Seguridad, transparencia y protección de datos: el futuro de un necesario e incierto equilibrio

José Luis Piñar Mañas

Documento de trabajo 147/2009

José Luis Piñar Mañas

Doctor en Derecho. Catedrático de Derecho administrativo de las Universidades de Castilla-La Mancha (excedente) y CEU-San Pablo de Madrid, de cuyas facultades de Derecho ha sido decano. Ha sido director de la Agencia Española de Protección de Datos, vicepresidente del Grupo Europeo de Autoridades de Protección de Datos y presidente-fundador de la Red Iberoamericana de Protección de Datos, de la que es presidente honorario. Presidente de la Junta de Garantías Electorales del Consejo Superior de Deportes. Abogado. *Adjunct Professor of Law* de la Georgetown University (2005-2007). Profesor invitado de las Universidades de Florencia, Bolonia, Pisa, Macerata, Lusiada de Lisboa, Guadalajara (México), Católica de La Plata (Argentina), Rio Grande do Sul (Brasil) y Segio Arboleda (Colombia). Premio de Investigación San Raimundo de Peñafort, de la Real Academia de Jurisprudencia y Legislación (1997). Es autor de numerosas publicaciones sobre Derecho público y ha impartido numerosas conferencias en España, Europa, América y Australia. Miembro de los consejos de redacción de diversas revistas especializadas en Derecho público, de la Junta Directiva de la Asociación Española de Profesores de Derecho Administrativo, de la Asociación Italo-Española de Profesores de Derecho Administrativo y de la *International Association of Privacy Professionals*. Miembro del Consejo Asesor de la Asociación Española de Fundaciones y de la Comisión Jurídica Asesora del Consejo General de la Abogacía Española.

ISBN: 978-84-92424-66-5

Depósito Legal: M-16015-2009

Impreso en papel ecológico

Contenido

Siglas y abreviaturas

BOE	Boletín Oficial del Estado
CEDH	Convenio Europeo de Derechos Humanos
CGPJ	Consejo General del Poder Judicial
LOPD	Ley Orgánica de Protección de Datos
PNR	*Passenger Name Record* (registro de nombre de los pasajeros)
STPI	Sentencia del Tribunal de Primera Instancia de las Comunidades Europeas
STS	Sentencia del Tribunal Supremo
TJCE	Tribunal de Justicia de las Comunidades Europeas
UE	Unión Europea

resumen ejecutivo

Seguridad, transparencia y protección de datos: el futuro de un necesario e incierto equilibrio

José Luis Piñar Mañas
Catedrático de Derecho Administrativo

El presente documento, que gira en torno a tres derechos fundamentales, esenciales en cualquier sociedad democrática avanzada (protección de datos, seguridad y transparencia), pretende descifrar algunas de las claves que configuran la tensión entre las exigencias de seguridad ciudadana, la necesaria implantación de una cultura de la transparencia y el respeto al derecho a la protección de datos.

La Carta de los Derechos Fundamentales de la Unión Europea reconoce expresamente el derecho fundamental a la seguridad (art. 6), el derecho a la protección de datos de carácter personal (art. 8) y el derecho de acceso a los documentos (art. 42). La Constitución Española recoge el primero en el art. 17.1, mientras que el derecho a la protección de datos deriva del art. 18.4 y el derecho a la transparencia de los arts. 20, 23 y 105.b).

El derecho a la protección de datos atribuye al titular un poder de disposición sobre sus propios datos personales y se configura como un derecho autónomo e independiente del derecho a la intimidad. Hoy está sometido a constantes amenazas derivadas del uso de las nuevas tecnologías, que permiten el tratamiento masivo de datos personales y nos sitúan en una sociedad constantemente vigilada. Además, razones de seguridad, no siempre justificadas ni contrastadas, pretenden habilitar la adopción de medidas altamente intrusivas para la protección de datos. En este escenario, debe alcanzarse el justo equilibrio entre seguridad y protección de datos partiendo de las siguientes premisas:

- Es falsa la pretendida contradicción entre seguridad y libertad y entre seguridad y protección de datos.
- Los poderes públicos deben adoptar medidas para garantizar la seguridad pública.
- Las medidas que se adopten deben ser necesarias y proporcionadas.
- Tales medidas deben ser respetuosas con los derechos fundamentales y, en particular, con la protección de datos.

- Deberán respetar los principios configuradores del contendido esencial del derecho a la protección de datos: habilitación legal suficiente, información, finalidad, calidad del dato, seguridad y control independiente.

Las exigencias de la seguridad pública junto con la protección de datos personales pueden llevar a una sociedad enormemente opaca. La información puede considerarse de acceso restringido, cuando no imposible, bien por hipotéticos motivos de seguridad, bien en aras de un pretendido respeto a la privacidad. Por ello, junto con la seguridad y la protección de datos, es necesario incorporar el derecho a la transparencia.

España, aislada en el entorno europeo, carece de una ley de transparencia y acceso a la información. El art. 37 de la Ley 30/1992 es a todas luces insuficiente y la legislación sectorial no acierta a resolver los problemas. Gran parte de las situaciones de corrupción que se producen (sobre todo en el ámbito del urbanismo) se deben a la falta absoluta de transparencia en los sectores afectados, que se escuda a menudo en la legislación de protección de datos, utilizada como excusa para no facilitar la información requerida.

Transparencia y protección de datos tampoco son contradictorias, pero, al igual que en el caso de la seguridad, es preciso buscar el necesario equilibrio entre ambos derechos.

La seguridad y la protección de datos amparan excepciones al acceso a la información, que deben ser interpretadas de acuerdo con los siguientes principios:

- El acceso a los documentos constituye el principio jurídico y la posibilidad de denegación es la excepción.

- Las excepciones deben interpretarse y aplicarse de forma estricta, "a la luz del principio del derecho a la información y del principio de proporcionalidad".

- La decisión sobre el acceso a los documentos que contengan datos personales debe resultar de una ponderación de los derechos e intereses en juego.

- Las excepciones deben estar expresamente previstas en la ley.

Pese a que el debate político en torno a la necesidad de incrementar la transparencia en nuestro sistema democrático es escaso, debe aprobarse cuanto antes una ley de transparencia. Dicha ley (para cuya aprobación el Estado tiene competencia según los apartados 1 y 18 del art. 149.1 de la Constitución) debe regular, al menos, los siguientes aspectos: objeto, ámbito subjetivo, sujetos legitimados, excepciones, procedimiento, sanciones y responsabilidad, autoridad independiente de supervisión y tutela del derecho. Entre las excepciones ha de prestarse especial atención a las que guarden relación con la seguridad pública y la protección de datos personales. Por otra parte, sería aconsejable que las Agencias de Protección de Datos asumiesen las competencias de tutela del derecho de acceso.

1. Introducción. Planteamiento general. El derecho a la protección de datos de carácter personal

El presente documento gira en torno a tres derechos fundamentales que son esenciales en la configuración de cualquier sociedad democrática avanzada: el derecho a la protección de datos, el derecho a la seguridad y el derecho a la transparencia. Pretende descifrar algunas de las claves que configuran la tensión existente entre las exigencias de seguridad ciudadana, la necesaria implantación de una cultura de la transparencia y el respeto al derecho a la protección de datos de carácter personal.

El derecho a la protección de datos está hoy ampliamente regulado en el marco de la Unión Europea y en todos y cada uno de los Estados miembros. España no es una excepción, y posee una de las legislaciones más garantistas y uno de los sistemas de tutela más eficaces.

Pero la protección de datos está sometida a innumerables retos[1], entre los que podemos destacar los siguientes: protección de datos frente a: a) libertad de expresión; b) transparencia y acceso a la información; c) intereses y evolución del mercado; d) garantía de la seguridad ciudadana y lucha contra el terrorismo; e) proceso de globalización e inexistencia de instrumentos (no sólo normativos) que permitan garantizar la eficacia del derecho frente a ataques que no saben de límites fronterizos y que provienen en innumerables ocasiones de países carentes en absoluto de un marco jurídico de protección de la privacidad y en los que, por tanto, es imposible intentar siquiera poner en marcha mecanismos eficaces de reacción y tutela.

Al analizar estos retos ha de partirse de una premisa común a todos ellos: no existe en absoluto una contradicción entre tales derechos o situaciones (libertad de expresión, transparencia, seguridad…) y la protección de datos. Más bien al contrario: sólo respetando el derecho fundamental de todos a la protección de datos personales se conseguirá un marco adecuado de respeto a la libertad de expresión y al derecho de acceso a la información; un correcto desarrollo del mercado y una eficaz lucha contra el terrorismo.

1 Que ya tuve ocasión de exponer en la XXVII Conferencia Internacional de Autoridades de Protección de Datos, celebrada en Montreux los días 13 a 15 de septiembre de 2005 y que he recordado recientemente en Piñar Mañas (2008a:90 y ss.).

Dicho lo anterior, de entre los retos que se acaban de enumerar, el presente documento se centra en dos: la tensión entre protección de datos y seguridad y la que se produce entre protección de datos y transparencia.

1.1 El derecho a la protección de datos

Ya es un lugar común señalar que estamos viviendo un momento en el que, fundamentalmente como consecuencia de la aplicación de las nuevas tecnologías, es posible recabar ingentes cantidades de datos sobre cualquier persona y obtener información a veces vital sobre ella y su entorno. Se ha llegado a decir (Scott McNealy, CEO de Sun Microsystems), con tanta ironía como convencimiento, que carecemos de privacidad y que hemos de resignarnos a ello (*"You already have zero privacy. Get over it"*), o que si hoy disponemos de intimidad es porque alguien tolera que la tengamos.

Por ello, en los últimos años se han aprobado numerosas leyes reguladoras del derecho a la protección de datos de carácter personal. Europa es en este sentido referencia obligada: todos los países de la Unión Europea cuentan con legislación sobre la materia. Pero la protección de datos, o el respeto a la privacidad, van ganando espacio también más allá de las fronteras europeas. Están en marcha procesos normativos en varios países iberoamericanos, en los que estos temas van siendo regulados cada vez con más extensión en textos legales (o incluso se aprueban reformas constitucionales, como ha ocurrido recientemente en México, donde el 12 de diciembre de 2008 se aprobó la adición de un nuevo párrafo al artículo 16 de la Constitución al objeto de reconocer de forma expresa y como derecho fundamental el derecho a la protección de datos), pese a que son todavía pocos los países que cuentan con una regulación específica (Ley 25.326 de protección de datos de Argentina, o Ley 18.331, de agosto de 2008, de protección de datos de Uruguay; en México, Colombia, Chile o Perú existen regulaciones sectoriales que afectan a diversos aspectos relacionados con la protección de datos). También van produciéndose avances enormemente significativos en otras zonas geopolíticas (China, Kenia o Burkina Faso) que permiten albergar esperanzas.

El artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea reconoce expresamente el derecho fundamental a la protección de datos de carácter personal del siguiente modo:

> "Artículo 8: Protección de datos de carácter personal.
>
> 1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernen.
>
> 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legíti-

mo previsto por la Ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación.

3. El respeto de estas normas quedará sujeto al control de una autoridad independiente".

Tal precepto representa, por un lado, el fin de una evolución que tiene su origen más inmediato en las leyes de protección de datos de los años setenta del siglo pasado y en diversos textos europeos de indudable trascendencia, como por ejemplo el Convenio núm. 108 del Consejo de Europa para la Protección de las Personas con respecto al tratamiento automatizado de los datos de carácter personal (1.981), o la Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que se refiere al tratamiento de datos personales y a su libre circulación.

