se sustancia sin mutar en absoluto la naturaleza de la relación que subyace entre Administración pública y ciudadanos[47].

En todo caso, la reforma habida en octubre de 2015 en materia de Administración electrónica afecta, de forma fundamental y prioritaria, a la sustanciación del procedimiento administrativo. En este sentido, la propia Exposición de motivos de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, reconoce que "en el entorno actual, la tramitación electrónica no puede ser todavía una forma especial de gestión de los procedimientos, sino que debe constituir la actuación habitual de las Administraciones. Porque una Administración sin papel basada en un funcionamiento íntegramente electrónico no sólo sirve mejor a los principios de eficacia y eficiencia, al ahorrar costes a ciudadanos y empresas, sino que también refuerza las garantías de los interesados." Garantías que el legislador parece cifrar exclusivamente en términos de transparencia al continuar afirmando: "En efecto, la constancia de documentos y actuaciones en un archivo electrónico facilita el cumplimiento de las obligaciones de transparencia, pues permite ofrecer información puntual, ágil y actualizada a los interesados."

La incorporación real y efectiva de los avances alcanzados al efecto por las tecnologías de la información a la organización y a los procedimientos de nuestras Administraciones públicas ha abocado, necesariamente, a un cambio de paradigma en la concepción de las relaciones entre estas últimas y los ciudadanos[48]. No en vano, quedan afectados por el uso administrativo de medios informáticos, electrónicos y telemáticos tanto su *front office* como su *back office*, esto es, su gestión, presencia y relaciones propiamente externas, de un lado, y, sus tareas y gestión de puertas hacia dentro, de otro[49].

La adopción y el uso de tales innovaciones debieran desembocar así en un nuevo modelo de Administración pública, que habría de descansar sobre el triple eje de la Administración electrónica, la transparencia y la reutilización de la información en poder del sector público. No constituye, en todo caso, un fin en sí mismo, sino que debe abarcarlo todo dentro de la Administración, "desde la organización administrativa hasta los derechos de los ciudadanos, desde la constitución y el funcionamiento de los órganos colegiados hasta la notificación de las resoluciones, desde la transparencia hasta los contratos públicos", imponiendo un cambio no tanto en el fondo como en las formas administrativas[50].

A ello ha aludido también la Unión Europea al definir de forma expresa a la Administración electrónica como "el uso de las tecnologías de la información y las

[47] Se trata, en opinión de Baño León (2015), de un cambio meramente tecnológico.

[48] Hace hincapié en ello Martín Delgado (2016: 5).

[49] Así, siguiendo en este punto a Davara Fernández de Marcos y Davara Rodríguez (2016), si hablamos del *front office* de una Administración nos referimos a la relación *ad extra* entre Administración y administrado, esto es, a la gestión y la presencia de la Administración "de puertas hacia fuera", quedando incluidos los servicios ofrecidos a la ciudadanía, la gestión y el control de la participación del ciudadano, el cumplimiento y verificación del mismo en lo que a la aplicación de la normativa se refiere y todo lo relativo a la prestación de servicios de información del sector público, bajo los prismas de la transparencia y apertura administrativa. Mientras que en el *back office* de una Administración pública quedan incluidas tareas y cuestiones relacionadas con la gestión de "puertas hacia dentro" de la Administración, esto es, todo lo relacionado con la regulación de la entidad pública, la colaboración inter-departamental, la gestión del conocimiento y la resolución de conflictos internos de la Administración, el control y desarrollo de las compras públicas y la interoperabilidad en el conjunto de la Administración pública de que se trate.

[50] En expresión de Martín Delgado (2016: 5 y ss.).

comunicaciones en las Administraciones públicas, combinado con cambios organizativos y nuevas aptitudes, con el fin de mejorar los servicios públicos y los procesos democráticos y reforzar el apoyo a las políticas públicas"[51].

El legislador español había dado ya algunos pasos significativos en esta dirección, si bien hasta el momento las modificaciones habían tenido por objeto reconocer la validez de las actuaciones que implicaban un cambio de "tecnología" en comparación con el modo anterior de hacer las cosas[52]. A esta filosofía responden, en concreto, tres hitos fundamentales. De un lado, el paso del documento en papel al documento electrónico sancionado por la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común[53]. De otro, la introducción en nuestro ordenamiento jurídico administrativo de la firma electrónica por la Ley 59/2003, de 19 de diciembre, de Firma Electrónica[54]. Y, en última instancia, la primera regulación general del fenómeno de la Administración electrónica por Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, que se concentró principalmente en el *front office* descuidando en cierta medida el *back office* o ámbito interno de la Administración pública[55].

No cabe duda de que, en este contexto, la reforma efectuada en el año 2015 podría haber sido más ambiciosa[56]. En todo caso, contribuye de forma decisiva a situar la Administración electrónica "en el corazón mismo del Derecho Administrativo básico-común"[57]. Y así, desde la perspectiva del tráfico externo o *front office*, la reforma legal de la Administración electrónica efectuada por la Ley de Procedimiento Administrativo Común de 2015 alumbra nuevas posibilidades, cuando no auténticas obligaciones, que habrán de ofrecer, sin duda, nuevos modelos de relación entre la Administración pública y los administrados[58], estructurando a tal efecto en varios niveles la obligación de los ciudadanos de utilizar medios electrónicos en sus relaciones con las Administraciones

[51] Vid. la Comunicación de la Comisión al Consejo, Parlamento Europeo, Comité Económico y Social Europeo y Comité de las Regiones sobre *El papel de la Administración electrónica en el futuro de Europa*, COM (2003) 567 final, p. 7.

[52] Vid., en este mismo sentido, Martín Delgado (2016: 7).

[53] Vid., en concreto, la redacción original de su artículo 45, relativo a la incorporación de medios técnicos a la actividad de las Administraciones públicas.

[54] Esta Ley trae causa del Real Decreto-ley 14/1999, de 17 de septiembre, sobre Firma Electrónica, al que deroga y que había sido aprobado con el objetivo de fomentar la rápida incorporación de las nuevas tecnologías de seguridad de las comunicaciones electrónicas en la actividad de las empresas, los ciudadanos y las Administraciones pública.

[55] No en vano, su propia Exposición de motivos subraya que la norma "pretende dar el paso del «podrán» por el «deberán»", de forma que supone "pasar de la declaración de impulso de los medios electrónicos e informáticos -que se concretan en la práctica en la simple posibilidad de que algunas Administraciones, o algunos de sus órganos, permitan las comunicaciones por medios electrónicos- a que estén obligadas a hacerlo porque la Ley reconoce el derecho de los ciudadanos a establecer relaciones electrónicas".

[56] Así lo entiende también, entre otros, desde la perspectiva concreta de la innovación, Martín Delgado (2016: 7). No en vano, como bien destaca Chaves (2016), la reforma "cede a la tentación de ofrecer visos de modernidad electrónica", derogando la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, para resucitarla de nuevo con preceptos sustancialmente similares cuando no idénticos en su tenor literal.

[57] De forma que deja de estar regulada en una ley especial, tal y como destaca Gamero Casado (2016: 15).

[58] Para Sánchez Sánchez (2016: 65) uno de los logros de la Ley 39/2015, de 1 de octubre, ha sido, precisamente, el de uniformar la regulación en materia electrónica, frente a la dispersión hasta ahora vigente, y sentar las bases o requisitos mínimos que, en esta materia, deben regir en las relaciones entre el ciudadano y la Administración.

públicas. Una regulación con la que se mostró crítico el Consejo General del Poder Judicial al subrayar que la "imposición *ex lege* de esta obligación no parece que pueda hacerse a espaldas de los principios de necesidad y proporcionalidad", proclamados por el artículo 1.2 de la propia Ley, "como tampoco soslayando las exigencias del principio de igualdad, de carácter constitucional e integrador del acervo del Derecho de la Unión Europea"[59].