Por otra parte, supone el punto de partida de una nueva etapa en la protección de datos de carácter personal, reconocida ya como derecho fundamental, autónomo e independiente del derecho a la intimidad. Punto de partida que arranca precisamente en el ámbito europeo, en el año 2000, con el ya citado artículo 8 de la Carta Europea de Derechos Fundamentales adoptada en Niza en mayo de ese año y, además, con diversas sentencias del Tribunal Europeo de Derechos Humanos, en particular las dictadas en los asuntos Amann contra Suiza, de 16 de febrero de 2000 y Rotaru contra Rumania, de 4 de mayo de 2000. En España la consideración de la protección de datos como un derecho autónomo e independiente ha sido consolidada por el Tribunal Constitucional en su ya conocida Sentencia 292/2000, de 30 de noviembre, de la que debemos recordar el fundamento jurídico séptimo:

"7... el contenido del Derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del Derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular.

Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos.

En fin, son elementos característicos de la definición constitucional del Derecho fundamental a la protección de datos personales, los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos.

> Y resultan indispensables para hacer efectivo ese contenido el reconocimiento del derecho a ser informado de quién posee sus datos personales y con qué fin, y el derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos. Es decir, exigiendo del titular del fichero que le informe de qué datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios; y, en su caso, requerirle para que los rectifique o los cancele".

La construcción del Tribunal Constitucional es, en mi opinión, impecable (ojalá resista el envite que se ha producido desde el propio Tribunal, en su más que discutible Sentencia 114/2006, de 5 de abril de 2006).

Ante todo, es capital la consideración del derecho a la protección de datos como autónomo, diferenciado de los de privacidad e intimidad. Un derecho que (y éste es el elemento estructural del mismo) atribuye a su titular un poder de disposición sobre sus propios datos personales, sean o no íntimos. Pasa así a un segundo plano la discusión acerca de qué se entiende por privacidad o intimidad, pues el núcleo protector del derecho, como acabo de resaltar, se extiende a todo tipo de datos, sin perjuicio, obviamente, de que unos, por su especial naturaleza, requieran de mayor protección que otros. Este sería el caso de los llamados datos sensibles o especialmente protegidos (a los que se refiere el artículo 7 de la LOPD).

Esa consideración del derecho fundamental a la protección de datos explica y justifica el contenido de los principios que configuran su núcleo esencial. Tales principios, cuya violación o desconocimiento implica la violación o desconocimiento del derecho, pueden reconducirse a los siguientes: consentimiento, información, finalidad, calidad de los datos (con especial referencia a la proporcionalidad), seguridad y control independiente. Principios a los que pueden añadirse los de utilización leal de los datos y minimización en el uso de los mismos (éste, por cierto, reconducible también, en mi opinión, al de proporcionalidad). Principios que para ser efectivos requieren el reconocimiento, garantía y tutela de los derechos de acceso, rectificación, cancelación y oposición[2].

Ante los avances tecnológicos, este derecho sigue evolucionando para hacer frente a nuevos y sofisticados ataques que pueden amenazar su contenido y razón de ser. Tal es el caso, por ejemplo, de la muy importante sentencia del Tribunal Constitucional alemán de 27 de febrero de 2008 (a la que también se ha referido Rodotá, 2008), fruto del recurso interpuesto contra la reforma de la Ley de los Servicios de Inteligencia del Estado de Renania del Norte Westfalia, en virtud de la cual se permitía expresamente que tales servicios pudiesen utilizar de forma secreta *spywares* troyanos para espiar los ordenadore de cualquier sospechoso: se introducen en los ordenadores sin que el interesado sea cons-

2 Sobre los principios de protección de datos, Piñar Mañas (2005:21 y ss. y bibliografía allí citada). Más recientemente, véase Castillo Vázquez (2007).

ciente de ello y captan todo tipo de información que luego puede ser analizada. El Tribunal declara inconstitucional la reforma y configura, por primera vez, lo que se ha considerado ya como un nuevo derecho fundamental a la protección de la confidencialidad e integridad de los sistemas tecnológicos de información. El Tribunal de Karlsruhe da así un paso más en el reconocimiento, primero, del derecho a la autodeterminación informativa (1983) y más tarde del derecho a la protección absoluta de la zona nuclear *(core area)* del comportamiento privado (*private conduct of lif*). El Tribunal llega al siguiente razonamiento:

> "De la relevancia del uso de los sistemas tecnológicos de información para expresar la personalidad y de los peligros que para la personalidad representa tal uso, deriva una necesidad de protección que es significativa para los derechos fundamentales. El individuo depende de que el Estado respete las expectativas justificables de confidencialidad e integridad de tales sistemas de cara a la irrestricta expresión de su personalidad" (epígrafe 181 de la sentencia).

Los sistemas de información protegidos por este nuevo derecho son todos aquellos (ordenadores personales, agendas electrónicas, teléfonos móviles…) que solos o interconectados con otros puedan contener datos personales del afectado de modo que el acceso al sistema permita hacerse una idea sobre partes relevantes del comportamiento vital de una persona o incluso obtener una imagen representativa de su personalidad (epígrafe 203). Este derecho a la integridad y confidencialidad de los sistemas tecnológicos de información, que tendría la consideración de verdadero derecho constitucional, sólo puede ser restringido en casos muy limitados.

Sólo en casos de evidencia de un peligro concreto para la vida, la integridad física o la libertad de las personas, así como para los fundamentos del Estado, los poderes públicos pueden hacer uso de técnicas de registro en línea. Técnicas que, en consecuencia, no pueden ser utilizadas en las investigaciones relacionadas con delitos "normales" ni en la actividad genérica de los servicios de inteligencia y que, en cualquier caso, requieren la adopción de medidas para proteger el núcleo esencial de la vida privada (el *core area of private conduct of life*) que incluye la información relativa a las relaciones y los sentimientos personales. Por ello, el Tribunal señala que, en caso de que de forma accidental se recabasen datos referidos a esa área vital, deben ser suprimidos de inmediato sin que puedan ser utilizados en ningún caso.

En España, el marco normativo del derecho a la protección de datos se fundamenta en el artículo 18.4 de la Constitución y tuvo su primer reflejo expreso en la Ley Orgánica 5/1992, de 29 de octubre, de Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD). Posteriormente fue derogada y sustituida por la vigente Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD). Junto con ésta deben tenerse en cuenta una gran cantidad de normas reguladoras de muy diversos sectores (telecomunicaciones, sanidad, seguridad, consumo, seguros,

entidades financieras, administración electrónica, sociedad de la información…[3]), que configuran un marco jurídico realmente complejo, y que por el momento se ha completado con el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica de Protección de Datos (BOE de 19 de enero de 2008).

Tal diversidad normativa pone además de manifiesto el hecho de que la protección de datos es una materia con presencia en la práctica totalidad de los sectores de actividad. El impacto de la protección de datos es hoy incuestionable.

1.2 Protección de datos y otros derechos

La protección de datos permite, además, hacer más efectivos (directa o indirectamente) otros derechos y libertades. En efecto, siendo como es un derecho fundamental, es asimismo requisito para que otras libertades sean respetadas. Impide (debería impedir) que la información disponible sobre las personas pueda ser utilizada en contra de sus derechos y libertades. El mal uso de los datos personales puede traer como consecuencia la restricción ilegítima de derechos tales como el de libertad de circulación, libertad religiosa, libertad de sindicación, acceso a funciones públicas, o el derecho al trabajo. Son muchos los supuestos reales que se han producido en este sentido, con el agravante, además, de que la violación del derecho a la protección de datos puede pasar inicialmente (o constantemente) desapercibida para su titular, de modo que no puede identificar el motivo por el que se producen consecuencias negativas en la esfera de sus derechos.

Por otra parte, las nuevas tecnologías hacen posible situaciones de invasión de los derechos de libertad difícilmente imaginables hasta la fecha. Cada vez es más frecuente la violación de la intimidad derivada del uso de cámaras de videovigilancia o de dispositivos de radiofrecuencia, así como de sistemas de identificación y/o localización, o de información genética. Por ello debe recalcarse la importancia que ha de otorgarse a la

3 Entre otras, ténganse en cuenta las siguiente leyes: Ley 19/1993, de 28 de diciembre, sobre determinadas medidas de prevención del blanqueo de capitales; Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las fuerzas y cuerpos de seguridad en lugares públicos; Ley 41/2002, de 14 de noviembre, reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica; Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos; Ley Orgánica 10/2007, de 8 de octubre, reguladora de bases de datos policiales sobre identificadores obtenidos a partir del ADN; Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones; Ley 30/2007, de 30 de octubre, de contratos del sector público, o Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.

protección de datos de carácter personal como derecho que favorece el ejercicio efectivo de la libertad.

Sin embargo, la protección de datos puede considerarse como un límite para el ejercicio de ciertos derechos. Así se ha señalado, por ejemplo, en relación con el derecho a la libertad de expresión o de información, o con el derecho a la transparencia. Se ha llegado a considerar que la protección de datos puede dificultar el ejercicio efectivo de estos derechos. Aunque, como ya apunté anteriormente, esto no es así en absoluto. El reto está en encontrar el justo equilibrio entre ambos derechos, tal como se desprende, por ejemplo, del artículo 9 de la Directiva 95/46/CE, según el cual en lo referente al tratamiento de datos personales con fines exclusivamente periodísticos o de expresión artística o literaria, los Estados miembros establecerán exenciones y excepciones sólo en la medida en que resulten necesarias para conciliar el derecho a la intimidad con las normas que rigen la libertad de expresión. Sobre este artículo acaba de pronunciarse el Tribunal de Justicia de la Comunidad Europea en su sentencia de 16 de diciembre de 2008, Asunto C-73/07, *Tietosuojavaltuutettu* (garante finlandés de la protección de datos). Sobre la relación entre libertad de expresión y protección de datos, téngase en cuenta también la conocida sentencia del TJCE de 6 de noviembre de 2003, *Linqvist*, Asunto C-101/01.

En cualquier caso, el derecho a la protección de datos puede considerarse un derecho jurídicamente consolidado. Sin embargo, su implantación efectiva ha de enfrentarse a no pocos retos. Como ya he señalado, el objetivo principal del presente documento es analizar las relaciones entre protección de datos, seguridad y transparencia, al objeto de intentar identificar los puntos de fricción y las posibles soluciones. Para ello, debemos dejar sentadas algunas consideraciones con carácter previo:

- Primera: la protección de datos es un derecho ya consolidado, al menos en Europa. Pese a ello, son muchos los pasos que han de darse todavía hasta conseguir un nivel de concienciación suficiente, aunque ya no es posible considerar que una sociedad es abierta y plenamente democrática si tal derecho no es reconocido y amparado (mejor si es a través de un marco jurídico específico, aunque en no pocos países es la jurisprudencia la que va configurando sus contornos). Tengamos en cuenta que la protección de datos limita, por ejemplo, el uso que llevan a cabo los poderes públicos de la información personal, lo que en consecuencia limita el control que pueden ejercer sobre los ciudadanos. Control omnipresente que no sólo es posible, sino en algún caso real, y que lleva a la eliminación de las libertades y de la democracia a partir de la eliminación de la privacidad.

- Segunda: dicho lo anterior, podría afirmarse que en las relaciones entre protección de datos, seguridad y transparencia se da una situación en cierto modo paradójica. En ambos casos, la protección de datos es considerada en no pocas ocasiones como un obstáculo para la garantía de la seguridad pública y el establecimiento de una socie-

dad transparente que asegure el derecho de acceso a la información. Pero a partir de aquí la percepción de la protección de datos y de las consecuencias de su reconocimiento varían:

- Por un lado, parece que en la tensión entre seguridad y protección de datos, la primera está ocupando un papel prevalente, de forma que podría decirse que está ganando la batalla a la segunda y que lo está haciendo a nivel global. Parecería que el derecho fundamental a la protección de datos debe ceder ante las exigencias de la seguridad pública que, con todos los instrumentos que tenga a su alcance, debe hacer frente a los constantes riesgos y amenazas a que está sometida. Las medidas que se han adoptado en relación con el control de los datos de pasajeros (no sólo en Estados Unidos, sino ahora también en la Unión Europea); con el control de las transacciones financieras llevadas a cabo a través de SWIFT; o con la retención de datos de tráfico por parte de los operadores de servicios de telecomunicaciones, son buena prueba de ello.

- Por otro lado, sin embargo, en la tensión o incluso conflicto que se da entre transparencia y protección de datos la situación es muy diferente. En este caso es preciso definir el marco de referencia, pues, a diferencia de lo que apuntaba al comentar la relación entre privacidad y seguridad (que permite afirmar la prevalencia de la segunda con carácter global, es decir, en la gran mayoría de los países, por no decir en todos), lo cierto es que el predominio de la transparencia o de la privacidad depende en gran medida del país en concreto y del marco normativo aplicable. De modo que, al no ser posible alcanzar una respuesta general de alcance global, tendremos que hacer un esfuerzo de sistematización, pudiendo distinguir claramente entre aquellos países que cuentan con una tradición de transparencia consolidada, los que se han incorporado recientemente al grupo de quienes cuentan con legislación sobre la materia, y aquéllos que carecen de ley de acceso a la información. España se encuentra entre estos últimos, y hemos de señalar que la batalla en este caso la está perdiendo, claramente, la transparencia. En otras palabras, la seguridad se impone sobre la privacidad de forma clara y global, mientras que, en España, la transparencia cede ante la protección de datos.

• Tercera: lo anterior debe llevarnos a otra reflexión de no menor alcance. Debido a la no existencia en España de una legislación adecuada sobre el derecho de acceso a la información, están produciéndose situaciones muy cercanas a lo que sin duda es una instrumentalización de la protección de datos (sobre lo que ha llamado la atención el Defensor del Pueblo Europeo, 2001). Esta situación no es admisible. No facilitar el acceso a documentos o a informaciones en poder de las Administraciones públicas so pretexto de ser contrario a la Ley de Protección de Datos, encierra simplemente, en muchas ocasiones, la intención nada confesable de ocultar dicha información por pura conveniencia de quien dispone de ella, sin que se pueda invocar la LOPD. Ahora bien, también es cierto que la falta de una ley reguladora del acceso a la información impide

en no pocas situaciones contar con la habilitación legal necesaria para ceder los datos que tal acceso pueda implicar. Habilitación que una ley facilitaría, en los términos regulados en ella.

Hechas las anteriores consideraciones, analizaré a continuación la relación existente entre protección de datos y seguridad pública, para después centrarme en la que se da entre protección de datos y transparencia.

2. Protección de datos y seguridad pública

2.1 La idea de seguridad en la sociedad actual y el desarrollo de nuevas tecnologías

Sin duda una de las tensiones que más se ha puesto de relieve al hablar de la protección de datos es la que deriva de su relación con la seguridad pública. Los terribles atentados del 11-S, así como los de Londres y Madrid (y tantos otros después), han modificado los estándares de seguridad y las exigencias que de ello derivan, que afectan mucas veces al ejercicio de otros derechos, como es, señaladamente, la protección de datos de carácter personal.

El derecho a la seguridad está expresamente reconocido en el artículo 17.1 de nuestra Constitución y ha sido reconocido por el Tribunal Europeo de Derechos Humanos, como recientemente ha recordado el Comisionado para los Derechos Humanos del Consejo de Europa (2008:12). Según el artículo 29 del Tratado de la Unión Europea: "el objetivo de la Unión será ofrecer a los ciudadanos un alto grado de seguridad dentro de un espacio de libertad, seguridad y justicia". El artículo 6 de la Carta de los Derechos Fundamentales de la Unión Europea afirma que "toda persona tiene derecho a la libertad y a la seguridad". Sin embargo, es incuestionable que la seguridad ciudadana está sometida a retos que nunca hasta ahora habían podido imaginarse, por lo que es necesario que se adopten medidas dirigidas a protegerla. Los Estados tienen la obligación de adoptar medidas dirigidas a proteger a los ciudadanos frente a la inseguridad. En no pocas ocasiones tales medidas inciden o pueden incidir en los derechos fundamentales, lo cual exige, ante todo, la identificación de los retos a los que está sometida la seguridad, para así poder reaccionar con eficacia frente a ellos (precisamente en defensa de los derechos fundamentales). Pero también requiere que la seguridad esté sometida a retos reales, no imaginarios, y que las medidas adoptadas sean necesarias y proporcionales al riesgo existente.

Y adelanto ya una reflexión conclusiva: las sociedades democráticas están legitimadas para (y obligadas a) adoptar, en el marco del Estado de derecho y el respeto a la legalidad, las medidas que sean necesarias para garantizar la seguridad de las personas y en particular para combatir el terrorismo y las formas graves de delincuencia organizada. En un reciente estudio llevado a cabo en el ámbito europeo, se ha puesto de manifiesto que la mayoría de los encuestados estaría de acuerdo con la adopción de medidas que limitasen su privacidad a cambio de mayor seguridad. Así, el 82% estaría a favor de permitir la

posibilidad de que los datos personales fuesen supervisados cuando tomaran un vuelo, y el 75% admitiría la supervisión de la utilización de Internet (Jonathan Faull, 2008).

Pero debe afirmarse con toda convicción que tales medidas han de ser respetuosas con los derechos fundamentales, pues de lo contrario se estaría sufriendo la primera y capital derrota de la democracia: restringir el marco de libertades y derechos que caracteriza a las sociedades occidentales. Y uno de esos derechos es el de la protección de datos de carácter personal: cualquier medida que se adopte para garantizar la seguridad ha de ser respetuosa con el contenido esencial del derecho a la protección de datos.

John Henry Clippinger, en su sugerente libro *A crowd of one. The future of individual identity* (2007) nos ofrece una serie de reflexiones sobre la seguridad y la inseguridad en la sociedad contemporánea y sobre los retos que para la seguridad pueden derivar de las nuevas tecnologías. Retos que provienen de "innovaciones tecnológicas sin precedentes que abarcan las tecnologías de la información, robótica, ciencias de la vida, energía, transportes, armas, comunicaciones y nanotecnologías. En su conjunto, los cambios tecnológicos redefinirán permanentemente el horizonte global" (2007:3), que se caracteriza por un escenario de seguridad extraordinariamente volátil que requiere que los gobiernos se anticipen a los acontecimientos: se trata de adaptarse o morir (2007:26).

En opinión de Clippinger existen tres circunstancias que sitúan a toda la comunidad en una situación de "hiper-inestabilidad" *(hyper-instability)*:

a) La aplicación de la "Ley de Moore"[4] a la relación coste-beneficio en el uso de las armas, de modo que hoy es posible causar víctimas y estragos a un bajísimo coste (Clippinger recuerda que los atentados del 11-S tuvieron un coste para Al Qaeda de unos 500.000 dólares, 2007:28), sobre todo utilizando nuevas tecnologías y recursos biogenéticos.

b) El efecto *small world,* derivado de los avances en el transporte y las comunicaciones. No sólo las personas pueden comunicarse con otros y gozar de una gran movilidad, sino que también las ideas, la información, circulan rápidamente a nivel global, y a un bajísimo coste.

c) El crecimiento de la población, que a su vez incrementa su densidad, lo que supone elevar "la presión económica, social y psicológica". En la medida en que aumente la

4 Gordon Moore (1965) expuso su visión del futuro de las tecnologías en un breve artículo, de apenas cuatro páginas, publicado en 1965, en términos que más adelante se conocerían (y así se conocen hoy) como la "Ley de Moore". Avanzó entonces que la relación entre coste y complejidad de los componentes tecnológicos varía a razón, aproximadamente, de la mitad por año. A corto plazo esta relación puede mantenerse o incluso incrementarse. A largo plazo la tendencia es algo más incierta, si bien puede creerse que puede permanecer casi constante durante unos diez años.

> población aumentará la lucha feroz por los escasos recursos existentes o por la búsqueda de otros nuevos, y es posible predecir que "tal competición producirá conflictos (financieros, políticos y militares) antes de que sea posible alcanzar soluciones para ello (energías renovables, reciclaje, tecnologías agrícolas más eficientes)" (2007:29-30).

De estas circunstancias la que más nos interesa ahora es la que hace referencia a las nuevas tecnologías. No se añade nada nuevo al afirmar que la revolución tecnológica es imparable. Pero las características de tal revolución carecen de cualquier precedente.

Retomando lo que ya he tenido ocasión de apuntar en otro lugar (2007:54 y ss.), y siguiendo a Manuel Castells (2005:61), puede afirmarse que la revolución de la tecnología de la información es "un acontecimiento histórico al menos tan importante como lo fue la revolución industrial del siglo XVIII".

La evolución está siendo, además, extraordinariamente rápida y profunda, lo que permite hablar de verdadera revolución. Tan rápida, que "cualquier relato de ese tipo (sobre la historia de la revolución de la tecnología de la información) quedaría obsoleto de inmediato" (Castells, 2005:70). Como ha señalado expresivamente Clippinger, "el cambio es tan rápido que ningún día guarda relación significativa con el anterior". En la actualidad, la referencia en cuanto a los cambios es la década. Y se pregunta: "si el ciclo vital de los productos se mide en semanas e incluso en días, ¿qué acontecerá con las instituciones sociales y culturales, tales como las relaciones, el trabajo, el matrimonio, la iglesia, el gobierno o la escuela?" (2007:24 y 25)

Castells habla de "la microingeniería de los macrocambios: electrónica e información", para expresar cómo se ha desarrollado la revolución tecnológica en los últimos años. Y los datos son sencillamente espectaculares (2005:71 y ss.). Evolución que tiene muy directas y graves repercusiones sobre la privacidad de las personas: sistemas RFID, videovigilancia, sistemas de reconocimiento facial (*face recognition technologies)* (véase por ejemplo, K.W. Bowyer, 2004: 9 y ss.; Jay Stanley y Barry Steinhardt, 2004), *ubiquitous computing* (término utilizado por primera vez en torno a 1988 por Mark Weiser, 1988), La nanotecnología permite ya contar con dispositivos capaces de captar y elaborar información hasta extremos insospechados y de un modo totalmente indetectable; tal es el caso de los llamados *roboflies*, o de los *nanobots* (Clippinger, 2007:28 y 32). Por otro lado, el coste económico de los avances tecnológicos y de los nuevos dispositivos es cada vez menor, lo que facilita aún más su uso e implantación. Los ejemplos pueden multiplicarse (Piñar Mañas, 2008 b:13 y ss.), sin olvidar que el uso indiscriminado de nuevas tecnologías puede implicar graves discriminaciones entre la ciudadanía. El Congreso de Estados Unidos, tras más de diez años de debate en la opinión pública y entre las fuerzas políticas, acaba de aprobar una Ley que prohíbe la discriminación por motivos genéticos, tras haber sido ya aprobada por el Senado, basada en una lógica aplastante: nadie puede sufrir consecuencias negativas por algo que, como la herencia genética, está total-

mente fuera de su control (Michael Kinsley, 2008:60). En fin, incluso se ha demostrado que ya no es ciencia ficción la posibilidad de leer el pensamiento a partir del desarrollo de técnicas basadas en la resonancia magnética funcional.