Ahora bien, aunque las novedades y reformas más importantes en materia de Administración electrónica atañen al procedimiento administrativo entablado con los ciudadanos, no cabe ignorar que es un tema asimismo recurrente e importante en la LRJSP[60]. De acuerdo con esta última, el tráfico interno administrativo, su vertiente *ad intra* o *back office* administrativo, se alzará también sobre claves electrónicas. A estos efectos, recoge, con algunas modificaciones, lo ya dispuesto al respecto en su momento por la Ley 11/2007, de 22 de junio, y por el Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente dicha Ley.

Como declara significativamente su propia Exposición de motivos, "se integran así materias que demandaban una regulación unitaria, como corresponde con un entorno en el que la utilización de los medios electrónicos ha de ser lo habitual, como la firma y sedes electrónicas, el intercambio electrónico de datos en entornos cerrados de comunicación y la actuación administrativa automatizada", estableciéndose, asimismo, la obligación de que las Administraciones públicas se relacionen entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes a través de medios electrónicos[61], previsión que alcanza, significativamente, a la cooperación interadministrativa mediante una regulación específica de las relaciones electrónicas entre Administraciones[62].

Y es que la Ley 40/2015, de 1 de octubre, tiene, ante todo, una función de consolidación y de refundición de la regulación precedente, sin que suponga una modificación profunda del régimen legal hasta entonces vigente, aunque no falten en ella algunas innovaciones puntuales importantes, entre otras, el fortalecimiento de la Administración electrónica, reforzando y completando la normativa anterior[63].

En este contexto se aprueba la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014. Pretende, en clave de Derecho interno, luchar contra la corrupción y así, conforme al tenor literal de su Exposición de motivos, aspira señaladamente a "diseñar y ejecutar un nuevo sistema de contratación pública, más eficiente, transparente e íntegro, mediante

---

[59] Conclusión vigesimotercera del Informe adoptado por el Pleno del Consejo General del Poder Judicial con fecha 5 de marzo de 2015, sobre el Anteproyecto de Ley del Procedimiento Administrativo Común de las Administraciones Públicas.

[60] Vid., a tal efecto, con mayor profundidad, Rodríguez-Piñero Bravo-Ferrer (2016) y Santamaría Pastor (2015), quien refiere la "preocupación abrumadora" del legislador por la Administración electrónica. En todo caso, se muestra crítico con la disgregación de la materia en dos textos legales diversos, Gamero Casado (2016: 17).

[61] Artículo 3.2 de la Ley 40/2015, de 1 de octubre.

[62] En todo caso, Gamero Casado (2016: 21) aprecia un "decepcionante atavismo", cuando no auténtica "involución" en materias que venían siendo ampliamente criticadas en su regulación anterior, así, señaladamente, registros y notificaciones.

[63] En idéntico sentido, Rodríguez-Piñero Bravo-Ferrer (2016).

el cual se consiga un mejor cumplimiento de los objetivos públicos, ya señalados, tanto a través de la satisfacción de las necesidades de los órganos de contratación, como mediante una mejora de las condiciones de los operadores económicos, así como un mejor servicio para los usuarios de los servicios públicos". En sintonía, por otra parte, con el Informe de la Comisión al Consejo y al Parlamento Europeo sobre *La lucha contra la corrupción en la Unión Europea*, de 3 de febrero de 2014, en el que se afirma que "la contratación electrónica, además de la mejora de la eficacia de los procedimientos de contratación pública, ofrece garantías adicionales en términos de prevención y detección de las prácticas corruptas, porque contribuye a aumentar la transparencia y permite una mejor aplicación de procedimientos normalizados, así como la provisión de mecanismos de control"[64], razón por la que se apuesta decididamente, también en este sector, por la exigencia no solo del empleo de medios electrónicos sino también de una mayor transparencia a partir de la imposición de deberes concretos de publicidad activa.

Qué duda cabe que a estos efectos la transparencia, el acceso a la información pública y las normas de buen gobierno, cuyo régimen jurídico había sido apuntalado poco antes por la aprobación de la Ley 19/2013, de 9 de diciembre, plantean nuevos retos y dudas o al menos magnifican los preexistentes ante la propia apertura, la inconcreción y la mudanza constantes inherente al proceso de transformación digital de la actuación pública y, en especial, de la administrativa. Así lo ha demostrado, en los últimos tiempos, la pandemia ocasionada por la expansión de la Covid-19, auténtico fenómeno disruptivo que ha impulsado la adopción de nuevas políticas y de acciones reformadoras del modo de comprensión de la actividad administrativa, en especial, de la atención al público y la prestación de los servicios públicos. Cabe citar, a título de ejemplo, el despliegue general del teletrabajo en el ámbito público, la automatización de ciertas decisiones administrativas, los proyectos piloto de inteligencia artificial desplegados en el ámbito público, el avance en la tramitación electrónica de procedimientos o en la digitalización para la mejora de la cogobernanza. De ahí que debamos situar el debate sobre los postulados que han de presidir la relación, no siempre pacífica, entre Administración, tecnología y transparencia, cuando menos a la misma altura que los sustanciados en torno a la selección entre las distintas opciones tecnológicas actualmente admitidas por el proceso de digitalización.

No en vano, la digitalización del ámbito público debe desplegarse con conciencia de los riesgos que comportan el uso masivo de datos personales o las transferencias nacionales e internacionales de los mismos. La tecnología no es inocua para el ser humano, conlleva progreso, pero, también, en ocasiones, retroceso en el disfrute de los derechos y libertades[65]. Por ello mismo, y en un contexto como el actual, se torna imprescindible que la transformación digital de nuestros poderes públicos y, en particular, Administraciones[66], posea unos cimientos sólidos e ineludibles que respeten, desde la perspectiva concreta de nuestro ordenamiento jurídico, el sistema de libertades construido

[64] COM (2014) 38 final, p. 34.

[65] Vid. a tal efecto las recomendaciones del Comisario de Derechos Humanos del Consejo de Europa, *Unboxing Artificial Intelligence: 10 steps to protect Human Rights*, de mayo de 2019, y la subsiguiente *Human rights by design. Future-proofing human rights protection in the era of AI*, de mayo de 2023.

[66] Souza y Costa (2023: 122) sostienen por ello que "una carta de derechos digital no estaría completa si no aborda la forma en que los ciudadanos se relacionan con la Administración pública y cómo esta debe hacer uso de las modernas tecnologías para garantizar una mayor eficiencia y confianza en la ejecución de sus actos".

por la Unión Europea y la Constitución Española. Sin esa base, el edificio tecnológico posterior correrá riesgo de derrumbe.

Toda transformación digital supone riesgos, entendidos como las potenciales consecuencias indeseadas no conocidas *ab initio* y que solo se manifestarán en su puesta en práctica. Algunos serán previsibles por ser comunes a toda implementación de un proceso de cambio digital. La dificultad inherente al ámbito público está en que los riesgos más relevantes no son los previsibles (tecnológicos) sino precisamente los imprevisibles (jurídicos), consecuencia de la inevitable interrelación entre ambos y de la necesidad de que cualquier solución digital ensayada en el ámbito público sea capaz de poder mantener los márgenes de decisión, interpretación, adecuación, individualización y autonomía de cualquier órgano administrativo[67]. El sector público es muy amplio y comprende personas jurídicas, órganos administrativos y entidades diferentes. La inadecuación o dificultad en la transformación de una parte supondrá, sin duda, un efecto mariposa en las demás.

Desde la perspectiva concreta de la transparencia en su doble vertiente de publicidad activa y derecho de acceso a la información pública cabe citar varios riesgos esenciales a tal efecto, en concreto tres. Existe, de un lado, el peligro de aumentar las brechas digitales entre los ciudadanos, especialmente en términos de acceso a los procedimientos y servicios digitales, también, en concreto, en lo que al acceso a la información pública se refiere, y, en especial, respecto de los colectivos de personas más vulnerables, de quienes viven en territorios rurales con problemas de conexión, o de quienes se encuentran en riesgo de exclusión social[68]. La ausencia de ciertas habilidades o la carencia de formación o información pudiera desembocar en diferencias sociales en la sustanciación de la transparencia pública.

Cabe citar, asimismo, las amenazas derivadas de la falta de transparencia algorítmica. El empleo de algoritmos y sistemas de inteligencia artificial puede generar falta de transparencia y opacidad en la toma de decisiones administrativas, lo que puede provocar, a su vez, desconfianza en la ciudadanía[69]. Aunque la digitalización supone una oportunidad para liberar a los empleados públicos de tareas cotidianas y repetitivas que no exigen mucha cualificación plantea también serios interrogantes cuando la adopción de decisiones administrativas se produce a partir de *software* predictivo en vez de un razonamiento jurídico basado en principios y reglas preestablecidas y conocidas. Se trata de un cambio de paradigma que corre el riesgo de auspiciar la deshumanización de la actividad pública en aras de soluciones tecnológicas que nos aseguren certeza y precisión de resultados.

---

[67] Así se subraya desde la perspectiva de la digitalización de la Administración de Justicia en *Diálogos para el futuro judicial LXII. La Ética de la Transformación Digital de la Justicia*, de Diario La Ley.

[68] Vid., desde la perspectiva de América Latina, Ávila (2023: 147 y ss.).

[69] Algunos autores plantean ya la conveniencia de amparar por vía constitucional el derecho de los ciudadanos al conocimiento de los algoritmos utilizados por las administraciones en la toma de decisiones automatizadas en el sector público. La justificación de la ampliación del reconocimiento constitucional a este pretendido derecho se motivaría por vía del art. 18.4 CE, en el que se consagran como derechos fundamentales la libertad informática y la protección de datos personales. Vid., por todos, Medina Guerrero (2022), quien subraya la importante vía abierta asimismo al respecto, a menudo complementaria, por la Ley 19/2013, de 9 de diciembre, a la que dedican mayor atención, entre otros, Cerrillo i Martínez (2020) y Gutiérrez David (2021).

Son también muy relevantes las cuestiones relativas, en fin, a la ciberseguridad y a la protección de datos, no solo desde la perspectiva del acceso no autorizado a los datos personales en manos públicas sino también del riesgo de una súbita paralización o disfunción total del sistema en el caso de que un gran ataque pudiera eliminar, masivamente, bases de datos o archivos administrativos falseando o eliminando la información pública (ya sea conocida y publicada o en poder de los organismos públicos).

Asistimos, sin duda, a un cambio esencial y novedoso. No tanto de los presupuestos básicos (la existencia y el manejo público de la información y los datos), sino de las posibilidades alumbradas por la innovación tecnológica para el tratamiento de su ingente cantidad, sus formas de acumulación y de gestión, así como su potencial uso masivo por la Administración, entre otras muchas cuestiones, en relación con su selección para la adopción o para formar parte de la base misma de decisiones administrativas vinculantes[70]. Este cambio de paradigma no supone romper con todo lo inmediatamente anterior sino ser conscientes de la riqueza que esta nueva gestión de los datos puede aportar y utilizarlos para mejorar, en todo caso, la seguridad jurídica y la propia visión que el ciudadano tiene de la Administración, publicitando lo que ocurre dentro de ella y permitiendo optimar el desarrollo de las políticas públicas no sólo mediante el análisis de los datos propios e internos, sino también a partir de la interoperabilidad con otras fuentes de datos pertenecientes a otras Administraciones Públicas y organismos externos[71]. No en vano, una parte significativa de las cartas sobre derechos digitales existentes en el ámbito comparado dedican algunos de sus preceptos a la actuación administrativa, enfatizando cómo las Administraciones públicas deben hacer uso de los recursos tecnológicos para lograr que su relación con la sociedad se produzca de manera cada vez más incluyente, transparente y eficiente[72].

II. La difícil conciliación y ponderación de los derechos de acceso a la información pública y a la protección de datos personales.

Las causas de inadmisión y los límites aplicables al derecho de acceso resultan en buena medida similares en el ámbito comparado, dejando a un lado las distancias marcadas por la eventual configuración, en su caso, de este último como derecho fundamental propiamente constitucional o, por el contrario, como derecho subjetivo de configuración meramente legal. Encuentra así un límite importante en lo que atañe al derecho de los eventualmente afectados por la divulgación de la información solicitada a la protección de sus datos personales, planteando incógnitas de gran complejidad que

[70] Martín Delgado (2018: 188 y ss.) incide en que "en el contexto de la revolución tecnológica, la información fluye de forma rápida y sencilla y, en la mayor parte de los casos, se encuentra en poder de la Administración". Sostiene que "ello ha de derivar, necesariamente, en una inversión de los términos y, en consecuencia, ha de afectar a la forma en la que la Administración actúa", propugnando, en concreto, la inversión de "la carga de obtención de la información" y defendiendo que "puede prescindirse del procedimiento en determinados supuestos", por ejemplo, ante solicitudes de acceso a información pública cuando no concurran otros derechos o intereses, públicos o privados, de forma que la información haya de ser facilitada sin necesidad de ponderar límites.

[71] Souza y Costa (2023: 140) hacen hincapié, por ejemplo, en las posibilidades de mejora que brinda la reutilización de la información pública, cuyo uso puede dar lugar a la creación de aplicaciones innovadoras, por ejemplo, en el ámbito de *startups* u organizaciones del tercer sector, dedicadas a analizar y generar inteligencia de los datos públicos, complementando los usos gubernamentales de estos datos y contribuyendo a generar "nuevas soluciones a problemas complejos".

[72] Souza y Costa (2023: 139).

suelen ser abordadas por los distintos ordenamientos jurídicos internacionales recurriendo a la inevitable ponderación de derechos en liza.

Conviene subrayar desde un primer momento que pese a la generosidad con que ha tendido a definirse el dato personal y a extendérsele el manto protector de los distintos ordenamientos jurídicos frente a la incesante innovación tecnológica y su progresiva implantación en todas las facetas de la vida y actividad humanas, en particular, la pública[73], la protección de datos no se ha erigido con carácter general en límite total o absoluto a la transparencia pública[74]. Al igual que sucede con otros derechos, por ejemplo, al honor, la intimidad y la propia imagen, según las circunstancias del caso concreto puede llegar a ceder en caso de colisión con otros derechos ante la necesidad de preservar otros bienes jurídicos. En este sentido, la ley española no ha sancionado la subordinación de un derecho, el de acceso, frente al otro, la protección de datos personales, sino más bien el mandato de conciliar su ejercicio arribando a un adecuado punto de equilibrio entre ambos[75].

La complejidad del enunciado legal, los factores que deben tomarse en consideración a efectos de determinar si procede dar acceso o no a la información solicitada, el carácter restrictivo con que deben interpretarse los límites del derecho de acceso regulado por la Ley 19/2013[76], avalado, por lo demás, por la doctrina de los órganos de garantía que se han constituido en materia de transparencia y sancionado por la propia jurisprudencia del Tribunal Supremo[77], abocan al operador jurídico y, en particular, al organismo obligado a resolver sobre una solicitud concreta de acceso a una

[73] Vid. a tal respecto Menéndez Margolles (2020: 463 y ss.), para quien, pese al paternalismo de la regulación aplicable en el ámbito europeo, "la protección del dato ni es actualmente desmedida ni será nunca suficiente".