Tan espectacular (r)evolución tecnológica tiene sin duda un efecto directo y positivo sobre la calidad de vida, efecto indiscutible e irreversible. Pero al mismo tiempo representa, como ya he subrayado, un potencial peligro para la seguridad, así como un riesgo para los derechos fundamentales y en particular para el derecho a la protección de datos. Las nuevas tecnologías van a configurar, están configurando, el futuro del escenario global de la seguridad (Clippinger, 2007:31), pero para comprender el alcance de tal consideración es imprescindible ser consciente de la naturaleza y el poder de esas nuevas tecnologías, así como de su capacidad de influencia sobre la propia sociedad. En este sentido, Clippinger ha señalado, con razón, que "nos movemos desde modelos mecánicos basados en la masa, la fuerza y el volumen, a otros en que se refuerza la importancia de las reglas, el lenguaje, los protocolos, que permiten complejas fórmulas de control, replicación y comunicación" (2007:33). Las nuevas tecnologías hacen además que la naturaleza del adversario sea diferente: los enemigos no son otras naciones-estado, sino un nuevo tipo de adversario: el "adversario asimétrico", que representa a su vez "retos asimétricos" (2007:5, 37 y 40) para la seguridad, que han de ser considerados desde planteamientos distintos a los tradicionales.

En conclusión, la irrupción y aplicación de nuevas tecnologías exigen reorientar las reflexiones que sobre la seguridad y sus retos han venido planteándose hasta este momento.

Ahora bien, a pesar de ser cierto el enfoque que acabo de exponer, también es verdad que, en no pocas ocasiones, se intenta ofrecer un panorama de inseguridad que no siempre coincide con la realidad y que se utiliza como coartada para justificar la adopción de medidas restrictivas de derechos, que buscarían, por el bien de todos, garantizar y fortalecer la seguridad hipotéticamente amenazada.

Charles Krauthammer (2004), uno de los ideólogos de los neoconservadores en Estados Unidos, ha llamado insistentemente la atención acerca de la misión que corresponde a ese país de proteger a la humanidad de los peligros que nos acechan. "América –afirma– es el campo de minas entre la barbarie y la civilización" (*"is the land mine between barbarism and civilization"*). Y ello implica ser intransigentes frente a la inseguridad, lo que lleva a adoptar medidas que se inscriben en lo que él llama "realismo democrático", cuyo axioma es el siguiente: *"We will support democracy everywhere, but we will commit blood and treasure only in places where there is a strategic necessity-meaning, places central to the larger war against the existential enemy, the enemy that poses a global mortal threat to freedom"* (2004). Como señala Clippinger, se trata de una nueva interpretación y aplicación del Leviatán de Hobbes; Estados Unidos interpreta qué debe entenderse por seguridad y lo aplica tajantemente: "estás con nosotros o contra nosotros. Una parte gana, otra parte pierde. Es un juego de suma cero en términos de la teoría de los juegos". Por ello no debe causar sor-

presa que los "hobbesianos contemporáneos" tiendan a ser "patriarcales, autoritarios y conservadores en sus políticas sociales y culturales" (2007:12 y 13). Paul Krugman (2008) ha llamado la atención acerca de la "vasta conspiración" que los *think tanks* neoconservadores y vinculados al Partido Republicano están llevando a cabo en Estados Unidos. Una situación que debería cambiar radicalmente tras la victoria de Obama, que ya en su discurso inaugural, pronunciado el 20 de enero de 2009, resaltó con énfasis que "en cuanto a nuestra defensa común, rechazamos como falso que haya que elegir entre nuestra seguridad y nuestros ideales". Y añadió: "Nuestros Padres Fundadores, enfrentados a peligros que apenas podemos imaginar, elaboraron una carta que garantizase el imperio de la ley y los derechos humanos, una carta que se ha perfeccionado con la sangre de generaciones".

Con estas consideraciones quiero llamar la atención acerca de la necesidad de ser muy conscientes de algunos aspectos:

- Primero, de los riesgos a los que está sometida nuestra seguridad, individual y colectiva; riesgos que ni pueden ni deben ser minusvalorados, que provienen, en una medida nada desdeñable, de la aplicación de nuevas tecnologías del conocimiento, y que exigen adoptar medidas eficaces para eliminarlos o, cuando menos, minimizarlos.

- Segundo, que tales medidas pueden inevitablemente afectar a ciertos derechos fundamentales, y en particular a la protección de datos.

- Tercero, que es imprescindible llevar a cabo un análisis objetivo y desapasionado de la situación real de seguridad o inseguridad, para de este modo poder valorar y evaluar qué medidas son realmente necesarias y con qué alcance y límites. En particular, y en lo que ahora nos afecta, qué medidas limitativas del derecho a la protección de datos son necesarias, eficaces y proporcionales, y cuáles son, por el contrario, una vía para ejercer un control innecesario e injustificado sobre los ciudadanos que nos convierte a todos, no ya en meros sospechosos, sino en sujetos-objetos expuestos a una vigilancia y control tan omnipresentes como constantes.

Hemos de intentar tomar en consideración las situaciones de inseguridad real, no la que me atrevería a llamar "inseguridad inducida": sensación de inseguridad que no se corresponde con la realidad, pero que podría ser fundamento e incluso pretendida justificación de la adopción de medidas restrictivas de derechos no siempre necesarias o justificadas, como tampoco proporcionadas a la situación real.

2.2 Reacciones para proteger la seguridad frente a los riesgos actuales

La aprobación en Estados Unidos tras el 11-S de la *Patriot Act ("Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism*

[USA PATRIOT ACT] Act of 2001") ha venido seguida de la adopción de medidas restrictivas que inciden considerablemente en la protección de datos (Amitai Etzioni (2004). Los llamados casos PNR (cesión de datos de pasajeros a las autoridades aduaneras de Estados Unidos) o SWIFT (posibilidad que tiene el Departamento del Tesoro de Estados Unidos de acceder a datos relativos a transferencias financieras que se operen a través del sistema Swift), a los que ya me he referido, son expresión de ello. La tensión que se ha producido entre Europa y Estados Unidos (con dos perspectivas diferentes en cuanto a la virtualidad de los derechos y la aplicación extraterritorial de las normas) es, en definitiva, expresión de la que existe entre seguridad y libertad. Pero esa tensión también se ha producido en el seno de Europa. La Directiva sobre retención de datos de telecomunicaciones (Directiva 2006/24/CE, del Parlamento Europeo y del Consejo de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE) es prueba de ello. Por otra parte, cada vez se generaliza más la instalación de cámaras y videocámaras, de modo que puede afirmarse que corremos el riesgo de estar sometidos, como ya he señalado anteriormente, a una vigilancia omnipresente.

En algunas ocasiones parecería que las iniciativas de control son propias de la ciencia ficción. Tal es el caso del proyecto llamado *Total Information Awareness*, más tarde *Terrorism Information Awareness* (Solove, 2004:168 y ss). En otras se actúa al borde de la legalidad. Tras los atentados del 11-S, la Administración de Bush puso en marcha a través de simples decretos un programa de escuchas ilegales y espionaje electrónico que recientemente obtuvo el apoyo del Congreso y del Senado. Mediante dicho programa, el Gobierno puede espiar, sin necesidad de autorización judicial, las comunicaciones de ciudadanos estadounidenses y de los extranjeros considerados sospechosos de actividades terroristas. En base a la *Patriot Act*, es posible que en los controles de aduanas de los aeropuertos de Estados Unidos se registre el contenido de los ordenadores por las autoridades, lo cual supone una clara violación del derecho a la privacidad. Gran parte de esas medidas están siendo afortunada y profundamente revisadas por el Gobierno de Obama, pero no olvidemos que en Suecia se ha aprobado una ley por la que, sin necesidad de orden judicial, se permite que los servicios secretos rastreen los correos electrónicos, llamadas telefónicas y faxes enviados al extranjero (en principio las comunicaciones nacionales no serían vigiladas). En Italia se ha planteado un gran debate acerca de la posibilidad o no de interceptar conversaciones privadas por razones de seguridad y se pretende poner en marcha un gran proyecto de recolección de datos, incluidos datos biométricos, de la población romaní (lo que ha merecido la crítica del Parlamento Europeo). En Alemania, en diciembre de 2008, se ha aprobado una Ley que permite a la policía llevar a cabo un seguimiento y vigilancia de enorme alcance de los ciudadanos, pudiendo incluso espiar en línea los ordenadores, sin autorización judicial en "casos de urgencia" (como ya sabemos, el Tribunal Constitucional alemán ya se ha pronunciado, en su Sentencia de 27 de febrero de 2008, en relación con una ley semejante del Estado de Renania del Norte Westfalia).

Mientras tanto, en la Unión Europea, tras una primera posición en contra de las iniciativas que venían de Estados Unidos, se va aceptando poco a poco la adopción de medidas que pueden suponer importantes limitaciones para la libertad, los derechos fundamentales y, en particular, para la privacidad. Así, pese a la férrea oposición inicial contra los planes estadounidenses de recabar los datos de todos los pasajeros que volasen con destino o escala a/en Estados Unidos, ahora desde Bruselas se considera que tal medida es imprescindible en la lucha por la seguridad y se ha presentado una Propuesta de Decisión Marco del Consejo sobre utilización del registro de nombres de los pasajeros (*Passenger Name Record* – PNR) con fines represivos, que ha merecido una muy dura contestación por parte del Parlamento Europeo, de las Autoridades de Protección de Datos de los Estados miembros, y del Supervisor Europeo de Protección de Datos. Asimismo, se estudia la posibilidad de instalar en el interior de los aviones videocámaras y micrófonos que permitan un control constante de la actividad en cabina (*La Repubblica*, 9 de junio de 2008:15).

2.3 El necesario equilibrio entre seguridad y protección de datos de carácter personal

En este escenario se plantea con especial intensidad la tensión entre protección de datos y seguridad. Tensión que, una vez más, debe buscar el justo equilibrio valorando en todo caso el estricto respeto a los derechos fundamentales. Es el viejo y muchas veces falseado dilema del conflicto entre libertad y seguridad. Por ello, resulta imprescindible llevar a cabo una reflexión acerca de la necesidad de buscar el recto equilibrio entre el respeto a la privacidad y la adopción de medidas que garanticen la seguridad ciudadana. Ambos son bienes/derechos a los que no cabe renunciar en una sociedad democrática, lo que exige analizar con objetividad la situación. El Parlamento Europeo, en numerosas ocasiones, ha llamado la atención sobre ello.

Nuestro Tribunal Constitucional, en la ya citada STC 292/2000, se ha referido a la relación entre protección de datos y seguridad en los siguientes términos:

> "9. En cuanto a los límites de este derecho fundamental no estará de más recordar que la Constitución menciona en el art. 105.b) que la ley regulará el acceso a los archivos y registros administrativos 'salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas' (en relación con el art. 8.1 y 18.1 y 4 CE), y en numerosas ocasiones este Tribunal ha dicho que la persecución y castigo del delito constituye, asimismo, un bien digno de protección constitucional, a través del cual se defienden otros como la paz social y la seguridad ciudadana. Bienes igualmente reconocidos en los arts. 10.1 y 104.1 CE (por citar las más recientes, SSTC 166/1999, de 27 de septiembre, FJ 2, y 127/2000, de 16 de mayo, FJ 3.a; ATC 155/1999, de 14 de junio). Y las SSTC 110/1984 y 143/1994 consideraron que la distribución equi-

> tativa 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.
>
> El Convenio Europeo de 1981 también ha tenido en cuenta estas exigencias en su art. 9. Al igual que el Tribunal Europeo de Derechos Humanos, quien refiriéndose a la garantía de la intimidad individual y familiar del art. 8 CEDH, aplicable también al tráfico de datos de carácter personal, reconociendo que pudiera tener límites como la seguridad del Estado (STEDH caso Leander, de 26 de marzo de 1987, §§ 47 y ss.), o la persecución de infracciones penales (*mutatis mutandis,* SSTEDH, casos Z, de 25 de febrero de 1997, y Funke, de 25 de febrero de 1993), ha exigido que tales limitaciones estén previstas legalmente y sean las indispensables en una sociedad democrática, lo que implica que la ley que establezca esos límites sea accesible al individuo concernido por ella, que resulten previsibles las consecuencias que para él pueda tener su aplicación, y que los límites respondan a una necesidad social imperiosa y sean adecuados y proporcionados para el logro de su propósito (Sentencias del Tribunal Europeo de Derechos Humanos, caso X e Y, de 26 de marzo de 1985; caso/Iander, de 26 de marzo de 1987; caso/Iskin, de 7 de julio de 1989; /Iatis mutandis, caso/Inke, de 25 de febrero de 1993; caso, de 25 de febrero de 1997)".