[74] Quizá fuera imposible que lo hiciera en puridad en la práctica. No en vano, el aumento de la libertad de expresión y de la transparencia informativa entendida en sentido lato, es decir, más allá de la exigible *stricto sensu* a los poderes, instituciones u organismos públicos, ha traído consigo atropellos motivados por la proliferación de foros, blogs, redes sociales y aplicaciones diversas en que cualquier sujeto puede hacer llegar su mensaje a millones de usuarios de internet. En este sentido, para Escandón Prada (2017: 241) "las intromisiones en la privacidad y la protección de datos hablan de los efectos más injustos de una transparencia descontrolada".

[75] Se refiere, en concreto, al "sintomático dilema" sobre la creación de uno o dos órganos de control al respecto, López Calvo (2020: 382 y ss.), quien refiere como la duplicidad se palía con coordinación, si bien en ocasiones "situaciones conexas y relacionadas tanto con protección de datos como con transparencia se someten indistintamente a ambos órganos".

[76] Es importante reseñar que, de conformidad con el art. 5.3 de la ley, son límites aplicables también a las obligaciones de publicidad activa impuestas por la norma. Cabe citar, en este sentido y a título de ejemplo, la Sentencia del Tribunal Superior de Justicia de la Comunidad Valenciana de 18 de noviembre de 2019 (rec. 30/2018), que sanciona cómo en el control de la obligación de publicidad activa se debe ponderar con el derecho de acceso y la protección de datos al someter a revisión jurisdiccional la excusa pública de proteger los datos personales contenidos en las memorias justificativas de las subvenciones para soslayar la obligación legal de publicidad activa que pesa sobre los convenios y las citadas memorias.

[77] Ha destacado, entre otras, en su Sentencia de 16 de octubre de 2017 (rec. 75/2017), que la "formulación amplia en el reconocimiento y en la regulación legal del derecho de acceso a la información obliga a interpretar de forma estricta, cuando no restrictiva, tanto las limitaciones a ese derecho que se contemplan en el artículo 14.1 de la Ley 19/2013 como las causas de inadmisión de solicitudes de información que aparecen enumeradas en el artículo 18.1". Una doctrina que ha reiterado, asimismo, en sentencias posteriores, entre otras, las de de 16 de diciembre de 2019 (rec. 316/2018), así como 3 de marzo (rec. 600/2018) y 11 de junio de 2020 (rec. 577/2019).

delicada tarea de ponderación entre los intereses eventualmente enfrentados y los posibles derechos subyacentes a cada caso particular[78].

Y así, a nuestros efectos concretos, el artículo 15 de la Ley 19/2013 cataloga la información personal en función de la esfera concreta de la intimidad personal a que afecte y de su conexión, en última instancia, con el núcleo de mayor protección en relación con la propia privacidad[79]. Si la información solicitada contuviera datos especialmente protegidos relativos a la ideología, afiliación sindical, religión o creencias del afectado, sólo se autorizará el acceso en caso de contar con su consentimiento expreso y por escrito, a menos, claro está, que con anterioridad a la solicitud de acceso el propio afectado hubiese hecho "manifiestamente públicos" los datos en cuestión.

Si la información incluyese, en cambio, datos especialmente protegidos en relación con el origen racial, la salud o vida sexual del afectado, contuviese datos genéticos o biométricos o relativos a la comisión de infracciones penales o administrativas que no conllevasen la amonestación pública al infractor, el acceso requerirá consentimiento expreso del afectado, sin que en este caso la ley lo demande por escrito, o norma con rango de ley que lo ampare[80].

Para el resto de los supuestos que pudieran plantearse, esto es, solicitudes de información que incluyan o afecten a datos personales no especialmente protegidos, el órgano al que se dirija la solicitud estará abocado a una ponderación previa, conforme a los propios criterios que, con carácter abierto y no taxativo, determina a este efecto el legislador, acerca de la posible prevalencia de la protección de datos personales u otros derechos constitucionalmente protegidos sobre el interés público en la divulgación de la información solicitada. Entre los citados criterios se establecen, particularmente, los siguientes[81]:

[78] Incide en ello de forma harto elocuente Neira Barral (2022: 19): "Y digo esto siendo un acérrimo defensor de la transparencia y consciente de que la batalla pugilística (como describe el profesor Lorenzo Cotino) que mantiene el peso pesado de la protección de datos -ley orgánica- frente al peso pluma del derecho de acceso a la información -ley ordinaria-, de momento, parece que se pierde, y aunque mantengamos el empeño en la defensa del débil, esto no puede ser excusa para el 'vale todo'. El término clave que viene dibujándose para compensar el citado desequilibrio resulta del ejercicio de ponderación que realizarán los órganos de control. Así pues, si nos acogemos a la ponderación, esta vendrá determinada por el caso concreto y avalada por lo que digan las normas y el mayor interés general, siendo lo lógico volcarse hacia el lado de la transparencia y publicidad cuando más cerca nos encontremos, por ejemplo, de la toma de decisiones, que es lo que debería interesar al ciudadano."

[79] En todo caso este precepto debe ponerse en su debido contexto. Como bien señala López Calvo (2020: 386) la información a obtener tras ejercer el acceso depende de la posición jurídica del solicitante pudiéndose catalogar cuatro situaciones diferentes en función de que la solicite como interesado según la Ley 39/2015, de 1 de octubre, al amparo de normativa específica, en aplicación del principio general de transparencia o del principio de transparencia "preferente" como "interesado" en actuaciones sectoriales.

[80] Fernández Ramos y Pérez Monguió (2020: 320 y ss.) profundizan en el acceso a información pública que contenga datos de categorías especiales una vez fallecido el titular del dato personal.

[81] Profundiza en ellos Guichot (2019: 94 y ss.), para quien su incorporación trasluce "un intento de aportar más luz al aplicador, tan encomiable como errado". Vid., asimismo, sobre los criterios legales de ponderación, con mayor profundidad, Fernández Ramos y Pérez Monguió (2020: 337 y ss.), quienes apuntan a otros tres posibles criterios a emplear a tal efecto por el órgano competente, en concreto, la relevancia pública del titular de los datos personales, la titularidad de un interés legítimo por parte del solicitante y el tiempo transcurrido desde la elaboración o recepción de la información pública.

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[82].

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 contuviesen datos de carácter meramente identificativo de aquéllos.

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, o se refieran a menores de edad.

Fijadas de este modo las coordenadas respecto a la protección de datos personales como eventual límite a la transparencia del sector público regulada por la Ley 19/2013, ¿qué criterios pesan en la ponderación para decidir si el acceso tiene precedencia frente a otros derechos que pudieran erigirse en límite para la divulgación de la información pública? Aunque pueden sistematizarse y subdividirse, ofreciendo pautas más concretas, cabe reconducirlos fundamentalmente al potencial ofensivo que la información suministrada pudiera representar para los derechos de la personalidad y al interés público consustancial a que aparezca vinculada, en su caso, a los datos personales del interesado.

A falta de soluciones jurídicas que automaticen la respuesta al conflicto, el principio de proporcionalidad se revela sin duda en estos supuestos como herramienta esencial para constatar si la posible divulgación de la información personal pudiera quebrar la legitimidad del acceso a la información pública correspondiente que, aunque restrictivo del derecho fundamental, pudiera hallarse amparado, a su vez, conforme establece la jurisprudencia constitucional, por juicios de idoneidad, como "susceptible de conseguir el objetivo propuesto", necesidad, porque "no exista otra medida más moderada para la consecución de tal propósito con igual eficacia" y equilibrio, "por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto"[83]. Se alza así como un límite negativo del decisor[84].

[82] Se refiere, en concreto, a los plazos dispuestos a tal efecto por el art. 57.1 c) de la Ley 16/1985 para la consulta pública de documentos constitutivos del Patrimonio Documental Español que contengan "datos personales de carácter policial, procesal, clínico o de cualquier otra índole que puedan afectar a la seguridad de las personas, a su honor, a la intimidad de su vida privada y familiar y a su propia imagen" y que, salvo mediar consentimiento expreso de los afectados, alcanza al transcurso de un plazo veinticinco años desde su muerte, si su fecha es conocida o, en otro caso, de cincuenta años, a partir de la fecha de los documentos. Guichot (2019: 95) ha calificado de "despropósito" la acogida de este criterio.

[83] Resulta de gran interés a estos efectos la Sentencia de la Audiencia Nacional de 26 de marzo de 2019 (rec. 11/2017), que en su fundamento de derecho quinto argumenta cómo las obligaciones de transparencia activa relativas a la información institucional y presupuestaria no justifican en el caso concreto la publicidad de datos personales de los funcionarios afectados, encontrándose asimismo sujeta a los límites fijados por el art. 15 de la ley para conciliar derechos de acceso a la información pública y de protección de datos personales. A estos efectos, cobra especial trascendencia, a efectos de la ponderación, el puesto profesional ocupado en la Administración.

[84] Así lo afirma Ponce Solé (2020: 108), para quien el ordenamiento jurídico ofrece, además, "una orientación en positivo para la ponderación, derivada del derecho a una buena administración".

El conflicto entre derecho fundamental a la protección de datos y derecho de acceso a la información pública no supone cerrar la puerta al segundo cada vez que pudiera verse comprometido el primero, sino que implica, en realidad, valorar y ponderar intereses y derechos concurrentes y contrapuestos[85]. Toda la teoría de los derechos humanos y libertades fundamentales se erige sobre roces, fricciones y tensiones similares. Como pusiera de manifiesto Hegel, las verdaderas tragedias no resultan del enfrentamiento entre derecho e injusticia, sino del choque entre dos derechos. La balanza es conocida y su empleo consustancial al reconocimiento de derechos.

En todo caso, la aludida ponderación debe ponerse necesariamente en relación con lo dispuesto, asimismo, en los apartados segundo y cuarto del artículo 15 de la Ley 19/2013, donde se establece que "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"[86], sancionándose, además, que "no será de aplicación 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"[87].

Cabe entender, en relación con este último supuesto, que el legislador remite, en realidad, a la anonimización de la información, esto es, al tratamiento de los datos personales para que el nuevo conjunto de datos resultante, la información anonimizada, no guarde relación con una persona física identificada o identificable[88], y no a su seudonimización, que resultaría asimismo posible pero mucho más compleja, obligando, con toda seguridad, a una reelaboración de la información pública solicitada[89] en tanto exige, conforme al art. 4.5 del Reglamento General de Protección de Datos de la Unión Europea, "el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a

[85] Rodotà (2014: 17) incide, a tal efecto, en la necesidad de lograr un adecuado equilibrio entre los derechos a la protección de datos personales y al acceso a la información pública, pues "no puede ser dejado sólo a la deontología profesional, a la dinámica mercantil, a los intereses privados o a la idea de que los secretos de Estado deben ser protegidos".

[86] Guichot (2019: 90) refiere como la adición "meramente identificativos" es susceptible de "complicar el entendimiento del precepto y, llegado el caso, propiciar una gran cerrazón a la transparencia de la actuación pública". Vid., con mayor profundidad, Fernández Ramos y Pérez Monguió (2020: 324 y ss.).

[87] Apartado que cabría considerar tautológico en expresión de Guichot (2019: 102).

[88] Conforme al considerando 26 del Reglamento General de Protección de Datos de la Unión Europea, los principios de protección de datos no resultan aplicables "a la información anónima, es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo. En consecuencia, el presente Reglamento no afecta al tratamiento de dicha información anónima, inclusive con fines estadísticos o de investigación."

[89] El considerando 28 del propio Reglamento General de Protección de Datos de la Unión Europea reconoce que su aplicación "puede reducir los riesgos para los interesados afectados", si bien no los elimina, a la par que ayuda a los responsables y encargados del tratamiento a cumplir con sus obligaciones de protección de los datos, por lo que su introducción explícita en el Reglamento "no pretende excluir ninguna otra medida relativa a la protección de datos".

garantizar que los datos personales no se atribuyan a una persona física identificada o identificable"[90].

El Criterio Interpretativo 2/2015, de 24 de junio, aprobado conjuntamente para su ámbito de actuación respectivo por el Consejo de Transparencia y Buen Gobierno y la Agencia Española de Protección de Datos en aplicación de lo dispuesto en la disposición adicional quinta de la Ley 19/2013, se refiere, por lo demás, a la aplicación de los límites al derecho de acceso a la información que contienen los arts. 14 y 15 de la Ley 19/2013, de 9 de diciembre, expresando en sus antecedentes la preocupación del Consejo de Transparencia y Buen Gobierno por cuanto "viene observando una interpretación extensiva de los conceptos contenidos en determinados límites respecto de los cuales resulta conveniente identificar y precisar los criterios y condiciones que justifican su aplicación". Pese a las incógnitas planteadas por el propio ámbito de aplicación de estos criterios de interpretación uniforme de las obligaciones contenidas en la Ley 19/2013, de 9 de diciembre, adoptados por el Presidente del Consejo de Transparencia y Buen Gobierno[91], son sin duda "valiosos por su carácter informador en una materia novedosa y con escaso recorrido doctrinal y jurisprudencial", encontrándose "sujetos, en última instancia, a la interpretación que, en ejercicio de la función jurisdiccional, ejerzan jueces y tribunales, así como a una distinta y razonada aplicación de la norma por los sujetos incluidos en su ámbito de aplicación"[92].

Concreta los criterios de aplicación de las reglas contenidas en el art. 15 de la Ley 19/2013, en particular, en lo que respecta a la ponderación del interés público en el acceso a la información y la garantía de los derechos de los interesados cuyos datos se contuviesen en la misma, de conformidad con lo dispuesto no solo en la propia ley de 2013 sino, en particular, en la legislación aplicable en materia de protección de datos.

En primer lugar, enuncia las etapas o fases sucesivas que comprende la aplicación de los límites que establecen ambos preceptos, arts. 14 y 15, ordenándolas en función de su prelación temporal. Y así, se debe:

> «I. Valorar si la información solicitada o sometida a publicidad activa contiene o no datos de carácter personal, entendiéndose por estos los definidos en el artículo 3 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, LOPD)[93].
>
> II. En caso afirmativo, valorar si los datos son o no datos especialmente protegidos en los términos del artículo 7 de la LOPD, esto es: a) Datos reveladores de la ideología, afiliación sindical, religión y creencias; b) Datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual, y c) Datos de

[90] Vid. Menéndez Margolles (2020: 471 y ss.).

[91] *Ex* art. 38.2 a) de la Ley 19/2013. El art. 8.2 b) del Estatuto del Consejo de Transparencia y Buen Gobierno, aprobado por Real Decreto 919/2014, de 31 de octubre, introduce como requisito adicional el informe previo a su adopción de la Comisión de Transparencia y Buen Gobierno. Curiosamente, no todas las instituciones representadas en esta última Comisión están sujetas a los pronunciamientos del Consejo ante una eventual reclamación presentada en materia de acceso, suscitándose con ello la paradoja respecto a la falta de coincidencia entre los ámbitos subjetivos de aplicación de la ley y de los eventuales criterios interpretativos y los organismos sujetos a la nueva reclamación potestativa en materia de transparencia contra resoluciones en materia de acceso a la información pública solicitada.

[92] Neira Barral (2022: 96).