Las consideraciones del Tribunal Constitucional son, en mi opinión, perfectamente asumibles y aciertan a plantear el debate sobre el equilibrio entre seguridad y protección de datos en términos sumamente acertados. En efecto, tenemos que partir una vez más de la base de que la adopción de medidas tendentes a proteger la seguridad ciudadana es imprescindible y puede ser exigida a los poderes públicos. Tales medidas pueden incidir en los derechos fundamentales que –con excepción del derecho a la vida y el derecho a la dignidad humana (que no deben admitir restricción alguna)–, ciertamente están sometidos a límites. En consecuencia, el hecho de que ciertas medidas dirigidas a garantizar la seguridad puedan afectar al derecho a la protección de datos resulta en principio admisible.

A) Los límites admisibles de la protección de datos en su relación con la seguridad pública

Que la protección de datos es un derecho que admite límites es algo fuera de duda. Que tales límites pueden ser verdaderas restricciones derivadas de la necesidad de tomar en consideración otros derechos o intereses, también. Es lo que ocurre con la seguridad pública.

La propia LOPD establece en su artículo 2.2.c) que la misma no se aplica "a los ficheros establecidos para la investigación del terrorismo y formas graves de delincuencia organizada" [en el mismo sentido, art. 4.c) del Reglamento de desarrollo de la LOPD]. Por su parte, la Directiva 95/46/CE establece en su artículo 3.2 que la misma no se aplica al tratamiento de datos "efectuado en el ejercicio de actividades no comprendidas en

el ámbito de aplicación del Derecho comunitario, como las previstas por las disposiciones de los títulos V y VI del Tratado de la Unión Europea y, en cualquier caso, al tratamiento de datos que tenga por objeto la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando dicho tratamiento esté relacionado con su seguridad) y las actividades del Estado en materia penal". La Directiva, pues, no se aplica ni en el ámbito del Segundo Pilar (Política Exterior y de Seguridad Común), ni en el del Tercero (Cooperación policial y judicial en materia penal).

En lo que a la seguridad pública se refiere, el hecho de que la Directiva no se aplique en el ámbito del Tercer Pilar tiene especial relevancia. De hecho, gran parte de los debates acerca de la aplicación de las disposiciones sobre protección de datos en la Unión Europea giran en torno a la necesidad o no de respetar los principios de tal derecho en la adopción de medidas dirigidas a garantizar la seguridad y combatir el terrorismo y la delincuencia organizada. La Sentencia del Tribunal de Justicia de las Comunidades Europeas de 30 de mayo de 2006, Parlamento Europeo contra Consejo, asuntos acumulados C-317/04 y C-318/04, deja claro que la Directiva 95/46/CE no es norma jurídica que pueda servir de parámetro para enjuiciar la validez de diversos actos relacionados con el envío de datos de pasajeros a Estados Unidos, pues, por tratarse de iniciativas que se enmarcan en la lucha contra el terrorismo, quedan fuera de su ámbito de aplicación.

Precisamente por ello ha sido necesario aprobar la Decisión Marco 2008/977/JAI, del Consejo, de 27 de noviembre de 2008, relativa a la protección de datos personales en el marco de la cooperación policial y judicial en materia penal[5], por la que se pretende "garantizar un alto nivel de protección de los derechos y libertades fundamentales de las personas físicas y en particular de su derecho a la intimidad en lo que respecta al tratamiento de datos personales en el marco de la cooperación policial y judicial" (art. 1º). Ahora bien, dado que el ámbito de la Decisión es la cooperación policial y judicial, sólo se aplica al intercambio de datos entre los Estados miembros, no al tratamiento exclusivamente nacional.

La Decisión trae causa, sobre todo, del Programa de La Haya sobre la consolidación de la libertad, la seguridad y la justicia en la Unión Europea, adoptado por el Consejo Europeo el 4 de noviembre de 2004[6], y ha de entenderse también en relación con el Tratado de Prüm, de 27 de mayo de 2005, relativo a la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo, la delincuencia transfronteriza y la migración ilegal[7]. En todos los casos se pone de relieve la importancia que tiene el principio de disponibilidad establecido en el Programa de La Haya, en el

5 DOUE L. 350/60, de 30 de diciembre de 2008. Su entrada en vigor se prevé a los 20 días de su publicación (art. 30), mientras que los Estados miembros deben adoptar las medidas necesarias para dar cumplimiento a lo dispuesto en la Directiva antes del 27 de noviembre de 2010 (art. 29).

6 DOUE C-53, de 3 de marzo de 2005.

7 Instrumento de ratificación publicado en el BOE de 25 de diciembre de 2006. Entró en vigor en España el 1 de noviembre de 2006.

intercambio de datos, según el cual, estos no sólo podrán ser transmitidos entre los Estados miembros, sino que deben estar disponibles, sin obstáculos, para las autoridades competentes de los distintos Estados.

B) La frontera infranqueable

Ahora bien, admitido lo anterior, es necesario hacer algunas consideraciones. Tanto en Europa como en España la protección de datos es un derecho fundamental. No hace falta recordar lo que ya he señalado al respecto. El artículo 8 de la Carta Europea de Derechos Humanos y el artículo 18.4 de nuestra Constitución consagran un derecho autónomo que atribuye a las personas un verdadero poder de disposición sobre sus propios datos personales, sean o no íntimos. En consecuencia, como tal derecho fundamental, su contenido esencial ha de ser en todo caso respetado. Incluso a la hora de adoptar medidas para garantizar la seguridad pública y para hacer frente al terrorismo y la delincuencia organizada. Estaríamos ante lo que sería una frontera infranqueable para el legislador y, en general, para los poderes públicos.

En esta línea se mueve la Declaración adoptada por las Autoridades de Protección de Datos en la Conferencia de Primavera celebrada en Chipre los días 10 y 11 de mayo de 2007, que incluye una *Common position of the European Data Protection Authorities on the use of the concept of availability in law enforcement*, en la que se fijan las condiciones que deben ser respetadas en todo caso a la hora de intercambiar información basándose en el principio de disponibilidad. Tales condiciones son:

- Cualquier medida que afecte al tratamiento de datos en el ámbito de la cooperación policial y judicial deberá adoptarse por ley.

- Todas las medidas han de ser necesarias y proporcionadas.

- Deben adoptarse medidas concretas en función del tipo de dato que vaya a ser sometido a tratamiento, en particular, adecuadas medidas de seguridad.

- El acceso por los poderes públicos a datos personales debe estar limitado a casos concretos y sometidos a estrictas medidas de seguridad. Las autoridades destinatarias de los datos deben estar perfectamente delimitadas.

- Deben establecerse mecanismos que garanticen el control y supervisión del tratamiento de los datos. Los jueces y las Autoridades de Control de Protección de Datos deben poder actuar de modo efectivo.

También a nivel nacional es imprescindible respetar en todo caso los límites constitucionales del derecho: por un lado, los requisitos formales que la Constitución establece en orden a la regulación de los derechos y, por otro, el contenido esencial del derecho a la protección de datos.

En relación con el primer punto, la regulación del derecho a la protección de datos, en cuanto derivado del artículo 18.4 de la Constitución, requiere ley orgánica y, en consecuencia, su desarrollo, entendiendo por tal el desarrollo directo del mismo –como ya dejó sentado con carácter general y en época temprana el Tribunal Constitucional en su sentencia de 22 de febrero de 1982–, deberá hacerse por ley orgánica (artículo 81.1 de la Constitución). Por tanto, las limitaciones que afecten a la propia naturaleza del derecho (que entren dentro de lo que haya de entenderse por "desarrollo directo") deberán establecerse en ley orgánica, lo cual no significa que la ley ordinaria no tenga cabida en la delimitación del derecho. Precisamente esto es posible porque, por ejemplo, los artículos 6 y 11 de la LOPD permiten que una ley ordinaria habilite tratamientos sin consentimiento de los afectados.

Por otra parte, y sin olvidar que hablamos ahora de las relaciones entre derecho a la protección de datos y seguridad pública, debe tenerse en cuenta que el primero no es uno de los derechos que puedan ser suspendidos en los supuestos previstos en el artículo 55 de la Constitución.

Asimismo, y tal como señala el Tribunal Constitucional en la citada Sentencia 292/2000, es necesario que las limitaciones del derecho "estén previstas legalmente y sean las indispensables en una sociedad democrática, lo que implica que la ley que establezca esos límites sea accesible al individuo concernido por ella, que resulten previsibles las consecuencias que para él pueda tener su aplicación, y que los límites respondan a una necesidad social imperiosa y sean adecuados y proporcionados para el logro de su propósito".

Más adelante volveré sobre ello, pero merece la pena hacer una breve referencia a la exigencia constitucional de que la ley que establezca los límites al derecho sea accesible al individuo. Principio que tenía muy claro la abogada general Eleanor Sharpston en las Conclusiones presentadas el 10 de abril de 2008, en el Asunto C 345/06, *Gottfried Heinrich*, resuelto por Sentencia del Tribunal de Justicia de las Comunidades Europeas de 10 de marzo de 2009. El asunto se refiere al Reglamento (CE) nº 2320/2002, cuyo objeto es "establecer y aplicar las medidas comunitarias adecuadas para prevenir actos de interferencia ilícita contra la aviación civil". Medidas que se concretan en un Anexo del Reglamento nº 622/2003. Pues bien, para prevenir actos ilegales, las medidas fijadas en dicho Anexo se consideran secretas y no han sido publicadas.

Dicho Anexo contiene, entre otros elementos, normas básicas comunes de control de pasajeros (punto 4.1) y de control del equipaje de mano (punto 4.3). Todos los pasajeros en espera de embarcar serán controlados para evitar que se introduzcan artículos prohibidos en las zonas restringidas de seguridad y a bordo de una aeronave. El equipaje de mano de dichos pasajeros será controlado antes de poder acceder a las zonas restringidas de seguridad o a bordo de una aeronave, y se les retirará todo artículo prohibido o se les denegará el acceso a la zona de seguridad o a la aeronave, según corresponda. Pero

la relación de artículos prohibidos no ha sido objeto de publicación. Ante tal situación, el Tribunal concluye que la completa omisión de publicación del Anexo hace que el mismo carezca de fuerza vinculante en la medida en que pretenda imponer obligaciones a los particulares, por infringir el artículo 254 TCE.

Es decir, no es posible, en aras de la seguridad ciudadana, infringir un principio esencial del Estado de derecho, cual es el de la publicación de las normas, esencial para la efectividad de otro tipo de seguridad, la seguridad jurídica.

Nuestro Tribunal Supremo, sin embargo, parece tener otra opinión. La STS de 29 de enero de 2008, que tiene relación con el Acuerdo del Pleno del CGPJ de 7 de julio de 2004 sobre normas de seguridad, declara que tal acuerdo no tiene por qué ser publicado. Y para ello argumenta que las medidas de seguridad por las que se rige el acceso a los edificios judiciales no son disposiciones generales regidas por el principio de publicidad, sino normas de funcionamiento interno de un servicio del Estado dictadas en el ejercicio de la potestad de auto-organización que le corresponde. De modo que el interés de cualquier persona que no forme parte de los Cuerpos de la Administración de Justicia, únicamente está constituido por la concreta restricción individual que le haya sido impuesta como consecuencia de la aplicación de esas normas de seguridad interna, pero no requiere el conocimiento de la totalidad de su contenido.