[93] Actualmente, Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

carácter personal relativos a la comisión de infracciones penales o administrativas. Si contuviera datos de carácter personal especialmente protegidos, la información solo se podrá publicar o facilitar: a) En el supuesto de los datos de la letra a) anterior, cuando se cuente 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. b) En el supuesto de los datos de la letra b) anterior, cuando se cuente con el consentimiento expreso del afectado o estuviera amparado por una norma con rango de Ley, y c) En el supuesto de los datos de la letra c) anterior, y siempre que las correspondientes infracciones penales o administrativas no conlleven la amonestación pública al infractor, cuando se cuente con el consentimiento expreso del afectado o estuviera amparado por una norma con rango de Ley,

III. Si los datos de carácter personal contenidos en la información no fueran datos especialmente protegidos, valorar si son o no exclusivamente datos meramente identificativos relacionados con la organización, el funcionamiento o la actividad pública del órgano o entidad correspondiente. Si los datos contenidos son exclusivamente identificativos relacionados con la organización, el funcionamiento o la actividad pública del órgano o entidad, la información se publicará o facilitará con carácter general, salvo que en el caso concreto prevalezca la protección de datos personales y otros derechos constitucionalmente protegidos sobre el interés público en la divulgación.

IV. Si los datos de carácter personal no fueran meramente identificativos y relacionados con la organización, el funcionamiento o la actividad pública del órgano o no lo fueran exclusivamente, efectuar la ponderación prevista en el artículo 15 número 3 de la LTAIBG[94].

V. Finalmente, una vez realizados los pasos anteriores, valorar si resultan de aplicación los límites previstos en el artículo 14.»

El Consejo de Transparencia y Buen Gobierno y la Agencia Española de Protección de Datos subrayan, en conclusión, que los límites del derecho de acceso a la información *ex* arts. 14 y 15 "no operan de forma automática, sino que habrán de ser aplicados de acuerdo con las reglas de aplicación y los elementos de ponderación" que establecen tanto la ley de 2013 como la ley orgánica vigente en materia de protección de datos personales, afirmando de forma expresa que los límites ni operan "automáticamente a favor de la denegación ni absolutamente en relación a los contenidos".

Aclaran, en tal sentido, que "el orden de ponderación opera desde el art. 15 al 14 con valoración de los elementos que modulan la toma de decisiones", de manera que procedería analizar, en primer lugar, para garantizar su aplicación justificada y proporcional atendiendo a las circunstancias del caso concreto, si concurren datos personales susceptibles de protección que pudieran limitar el acceso y solo en caso de que procediera se pasaría a analizar la eventual concurrencia de alguno de los límites listados en el art. 14 que, a diferencia de los relativos a la protección de los datos de carácter

[94] Que apunta a unos criterios que el órgano "tomará *particularmente* en consideración", sin vedar, en cualquier caso, la valoración de otros diversos en su ponderación, en particular, de los test del daño y del interés público que cita expresamente el Criterio Interpretativo en relación con los límites del art. 14 de la Ley 19/2013.

personal, no se aplican directamente[95], sino tan solo tras analizar "si la estimación de la petición de información supone un perjuicio (*test del daño*) concreto, definido y evaluable" que de ninguna forma podrá afectar o ser relevando para un ámbito material concreto, "porque de lo contrario se estaría excluyendo un bloque completo de información". A ello se suma, en todo caso, la exigencia de examinar si concurre, además, un interés que justifique en el supuesto la publicidad o el acceso solicitado (*test del interés público*).

La aplicación de los límites deberá ser en cualquier caso justificada, motivándose la denegación y publicándose aquellas negativas dictadas en aplicación de los límites del art. 14, si bien con previa disociación de los datos de carácter personal que contuvieran y una vez que hubieran sido notificadas a los interesados. No se recoge, en cambio, una previsión similar para las resoluciones denegatorias recaídas al amparo del art. 15, seguramente por la dificultad de disociar completamente cualesquiera datos personales y, aún así, publicar una resolución que atendiendo a las circunstancias del caso pudiera resultar inteligible y comprensible acerca de las razones por las que se hubiera optado, a la vista del precepto y de la protección de los datos personales afectados, por desestimar la petición de acceso efectuada. Caso de proceder el acceso a la información, el art. 15.5 resulta meridianamente claro al sujetar, a su vez, el tratamiento posterior de los datos personales obtenidos a través del ejercicio del derecho de acceso a la normativa vigente en la materia (Reglamento General de Protección de Datos de la Unión Europea y Ley Orgánica 3/2018).

Interesa destacar que, desde una perspectiva meramente procedimental, el art. 19.3 de la Ley 19/2013 establece que "si la información solicitada pudiera afectar a derechos o intereses de terceros debidamente identificados, se les concederá un plazo de quince días para que puedan realizar las alegaciones que estimen oportunas. El solicitante deberá ser informado de esta circunstancia, así como de la suspensión del plazo para dictar resolución hasta que se hayan recibido las alegaciones o haya transcurrido el plazo para su presentación". Se trata de un trámite esencial, en tanto habrá de facilitar elementos para la debida consideración por parte del sujeto obligado de la solicitud de acceso a la información y de la eventual aplicación de alguno de los límites dispuestos a tal efecto por el legislador, en particular, del dispuesto en materia de protección de datos personales por el art. 15 de la ley[96].

En su Sentencia de 8 marzo de 2021 (rec. 3193/2019) el Tribunal Supremo ha sostenido al respecto que la finalidad perseguida con este trámite es que "las personas o entidades cuyos derechos o intereses puedan verse afectados por la información pública solicitada, y consecuentemente con la decisión que se adopte, puedan formular alegaciones". De ahí que "cuando en el procedimiento seguido ante el órgano administrativo no se ha dado trámite de audiencia a los interesados, si el Consejo de Transparencia tiene datos suficientes que permitían identificar a las personas o entidades cuyos derechos o intereses pudiesen verse afectados por la decisión que adopte, puede y

[95] Conforme al art. 16 de la ley, si no cupiera el otorgamiento del acceso a la totalidad de la información solicitada por aplicación de alguno de los límites previstos en el art. 14, que no afectara, sin embargo, a la totalidad de la información, se concederá acceso parcial previa omisión de aquella información que se viera afectada por el límite correspondiente, indicando al solicitante qué parte concreta de la información ha sido omitida y siempre a salvo de que de ello resultara una información distorsionada o que careciera de sentido.

[96] Y sin que quede condicionado, en cualquier caso, a que los interesados hayan sido oídos previamente en el procedimiento tramitado ante el órgano administrativo destinatario de la solicitud de acceso.

debe concederles un trámite de audiencia, con el fin de poder ponderar si el acceso a la información lesiona o no sus derechos o intereses. El trámite de audiencia ante el Consejo de Transparencia no se condiciona, por tanto, a que los interesados hayan sido oídos previamente en el procedimiento tramitado ante el órgano administrativo destinatario de la solicitud de información. La intervención del Consejo de Transparencia en fase de reclamación cuando constate que el órgano administrativo omitió el trámite de audiencia a los afectados puede adoptar las siguientes decisiones: a) si los interesados están identificados o son fácilmente identificables, debe conceder un trámite de audiencia a los afectados y después adoptar la decisión de fondo que pondere los intereses en conflicto; b) cuando desconozca la identidad de los afectados y no disponga de datos suficientes que le permitan una fácil identificación, puede ordenar la retroacción de actuaciones para que sea el órgano administrativo el que cumpla con el trámite de audiencia exigido por el art. 19.3 de la Ley de Transparencia".

Se trata, por tanto, de un trámite ineludible que habrá de ayudar a completar los elementos en manos del organismo correspondiente para ponderar los intereses o derechos en conflicto ante el eventual acceso a la información pública solicitada[97]. Con ocasión de este el tercero o terceros afectados pueden hacer las alegaciones que estimen oportunas, incluida su posible negativa a que se facilite la información con el fin de proteger sus derechos e intereses legítimos, por entender, en última instancia, que el acceso vulnera alguno de los límites previstos en los artículos 14 o 15 de la Ley 19/2013, en concreto, por lo que se refiere al segundo de los preceptos señalados, la protección de sus datos personales más allá de lo permitido al efecto por la adecuada conciliación e interpretación conjunta de la legislación aplicable en materia de transparencia y acceso a la información pública, de un lado, y de protección de datos personales, de otro.

V. BIBLIOGRAFÍA.

ABRIL, E., y PIZARRO MORENO, P. S. (2014): "La intimidad europea frente a la privacidad americana: una visión comparativa del derecho al olvido", *Indret*, núm. 1, 2014.

AGÚNDEZ LERÍA, I. (2010): "La protección de datos de carácter personal y la Agencia Española de Protección de Datos", en A. MORALES PLAZA, M. PARDO GONZÁLEZ y J. RODRIGO LAVILLA (coords.), *Tratado del sector público estatal*, Madrid, La Ley, pp. 938-978.

APARICIO SALOM, J. (2002): *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal*, Cizur Menor, Aranzadi.

ÁVILA, R. (2023): "La brecha digital en América Latina como barrera para el ejercicio pleno de derechos", en la obra colectiva *Derechos digitales en Iberoamérica: situación y* perspectivas, Madrid, Fundación Carolina y Telefónica, pp. 147-161.

BAÑO LEÓN, J. Mª. (2015): "La reforma del procedimiento. Viejos problemas no resueltos y nuevos problemas no tratados", *Documentación Administrativa*, núm. 2.

[97] Precisamente por ello la Sentencia de la Audiencia Nacional de 17 de julio de 2017 (rec. 40/2017) determina la improcedencia de denegar el acceso a la información solicitada alegando protección de datos (art. 15) e intereses comerciales [art. 14.1 h)] si no ha habido previamente un trámite de alegaciones a los interesados.

BELLO PAREDES, S. A. (2005): "Las Agencias de protección de datos en la sociedad de la información: un interesante ejemplo de actuación administrativa «tutelar» e «independiente»", en A. MURILLO VILLAR y S. A. BELLO PAREDES (coords.), *Estudios jurídicos sobre la sociedad de la información y nuevas tecnologías*, Burgos, Universidad de Burgos, pp. 135-150.

BETANCOR RODRÍGUEZ, A. (1994): *Las Administraciones independientes*, Madrid, Tecnos.

CANALES GIL, Á. (2007): "El derecho fundamental a la protección de datos de carácter personal", *Revista Jurídica de Castilla y León*, núm. 12, pp. 13-56.

CASARES MARCOS, A. (2012): *Principio de legalidad y ejercicio de la potestad administrativa sancionadora. En especial, la Administración institucional y las corporaciones de derecho público*, Sevilla, Instituto Andaluz de Administración Pública.

- (2016): "Novedades en materia de Administración electrónica en la nueva legislación administrativa básica", *Revista Jurídica de Castilla y León*, núm. 40, pp. 61-100.
- (2020): "Derecho al olvido en internet y autodeterminación informativa personal: el olvido está lleno de memoria", *Revista de Administración Pública*, núm. 212, pp. 401-438.

CASINO RUBIO, M. (2012): "El periódico de ayer, el derecho al olvido en internet y otras noticias", *Revista Española de Derecho Administrativo*, núm. 156, pp. 201-216.

CASTELFRANCHI, C. (2007): "Six critical remarks on science and the construction of the knowledge society", *Journal of Science Communication*, núm. 6, pp. 1-3.

CERRILLO i MARTÍNEZ, A. (2020): "La transparencia de los algoritmos que utilizan las Administraciones públicas", *Anuario de Transparencia Local*, núm. 3, pp. 41-78.

CHAVES, J. R. (2016): "El procedimiento administrativo común de la Ley 39/2015: nuevos forjados sobre viejos cimientos", *Actualidad Administrativa*, núm. 2.

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. 5-1, pp. 255-271.

CONDE ORTIZ, C. (2005): *La protección de datos personales. Un derecho autónomo con base en los conceptos de intimidad y privacidad*, Madrid, Dykinson.

DAVARA FERNÁNDEZ DE MARCOS, L., y DAVARA RODRÍGUEZ, M. Á. (2016): "Ley 39/2015, del Procedimiento Administrativo Común de las Administraciones Públicas: novedades en materia de Administración electrónica", *Actualidad Administrativa*, núm. 1.

DAVARA RODRÍGUEZ, M. Á. (2016): "Reglamento Europeo sobre Protección de Datos", *Actualidad Administrativa*, núms. 7-8.

DEL CASTILLO VÁZQUEZ, I.-C. (2007): *Protección de datos: cuestiones constitucionales y administrativas. El derecho a saber y la obligación de callar*, Madrid, Civitas.

DÍEZ-PICAZO, L. (1979): *Derecho y masificación social. Tecnología y Derecho privado (dos esbozos)*, Madrid, Civitas.

ESCANDÓN PRADA, V. (2017): "Privacidad, derecho al olvido y transparencia", en M. SÁNCHEZ DE DIEGO FERNÁNDEZ DE LA RIVA (coord.), *31 visiones actuales de la transparencia*, Madrid, DMK Consultores, Universidad Complutense de Madrid y Acreditra, pp. 240-250.

FERNÁNDEZ RAMOS, S. y PÉREZ MONGUIÓ, J. M. (2020): *El derecho de acceso a la información pública en España*, Cizur Menor, Aranzadi.

FERNÁNDEZ SALMERÓN, M. (2003): *La protección de los datos personales en las Administraciones públicas*, Madrid, Civitas.

GAMERO CASADO, E. (2016): "Panorámica de la Administración electrónica en la nueva legislación administrativa básica", *Revista Española de Derecho Administrativo*, núm. 175, pp. 15-27.

GUERRERO PICÓ, Mª. C. (2006): *El impacto de internet en el derecho fundamental a la protección de datos de carácter personal*, Madrid, Civitas.

GUICHOT, E. (2005): *Datos personales y Administración pública*, Madrid, Civitas.

- (2019): "Los límites de la transparencia y el derecho de acceso a la información", en I. MARTÍN DELGADO (dir.), *Transparencia y acceso a la información pública: de la teoría a la práctica*, Madrid, Iustel, pp. 55-105.

GUTIÉRREZ DAVID, M. E. (2021): "Administraciones inteligentes y acceso al código fuente y los algoritmos públicos. Conjurando riesgos de cajas negras decisionales", *Derecom*, núm. 30.

HERRÁN ORTIZ, A. I. (1998): *La violación de la intimidad en la protección de datos personales*, Madrid, Dykinson.

LÓPEZ CALVO, J. (2020): "La protección de datos como límite a la transparencia administrativa", en J. BERMÚDEZ SÁNCHEZ y A. DE MARCOS FERNÁNDEZ (coords.), *Transparencia, lobbies y protección de datos*, Cizur Menor, Aranzadi, pp. 381-409.

MANZANERO JIMÉNEZ, L., y PÉREZ GARCÍA-FERRERÍA, J. (2015): "Sobre el derecho al olvido digital: una solución al conflicto entre la libertad de información y el derecho de protección de datos personales en los motores de búsqueda", *Revista Jurídica Universidad Autónoma de Madrid*, núm. 32, pp. 249-258.

MARTÍN DELGADO, I. (2016): "La reforma de la Administración (electrónica): hacia una auténtica innovación administrativa", *Revista Democracia y Gobierno Local*, núm. 32, pp. 5-10.

- (2018): "El acceso electrónico a los servicios públicos: hacia un modelo de Administración digital auténticamente innovador", en T. DE LA QUEADRA-SALCEDO y J. L. PIÑAR MAÑAS (dirs.) y M. BARRIO ANDRÉS y J. TORREGROSA VÁZQUEZ (coords.), *Sociedad digital y Derecho*, Madrid, BOE, Ministerio de Industria, Comercio y Turismo y Red.es, pp. 179-201.