No es ahora momento de analizar con más detalles esta sentencia, pero desde luego choca abiertamente con la exigencia de que la norma que establezca límites a un derecho sea conocida por los destinatarios, sin poder oponer argumentos formales (distinción entre acto y norma) o materiales (garantía de la seguridad ciudadana) para admitirlo.

Por otro lado, es necesario que las medidas que se adopten respeten en todo caso los principios que configuran el contenido esencial del derecho a la protección de datos. De entre tales principios algunos alcanzan un especial significado: los de información, finalidad y calidad del dato, especialmente en lo que se refiere a la proporcionalidad.

En efecto, en ningún caso debe ponerse en cuestión el contenido mismo del derecho, es decir, el poder de disposición sobre los propios datos personales. Lo que exige que cualquier medida que se adopte para salvaguardar la seguridad y que implique el tratamiento de datos personales (videovigilancia, recogida de datos de pasajeros…) ha de ir acompañada del deber de información sobre dicho tratamiento (sin perjuicio de las posibles excepciones que tal deber pueda tener). Pero, sobre todo, es esencial que la finalidad para la que esté previsto el tratamiento de datos sea precisa y legítima, y que los datos recabados sean utilizados exclusivamente para ella y no para otra diferente; así como que los datos obtenidos sean sólo los adecuados, pertinentes y no excesivos para dicha finalidad.

Las anteriores cautelas son, por ejemplo, las que tuvo especialmente en cuenta el llamado Grupo Europeo de Autoridades de Protección de Datos (o Grupo del Artículo 29 –WP

29–[8]) al analizar las iniciativas estadounidenses referentes a la recopilación de datos de pasajeros, conocida como PNR[9]. Iniciativas que ahora se pretenden aplicar en el seno de los países de la Unión Europea y que también han merecido la crítica del Grupo de Trabajo. En el "Dictamen conjunto sobre la propuesta de Decisión marco del Consejo relativa al uso del registro de nombres de los pasajeros (*Passenger Name Record* - PNR) a efectos de la aplicación de la ley, presentado por la Comisión el 6 de noviembre de 2007", adoptado por el WP 29 y el Grupo de Trabajo sobre Policía y Justicia en diciembre de 2007 (Ref. WP-145) se afirma expresamente que "Las autoridades comunitarias responsables de la protección de datos consideran que la forma en que la propuesta está actualmente redactada no sólo es desproporcionada, sino que también puede violar principios fundamentales de normas reconocidas en materia de protección de datos recogidas en el artículo 8 del Convenio Europeo sobre Derechos Humanos y del Convenio 108 del Consejo de Europa". Y señala de forma tan clara como rotunda:

> "Las cuestiones relacionadas con la protección de datos de la presente propuesta tienen las siguientes características:
>
> 1. La propuesta no justifica una necesidad apremiante de recogida de datos, con excepción de los datos API de información previa sobre pasajeros (*Advanced Passenger Information*, API).
>
> 2. Es excesiva la cantidad de datos personales que deben transferir las compañías aéreas.
>
> 3. La filtración de datos sensibles debería ser hecha por la persona responsable del tratamiento de los datos.
>
> 4. El método de *push*, debe aplicarse a todas las compañías aéreas.
>
> 5. El período de conservación de los datos es desproporcionado.
>
> 6. El régimen de protección de los datos es totalmente insatisfactorio: en ninguna parte se especifican los derechos de los interesados ni las obligaciones de los responsables del tratamiento de los datos.

8 *Article 29 Working Party*, como usualmente se conoce en el ámbito de las instituciones europeas y en general en el escenario internacional de la protección de datos. Denominación que tiene su origen en el hecho de que dicho Grupo ha sido instituido por el artículo 29 de la Directiva 95/46/CE.

9 Véanse los Documentos 4-03 (WP 78), 2-04 (WP 87), 8-04 (WP 97), 7-06 (WP 124), 2-07 (WP 132 y 151) y 5-07 (WP 138). Todos los Documentos del WP29 pueden consultarse en http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/. El Tribunal de Justicia de la Unión Europea ha tenido ocasión de referirse al tema en su Sentencia de 30 de mayo de 2006, Asuntos C-317/04 y C-318/04, pero no ha entrado en el fondo del asunto, pues sólo se ha centrado en cuestiones formales.

7. El gran margen de discreción concedido a los Estados miembros podría dar lugar a interpretaciones diversas de la Decisión marco.

8. El régimen de protección de datos de las transferencias que se realizarán a terceros países es poco claro.

Las autoridades responsables de la protección de datos de la UE invitan al Consejo a tener en cuenta las conclusiones y recomendaciones del presente dictamen al debatir la actual propuesta antes de su adopción. Si se quiere enfocar la cuestión de manera equilibrada, es imprescindible emprender un debate abierto y franco con todas las partes interesadas, es decir, las compañías aéreas, los sistemas de reserva, el sector de la protección de datos, el Parlamento Europeo y los parlamentos nacionales.

La adopción de un régimen de PNR por parte de la UE no tiene por qué dar lugar al control general de todos los viajeros".

2.4 Conclusión

De acuerdo con todo lo anterior, podemos concluir:

- Es deber de los Estados adoptar medidas que tengan como objetivo garantizar la seguridad pública con todos los instrumentos que ponga en sus manos el Estado de derecho y el principio de legalidad. Ello exige un marco legal claro que permita la actuación de las Fuerzas de Seguridad y de los jueces y tribunales, pero que respete los derechos y libertades constitucionales de las personas.

- El equilibrio entre protección de datos y seguridad ha de partir del reconocimiento del derecho de las sociedades democráticas a adoptar medidas que garanticen la seguridad pública, pero con pleno respeto a los derechos fundamentales, y en particular a los principios que configuran el contenido esencial del derecho a la protección de datos.

- En particular, cuando tales medidas requieran el tratamiento de datos personales (datos que, como sabemos, no es necesario que se refieran a la intimidad de las personas, pues el derecho a la protección de datos alcanza a cualquier dato personal, afecte o no a la esfera íntima), debe tenerse en cuenta:

    - Que resulta imprescindible contar con habilitación suficiente para adoptar la medida de que se trate, lo que se traduce en la necesidad de que, a falta de consentimiento, sea una norma con rango de ley la que legitime el tratamiento de los datos. Norma que, en mi opinión, no podría ser un Real Decreto-ley, dados los

términos de los artículos 6 y 11 de la Ley Orgánica de Protección de Datos y el propio artículo 86.1 de la Constitución.

- En todo caso, debe respetarse el deber previo de información a los interesados. En consecuencia, aquéllos a los que se soliciten datos deberán ser previamente informados de modo expreso, preciso e inequívoco, de al menos la existencia de un fichero, la finalidad de la recogida de los datos y la identidad del responsable del fichero (art. 5º de la LOPD y art. 10 de la Directiva 95/46/CE).

- Los datos sólo podrán ser tratados para finalidades determinadas, explícitas y legítimas [art. 4.1 de la LOPD y art. 6.1.b) de la Directiva]. En este sentido, no debería ser posible el tratamiento de datos basándose en la finalidad genérica y abstracta de garantizar la seguridad pública, sin más. Debe existir un peligro real y cierto. En este sentido, el artículo 22.2 de la LOPD establece que la recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales.

- Los datos que vayan a ser sometidos a tratamiento han de responder al principio de calidad del dato, es decir, deben ser adecuados, pertinentes y no excesivos en relación con la finalidad para la que se recaben [art. 4.1 de la LOPD y 6.1.c) de la Directiva]. En ningún caso deben obtenerse y tratarse datos no necesarios para la finalidad de que se trate. Seguramente el juego de los principios de finalidad y calidad es el más importante a la hora de definir la legalidad (constitucionalidad, incluso) de las medidas que se adopten para garantizar la seguridad pública y que afecten a la protección de datos.

- Deben adoptarse las medidas de seguridad que sean necesarias para garantizar en todo caso un tratamiento legítimo de los datos (art. 9 de la LOPD y art. 17 de la Directiva).

- Debe garantizarse que una autoridad absolutamente independiente controle y supervise la legalidad del tratamiento de los datos que sean necesarios para preservar la seguridad pública.

3. Protección de datos y transparencia

Las exigencias de la seguridad pública (la obligación de ofrecer a los ciudadanos un alto grado de seguridad, como afirma el artículo 29 del Tratado de la Unión Europea) junto con la protección de datos personales, en los términos de equilibrio que acabamos de ver, pueden llevarnos a una sociedad enormemente opaca. En efecto, la información puede considerarse de acceso restringido cuando no imposible, bien por hipotéticos motivos de seguridad, bien en aras de un pretendido respeto a la privacidad. Cuando la recopilación y posterior uso de datos se ampara en el uso de nuevas tecnologías, la situación puede ser aun más delicada y desembocar en la ausencia real de transparencia, lo que generaría una sociedad totalitaria. Por ello, es imprescindible incorporar al presente documento la perspectiva de la transparencia, para lo cual analizaré brevemente su naturaleza y/o el derecho de acceso; para a continuación examinar su relación con el derecho a la protección de datos y por último insistir en la necesidad de aprobar cuanto antes una ley de transparencia, tras poner de manifiesto la insostenible situación normativa en la que nos encontramos en España respecto a esta materia.

3.1 Sobre la transparencia en una sociedad democrática. Acceso a la información y transparencia como derecho fundamental o como principio de actuación de los poderes públicos

La transparencia es esencial en las sociedades democráticas. No sólo en relación con el sector público, sino como principio configurador de la sociedad. En la Declaración de la Cumbre sobre los mercados financieros y la economía mundial, adoptada en Washington el pasado 15 de noviembre de 2008 con motivo de la profunda crisis financiera que está sufriendo el planeta, se insiste en numerosas ocasiones en la necesidad de incrementar la transparencia de las instituciones y los mercados financieros, en particular de los mercados de derivados crediticios, así como de los entes reguladores y los organismos internacionales responsables del establecimiento de normas contables. También se prevé impulsar la transparencia de las valoraciones de los sistemas regulatorios nacionales de cada país y se subraya que la falta de transparencia es uno de los aspectos que debe ser tratado "de manera enérgica" a medio plazo. Nadie duda ya de que uno de los motivos de la crisis ha sido y es la falta de transparencia de los mercados. Como nadie duda tampoco de que no pocos de los casos de corrupción en sectores como el urbanismo se deben tam-

bién a la falta absoluta de transparencia que en ellos se da. Falta de transparencia y corrupción van de la mano. Y no sólo en España: en Francia, el Consejo de Estado ya resaltó en su *Rapport 1995* sobre *La transparence et le secret*, que la transparencia es un medio de evitar que la opacidad en la adopción de decisiones haga saltar las sospechas de favoritismo, corrupción o arbitrariedad (Christine Maugüe, 2004:609).

Que la transparencia es un elemento esencial de cualquier Estado democrático es ya algo fuera de toda duda. Se trata de una de las más insistentemente reivindicadas exigencias de la democracia. Según decía el juez del Tribunal Supremo de Estados Unidos, Luis B. Brandeis (1932), *"Sunlight is said to be the best of disinfectants"*, ("la luz del sol es el mejor de los desinfectantes"). Rodota ha recordado la feliz cita del juez (2003). Gherardo Colombo resalta que lo que él denomina "sociedad horizontal", basada no en relaciones jerárquicas y competitivas, sino en la dignidad de la persona y en la igualdad con reconocimiento de la diversidad (2008:41 y ss.), "no tolera ninguna opacidad de las instituciones: la administración debe ser transparente; es necesario verificar su funcionamiento y controlar si todos son tratados de igual manera, bajo cualquier circunstancia (admisión del personal, oferta de prestaciones, corrección de los procedimientos…). La sociedad horizontal no tolera recomendaciones, y no puede convivir en absoluto con una información inexistente, facciosa o incompleta." (2008:55). Como se ha señalado, "la democracia exige un incesante proceso hacia la máxima transparencia de la Administración" (Sainz Moreno, 2004:166). El Tribunal Supremo, en su sentencia de 1 de abril de 2003, ha señalado en relación con el acceso a la información que "su relevancia implica que no se ponga meramente en cuestión un problema de transparencia informativa, sino la propia racionalidad del funcionamiento del sistema democrático y el Estado de Derecho".

> "Administración en democracia significa Administración *transparente*" (Sánchez Morón, 2008:81). Transparente para poder exigir responsabilidad a nuestros gobernantes. Como ha señalado en más de una ocasión la Comisión Europea, "un alto estándar de transparencia es parte de la legitimidad de cualquier Administración moderna"[10]. El Tribunal de Justicia ha resaltado la relación entre transparencia y democracia en su sentencia de 1 de julio de 2008. Ya mucho antes, en la Declaración de Derechos del hombre y el ciudadano de 1789, se afirmaba (artículo 15) que "La sociedad tiene derecho a pedir cuentas de su gestión a todo agente público"[11].

10 *Green Paper European Transparency Initiative*, Bruselas, 3.5.2006 COM(2006) 194 final, pág. 2.

11 La relación entre transparencia y rendición de cuentas, responsabilidad o *accountability* ha sido puesta de manifiesto también por Charles Lindblom (1990), tal como ha recordado J.P. Guerrero (2005) en M. Merino (Coordinador) (2005:51). También en Italia, Sorace (2002:57) parte del principio de la responsabilidad administrativa, que, tal como deriva del artículo 97 de la Constitución italiana, implica el deber de someter al control de los ciudadanos la actuación administrativa (dado que es función de la Administración servir los intereses de los ciudadanos en general. Por otra parte, considera el principio de transparencia como "principio o regla complementaria o instrumental" de la discrecionalidad administrativa, (2002:279).

La transparencia hace referencia a tres elementos y sus características: el proceso de elaboración de decisiones por los entes públicos que ha de ser abierto y participado; las decisiones que deben ser motivadas y razonables; la información que sirve de base a la adopción de decisiones debe ser, en la medida de lo posible, accesible al público (Supervisor Europeo de Protección de Datos, 2005:4).

Ahora bien, el acceso a la información, ¿es un derecho o un principio de actuación de las Administraciones públicas? La respuesta que se dé es de suma importancia en las relaciones entre protección de datos y transparencia, pues si aquélla es un derecho fundamental y ésta un simple principio de actuación, es evidente que la primera debe siempre prevalecer sobre la segunda. Si, por el contrario, consideramos que se trata de un derecho fundamental, el equilibrio debe buscarse desde otros parámetros muy diferentes.

En el Derecho español parece que prevalece la configuración de la transparencia como principio de actuación de las Administraciones públicas. Así se desprendería de la propia ubicación del artículo 105.b) de la Constitución, incluido en el Título IV, sobre el Gobierno y la Administración. El artículo 3.5 de la Ley 30/1992 dispone que "en sus relaciones con los ciudadanos las Administraciones públicas actúan de conformidad con los principios de transparencia y participación". El Preámbulo de la Ley 4/2006, de 30 de junio, de transparencia y de buenas prácticas en la Administración pública gallega, afirma que al regular la transparencia se contribuye a "hacer más efectivo el derecho a una buena Administración, como principio consagrado en nuestro acervo jurídico desde la aprobación de la Carta de los derechos fundamentales de la Unión Europea".

El Tribunal de Justicia también ha señalado en varias ocasiones que "el principio de transparencia tiene por objetivo asegurar una mejor participación de los ciudadanos en el proceso decisorio, así como garantizar una mayor legitimidad, eficacia y responsabilidad de la Administración frente a los ciudadanos en un sistema democrático. Contribuye a reforzar el principio de la democracia y el respeto de los derechos fundamentales" (sentencia del Tribunal de Primera Instancia de 7 de febrero de 2002, Kuijer contra Consejo, As. T-211/00, apartado 52. En ella se cita la anterior STPI de 14 de octubre de 1999, Bavarian Lager contra Comisión, As. T-309/97).

Sin embargo, en una declaración conjunta de la ONU, la OECE y la OEA, de 6 de diciembre de 2004, se afirma que "el derecho de acceso a la información en poder de las autoridades públicas es un derecho humano fundamental que debería aplicarse a nivel nacional a través de legislación global (por ejemplo, las Leyes de Libertad de Acceso a la Información) basada en el principio de máxima divulgación, el cual establece la presunción de que toda la información es accesible, sujeta solamente a un sistema restringido de excepciones" (Piñar Mañas, 2007:66 y ss.). Cada vez se habla con más insistencia del derecho a conocer, del *right to know* (entre otros, Blanton, 2002:50 y ss.; Foerstel, 1999).

La sentencia de la Corte Interamericana de Derechos Humanos de 19 de septiembre de 2006, Caso Claude Reyes y otros contra Chile, analiza la violación del derecho de acceder a información bajo el control del Estado. Afirma, en doctrina novedosa respecto a decisiones anteriores, que el artículo 13 de la Convención Americana de Derechos Humanos de 1969 (Pacto de San José de Costa Rica), por el que se reconoce la libertad de pensamiento y de expresión, al estipular expresamente los derechos a "buscar" y a "recibir" informaciones, protege el derecho que tiene toda persona a solicitar el acceso a la información bajo el control del Estado, con las salvedades permitidas bajo el régimen de restricciones de la Convención. Consecuentemente, "dicho artículo ampara el derecho de las personas a recibir dicha información y la obligación positiva del Estado de suministrarla, de forma tal que la persona pueda tener acceso a conocer esa información o reciba una respuesta fundamentada cuando por algún motivo permitido por la Convención el Estado pueda limitar el acceso a la misma para el caso concreto… Dicha información debe ser entregada sin necesidad de acreditar un interés directo para su obtención o una afectación personal, salvo en los casos en que se aplique una legítima restricción…".

Se trata de una doctrina que merece una especial atención, si bien es verdad que el derecho de acceso queda vinculado en exceso a la libertad de expresión e información[12]. En cualquier caso, contrasta con la fluctuante y poco ambiciosa de nuestros tribunales, tanto del Tribunal Supremo como del Constitucional.

Finalmente, es imprescindible hacer referencia a la Carta de Derechos Fundamentales de la Unión Europea. En ella, y en el Capítulo V, sobre "Ciudadanía", se recoge el derecho a una buena Administración (art. 41) que incluye entre otros aspectos "el derecho de toda persona a acceder al expediente que le afecte, dentro del respeto de los intereses legítimos de la confidencialidad y del secreto profesional y comercial". Pero en el artículo 42 se reconoce, ya no vinculado a la buena Administración, sino como derecho autónomo, el "derecho de acceso a los documentos" en los siguientes términos: "Todo ciudadano de la Unión o toda persona física o jurídica que resida o tenga su domicilio social en un Estado miembro tiene derecho a acceder a los documentos del Parlamento Europeo, del Consejo y de la Comisión".

Es decir, la Carta no se refiere a la transparencia en términos amplios, ni siquiera al derecho a la información: ha optado por el reconocimiento del derecho de acceso a los documentos, de alcance más limitado, si bien lo incorpora como derecho fundamental. Además, lo ha configurado como derecho de los ciudadanos europeos y de los residentes o domiciliados en algún Estado miembro, y referido sólo a tres de las Instituciones

12 Como ya hacía la Declaración sobre libertad de expresión e información del Consejo de Europa, de 29 de abril de 1982. El texto puede consultarse en la dirección https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=601273&SecMode=1&DocId=675536&Usage=2

Europeas. En principio, pues, podría parecer que estamos ante una regulación restrictiva de la transparencia. Basta, por ejemplo, con ver la diferencia que en cuanto a la regulación concreta de ambos derechos se produce respecto de la protección de datos que, como ya sabemos, se reconoce en el artículo 8º, pero a favor de "toda persona".

Sin embargo, además de que el derecho de acceso a la información puede hacerse derivar de la libertad de expresión e información reconocido a "toda persona" y de forma expresa en el artículo 11 de la Carta, está en marcha, como veremos más adelante, una propuesta de reforma del Reglamento Comunitario 1049/2001 (al que luego me referiré con más detalle) por la que se extiende notablemente el ámbito subjetivo de los titulares del derecho de acceso, al objeto de reconocerlo a cualquier persona física o jurídica, sin necesidad de demostrar interés legítimo alguno que justifique el acceso. Y se reconoce, no como simple derecho de acceso a los documentos, sino a la información en poder de las instituciones. Se da así un paso capital hacia el reconocimiento del acceso a la información como verdadero derecho fundamental.

3.2 Transparencia y protección de datos: las claves de una relación

Admitido lo anterior, debemos intentar fijar los términos de la relación entre ambos derechos: la transparencia y la protección de datos.

Daniel J. Solove se pregunta: "¿Cómo puede reconciliarse la tensión entre transparencia y privacidad? ¿Debe sacrificarse el acceso a los documentos en el altar de la privacidad? ¿O debe la privacidad evaporarse para poder desinfectar los gobiernos con la luz del sol?" (2004:150).

Resulta, en efecto, imprescindible aclarar la relación existente entre transparencia y protección de datos, sobre todo teniendo en cuenta que la transparencia es capital para el desarrollo de una sociedad abierta y democrática, y que el respeto a la protección de datos no debe considerarse un obstáculo al derecho de acceso a la información, sin olvidar que una de las excepciones que pueden invocarse al ejercer el derecho de acceso es la derivada de la protección de datos, o de la existencia de información o documentos que afecten a la intimidad de las personas, así como de información que afecte a la seguridad ciudadana. Westin (1967:23-25) ha señalado con acierto que los Estados totalitarios se apoyan en el secreto respecto del régimen y la visibilidad de los grupos e individuos, mientras que la sociedad democrática descansa sobre el control al gobierno y el respeto a la privacidad.

Ni la transparencia ni la protección de datos son absolutos. Es imprescindible conseguir un equilibrio entre ambos derechos.

El Grupo de Trabajo del Artículo 29 de la Directiva 95/46/CE, en su Dictamen 3/99, relativo a Información del sector público y protección de datos personales (WP 20) aprobado el 3 de mayo de 2003, señala que "el legislador, cuando desea que un dato se vuelva accesible al público no considera ,sin embargo, que haya de convertirse en *res nullius*. Tal es la filosofía del conjunto de nuestras legislaciones. El carácter público de un dato de carácter personal, resulte de una normativa o de la voluntad de la propia persona a la que alude el dato, no priva *ipso facto* y para siempre a dicha persona de la protección que le garantiza la ley en virtud de los principios fundamentales de defensa de la identidad humana". Resulta necesario conciliar el respeto del derecho a la intimidad y a la protección de los datos personales de los ciudadanos con el derecho a acceder a la información del sector público, y en este sentido el Grupo concluye que es necesario tener en cuenta los siguientes aspectos:

- Valoración caso por caso de la cuestión de si un dato de carácter personal puede publicarse/hacerse accesible o no, y en caso afirmativo en qué condiciones y en qué soporte (digitalización o no, difusión en internet o no, etc.).

- Principios de finalidad y legitimidad.