MARTÍNEZ MARTÍNEZ, R. (2004): *Una aproximación crítica a la autodeterminación informativa*, Madrid, Civitas.

MARTÍNEZ OTERO, J. Mª. (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, pp. 103-142.

MARTÍNEZ-ROJAS, Á. (2016): "Principales aspectos del consentimiento en el Reglamento General de Protección de Datos de la Unión Europea", *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 42, pp. 59-82.

MEDINA GUERRERO, M. (2022): "El derecho a conocer los algoritmos utilizados en la toma de decisiones. Aproximación desde la perspectiva del derecho fundamental a la protección de datos personales", *Teoría y Realidad Constitucional*, núm. 49, pp. 141-171.

MENÉNDEZ MARGOLLES, G. (2020): "Qué es dato personal y qué no lo es. ¿Hacia una protección desmedida del dato?", en J. BERMÚDEZ SÁNCHEZ y A. DE MARCOS FERNÁNDEZ (coords.), *Transparencia, lobbies y protección de datos*, Cizur Menor, Aranzadi, pp. 463-495.

MESEGUER YEBRA, J. e IBÁÑEZ PASCUAL, A. (2017): "Transparencia y acceso a la información pública en el nuevo contexto de la Administración electrónica", en J. PINTOS SANTIAGO (dir.), *La implantación de la Administración electrónica y de la e-factura*, Madrid, La Ley, pp. 19-71.

MINERO ALEJANDRE, G. (2014): "A vueltas con el 'derecho al olvido'. Construcción normativa y jurisprudencial del derecho de protección de datos de carácter personal en el entorno digital", *Revista Jurídica de la Universidad Autónoma de Madrid*, núm. 30, pp. 129-155.

MOURA VICENTE, D. (2019-2020): "¿Aplicación extraterritorial del derecho al olvido en internet?", *Anuario Hispano-Luso-Americano de Derecho Internacional*, vol. 24, 2019-2020, pp. 225-235.

MUÑOZ MACHADO, S. (2000): *La regulación de la red. Poder y Derecho en internet*, Madrid, Taurus.

MURILLO DE LA CUEVA, P. L. (2009): "La construcción del derecho a la autodeterminación informativa y las garantías para su efectividad", en P. L. MURILLO DE LA CUEVA y J. L. PIÑAR MAÑAS, *El derecho a la autodeterminación informativa*, Madrid, Fundación Coloquio Jurídico Europeo, pp. 11-80.

MURILLO DE LA CUEVA, P. L., y PIÑAR MAÑAS, J. L. (2009): *El derecho a la autodeterminación informativa*, Madrid, Fundación Coloquio Jurídico Europeo.

NEIRA BARRAL, D. (2022): *Transparencia de las Administraciones públicas y acceso a la información*, A Coruña, Colex.

PÉREZ CAMBERO, R. (2016): "Análisis de las últimas e importantes novedades en protección de datos: Reglamento Europeo de Protección de Datos y Escudo de Privacidad UE-EEUU", *Actualidad Administrativa*, núm. 11.

PIÑAR MAÑAS, J. L. (2008a): *¿Existe la privacidad? Inauguración Curso Académico 2008-2009*, Madrid, CEU Ediciones.

- (2008b): "El derecho fundamental a la protección de datos personales. Contenido esencial y retos actuales. En torno al nuevo Reglamento de Protección de Datos", en J. L. PIÑAR MAÑAS y Á. CANALES GIL, *Legislación de Protección de Datos*, Madrid, Iustel.

PIÑAR MAÑAS, J. L. (dir.) y ÁLVAREZ CARO, M. y RECIO GAYO, M. (coords.) (2016): *Reglamento General de Protección de Datos: hacia un nuevo modelo europeo de privacidad*, Madrid, Reus.

PONCE SOLÉ, J. (2020): "El derecho a una buena administración y los principios jurídicos de buen gobierno", en J. BERMÚDEZ SÁNCHEZ y A. DE MARCOS FERNÁNDEZ (coords.), *Transparencia, lobbies y protección de datos*, Cizur Menor, Aranzadi, pp. 81-143.

QUINTANA DAIMIEL, A. (2015): "Análisis preliminar de la nueva Ley Reguladora del Sector Público", *Actualidad Administrativa*, núm. 11.

RALLO LOMBARTE, A. (2002): *La constitucionalidad de las Administraciones independientes*, Madrid, Tecnos.

RODOTÀ, S. (2014): "Las lecciones de Wikileaks: nueva transparencia y nueva distribucion del poder", en J. L. Piñar Mañas (dir.), *Transparencia, acceso a la información y protección de datos*, Madrid, Editorial Reus, pp. 9-18.

RODRÍGUEZ-PIÑERO BRAVO-FERRER, M. (2016): "La nueva Ley de Régimen Jurídico del Sector Público", *Diario La Ley*, núm. 8696.

SALVADOR CODERCH, P. (1987): *¿Qué es difamar? Libelo contra la Ley del Libelo*, Madrid, Civitas.

SÁNCHEZ SÁNCHEZ, Z. (2016): "Las nuevas Leyes de Régimen Jurídico y Procedimiento Administrativo: afianzamiento de la Administración electrónica en las relaciones internas de la Administración y con los ciudadanos", en R. RIVERO ORTEGA, Mª. D. CALVO SÁNCHEZ y M. FERNANDO PABLO (dirs.), *Instituciones de Procedimiento Administrativo Común. Novedades de la Ley 39/2015*, Lisboa, Juruá.

SANCHO LÓPEZ, M. (2018): "Garantías legales del concepto de privacidad: entre el derecho al olvido y el nuevo Reglamento Europeo de Protección de Datos", *Actualidad Jurídica Iberoamericana*, núm. 9, pp. 176-201.

- (2019): "El derecho al olvido y las hemerotecas digitales. Breve recorrido por la jurisprudencia española", *Actualidad Jurídica Iberoamericana*, núm. 10 bis, pp. 748-759.

SANTAMARÍA PASTOR, J. A. (2015): "Los proyectos de ley del procedimiento administrativo común de las Administraciones públicas y de régimen jurídico del sector público: una primera evaluación", *Documentación Administrativa*, núm. 2.

SELIGRAT GONZÁLEZ, V. M. (2015): "El 'derecho al olvido digital'. Problemas de configuración jurídica y derivados de su incumplimiento a la vista de la Sentencia del Tribunal Supremo de 15 de octubre de 2015", *Actualidad Civil*, núm. 12, pp. 62-71.

SERRANO PÉREZ, Mª. M. (2003): *El derecho fundamental a la protección de datos. Derecho español y comparado*, Madrid, Civitas.

SIDHU, D. S. (2014): "Privacy Doesn't Exist in a Vacuum", *U.S. News & World Report*.

SOUZA, C. A. y COSTA, J. (2023): "Participación cívica y relaciones con la Administración pública en el marco de su innovación tecnológica", en la obra colectiva *Derechos digitales en Iberoamérica: situación y* perspectivas, Madrid, Fundación Carolina y Telefónica, pp. 121-145.

TONIATTI, R. (1991): "Libertad informática y derecho a la protección de los datos personales: principios de legislación comparada", *Revista Vasca de Administración Pública*, núm. 29, pp. 139-162.

TORNOS MAS, J. (2008): "Potestad sancionadora de la Agencia Española de Protección de Datos y principio de proporcionalidad", en *La potestad sancionadora de la Agencia Española de Protección de Datos*, Cizur Menor, Aranzadi, pp. 33-50.

TRONCOSO REIGADA, A. (2008): *La protección de datos personales. En busca del equilibrio*, Valencia, Tirant lo Blanch.

- (2009): "Las Agencias de Protección de Datos como Administración independiente", en C. PAUNER CHULVI y B. TOMÁS MALLÉN (coords.), *Las Administraciones independientes*, Valencia, Tirant lo Blanch, pp. 27-216.