- Información de la persona en cuestión.

- Derecho de oposición de la persona en cuestión; utilización de las nuevas tecnologías para contribuir al respeto del derecho a la intimidad.

El Supervisor Europeo de Protección de Datos, en su importante documento *Public access to documents and data protection,* ha centrado con brillantez los términos del debate.

También es importante la jurisprudencia europea, ya abundante. Me centraré en la sentencia del Tribunal de Justicia de 20 de mayo de 2003, Rundfunk y otros*,* Asuntos C-465/00, C-138/01 y C-139/01, y en la sentencia del Tribunal de Primera Instancia de 8 de noviembre de 2007, Bavarian Lager contra Comisión*,* Asunto T-194/04. Ambas son capitales para analizar la relación entre protección de datos y acceso a la información en el derecho comunitario (véase Piñar Mañas, 2003:61 y ss.).

La sentencia Rundfunk señala que en el tratamiento de datos personales son de aplicación los "principios relativos a la calidad de los datos" enunciados en el artículo 6 de la Directiva 95/46/CE y los "principios relativos a la legitimación del tratamiento de datos" enumerados en su artículo 7. En particular debe tenerse en cuenta el principio de finalidad y proporcionalidad, y el hecho de que según el citado artículo 7, letras c) y e), "el tratamiento de datos personales es lícito, respectivamente si, 'es necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento', o si 'es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento [...] a quien se comuniquen los datos'" (apartados 65 y 66 de la sentencia).

Además, la Directiva debe interpretarse a la luz de los derechos fundamentales que, como sabemos, forman parte de los principios generales del Derecho comunitario. En particular, el artículo 8 del Convenio Europeo de Derechos Humanos (CEDH) "al tiempo que enuncia, en su apartado 1, el principio de no injerencia de la autoridad pública en el ejercicio del Derecho a la vida privada, admite, en su apartado 2, que una injerencia de este tipo es posible en tanto en cuanto esté 'prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y libertades de los demás'" (apartado 71). Dicho esto, se afirma que la comunicación a terceros (aunque sea a otra autoridad pública) de los datos relativos a las remuneraciones del personal directivo de organismos públicos lesiona el derecho al respeto de la vida privada de los interesados, sea cual fuere la utilización posterior de los datos comunicados de este modo, y presenta el carácter de una injerencia en el sentido del artículo 8 del CEDH". Además, "la injerencia se produce al margen de que los datos comunicados tengan o no carácter sensible o que los interesados hayan sufrido o no eventuales inconvenientes en razón de tal injerencia... Basta con observar que el empleador ha comunicado a un tercero los datos relativos a los ingresos que percibe un trabajador o un pensionista" (apartado 74).

Partiendo de la base de que la comunicación de datos a un tercero supone una injerencia en la vida privada, el Tribunal analiza si la misma está o no justificada.

A tal fin señala que la finalidad de dar a conocer los datos de las retribuciones es presionar a las entidades públicas afectadas para que las mantengan en unos límites razonables y garantizar la utilización apropiada de los fondos públicos por la Administración. "Tal objetivo –dice el Tribunal– constituye un objetivo legítimo tanto en el sentido del artículo 8, apartado 2, del CEDH, que tiene por objeto el 'bienestar económico del país», como del artículo 6, apartado 1, letra b), de la Directiva 95/46, que se refiere a «fines determinados, explícitos y legítimos'" (apartado 81). Pero ¿es necesaria tal injerencia? El Tribunal señala que, por un parte, "no se puede negar que para controlar la buena utilización de los fondos públicos, el *Rechnungshof* (Tribunal de Cuentas) y las distintas Asambleas Parlamentarias necesitan conocer el importe de los gastos afectados a los recursos humanos en las distintas entidades públicas". A ello se suma, en una sociedad democrática, el derecho de los contribuyentes y de la opinión pública en general a ser informados de la utilización de los ingresos públicos, especialmente en materia de gastos de personal. Tales datos, reunidos en el informe, pueden contribuir al debate público relativo a una cuestión de interés general y sirven, por tanto, al interés público.

Se plantea, no obstante, la cuestión de si la indicación del nombre de las personas afectadas junto con los ingresos que perciben es proporcionada a la finalidad legítima perseguida y si los motivos invocados para justificar tal divulgación resultan pertinentes y suficientes (apartados 85 y 86). Y el Tribunal llega a la siguiente conclusión: "Procede declarar que la injerencia derivada de la aplicación de una normativa nacional como la

controvertida en los asuntos principales solamente puede justificarse, al amparo del artículo 8, apartado 2, del CEDH, en la medida en que la amplia divulgación no sólo del importe de los ingresos anuales, cuando éstos superan un límite determinado, de las personas empleadas por entidades sujetas al control del *Rechnungshof*, sino también de los nombres de los beneficiarios de dichos ingresos, sea a la vez necesaria y apropiada para lograr el objetivo de mantener los salarios dentro de unos límites razonables, extremo que ha de ser examinado por los órganos jurisdiccionales remitentes" (apartado 90). A la misma conclusión llega el Tribunal al analizar la cuestión a la luz de la Directiva 95/46/CEE: "Los artículos 6, apartado 1, letra c), y 7, letras c) y e), de la Directiva 95/46 no se oponen a una normativa nacional, como la controvertida en los asuntos principales, siempre que se demuestre que la amplia divulgación no sólo del importe de los ingresos anuales, cuando éstos superan un límite determinado, de las personas empleadas por las entidades sujetas al control del *Rechnungshof*, sino también de los nombres de los beneficiarios de dichos ingresos, es necesaria y apropiada para lograr el objetivo de buena gestión de los recursos públicos perseguido por el constituyente, extremo que ha de ser comprobado por los órganos jurisdiccionales remitentes" (apartado 94 de la Sentencia).

Como vemos, y pese a que el Tribunal de Justicia no acierta a ofrecer una solución clara a la cuestión planteada, una vez más salen a la luz los principios esenciales del derecho a la protección de datos, en particular los de finalidad y proporcionalidad. Es en éstos donde debe encontrarse el equilibrio entre transparencia y protección de datos.

La sentencia Bavarian Lager de 2007 juzga si era pertinente facilitar a terceros interesados los datos de las personas que intervinieron en una reunión de trabajo de la Comisión. El Tribunal parte de la base de que la lista de los participantes en la reunión que figuran en el acta de la misma contiene datos personales. Pero a partir de aquí lleva a cabo una serie de consideraciones que desembocan en la decisión de que tales datos deben ser facilitados cuando se lleva a cabo una solicitud de acceso a la información basándose en el Reglamento 1049/2001.

Según el Tribunal, "debe constatarse que el mero hecho de que un documento contenga datos personales no significa necesariamente que se ponga en peligro la intimidad o la integridad de las personas de que se trata, a pesar de que la actividad profesional no esté, en principio, excluida del concepto de 'vida privada' en el sentido del artículo 8 del CEDH" (apartado 123 de la Sentencia). En particular, contener los nombres de los representantes de las entidades que participaron en la reunión no pone en peligro la intimidad de las personas, pues éstas actúan en representación de sus entidades y las opiniones vertidas en la reunión no contienen opiniones individuales, sino posturas imputables a las entidades. Tales consideraciones son esenciales para la decisión del Tribunal: el asunto controvertido entra en el ámbito de aplicación del Reglamento 1049/2001 que (como de inmediato veremos) recoge como excepción al principio de apertura y derecho de acceso no la divulgación de cualquier dato, sino de datos personales que puedan suponer un perjuicio para la protección de la intimidad y la integridad de las personas.

Esto hace que el caso analizado deba considerarse diferente al que fue objeto de la sentencia Rundfunk a la que acabo de referirme, pues en ella lo relevante es que hubiese habido un tratamiento de datos personales, con independencia de que afectasen o no a la intimidad de los interesados. Ahora el Tribunal de Primera Instancia concluye que "la divulgación de los nombres en cuestión no da lugar a una injerencia en la intimidad de las personas que participaron en la reunión y no supone un perjuicio para la protección de su intimidad y de la integridad de sus personas" (apartado 132), por lo que tales datos pueden y deben ser facilitados a quien lo solicitó. Incluso aunque los interesados se hubiesen opuesto a ello, si no demuestran que su intimidad e integridad habrían sufrido un perjuicio con su divulgación.

Vemos pues que, en su relación con la transparencia, el respeto a la protección de datos personales no siempre ha de prevalecer. Es imprescindible llevar a cabo un análisis caso a caso.

3.3 La regulación del derecho de acceso en el Derecho comunitario. Especial referencia al Reglamento (CE) nº 1049/2001, del Parlamento y del Consejo, de 30 de mayo de 2001 (y la propuesta para su reforma)

La evolución del derecho de acceso en el ámbito comunitario[13] tiene un punto de referencia importante en el Tratado de Maastricht. La Declaración nº 17, relativa al derecho de acceso a la información, establece: "La Conferencia estima que la transparencia del proceso de decisión refuerza el carácter democrático de las Instituciones, así como la confianza del público en la Administración. La Conferencia recomienda, por consiguiente, que la Comisión presente al Consejo, a más tardar en 1993, un informe sobre medidas destinadas a mejorar el acceso del público a la información de que disponen las Instituciones".

El Tratado de Ámsterdam continúa el proceso de consolidación del derecho de acceso. Así, el artículo 255 del Tratado Constitutivo de la Comunidad Europea establece que todo ciudadano de la Unión, así como toda persona física o jurídica que resida o tenga su domicilio social en un Estado miembro, tendrá derecho a acceder a los documentos del Parlamento, del Consejo y de la Comisión (véase también la Declaración 35, Aneja al Acta Final del Tratado de Ámsterdam). Posteriormente, el Reglamento (CE) nº 1049/2001, del Parlamento y del Consejo, de 30 de mayo de 2001, ha regulado el acceso a los documen-

13 Esta evolución ha sido muy bien descrita por el Tribunal de Primera Instancia (TPI) en su sentencia de 19 de julio de 1999, Hautala, T-14/98, y por el Tribunal de Justicia en su sentencia de 6 de diciembe de 2001, Hautala, C-353/99 P (dictada en el recurso de casación interpuesto contra la Sentencia del TPI). Véase Piñar Mañas (2007:70-71).

tos de dichas Instituciones. Por otra parte, tanto el Tratado de Lisboa como la Carta de los Derechos Fundamentales de la Unión Europea reconocen el derecho de acceso.

El Reglamento constituye hoy por hoy la principal norma sobre el régimen de acceso a los documentos de las Instituciones. No regula con carácter general la transparencia y el derecho de acceso en el ámbito de la Unión Europea, pero sí constituye una referencia que debe tomarse en consideración. En cualquier caso, está ya muy avanzado el proceso de modificación de su texto, al objeto sobre todo de adaptarlo a la experiencia acumulada durante su vigencia y a la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas y del Tribunal de Primera Instancia. Existe ya una Propuesta formal para modificar el Reglamento, a la que haré referencia a continuación[14].

El principio general que da pie al Reglamento es el de "apertura". La apertura, como señala su segundo considerando, "permite garantizar una mayor participación de los ciudadanos en el proceso de toma de decisiones, así como una mayor legitimidad, eficacia y responsabilidad de la Administración para con los ciudadanos en un sistema democrático. La apertura contribuye a reforzar los principios de democracia y respeto de los derechos fundamentales contemplados en el artículo 6 del Tratado UE y en la Carta de los Derechos Fundamentales de la Unión Europea". Partiendo de lo anterior, pretende facilitar "el acceso más amplio posible a los documentos" (art. 1 a), al tiempo que determina los límites y excepciones a dicho acceso.

Los beneficiarios del derecho de acceso se especifican en el artículo 2.1: "todo ciudadano de la Unión, así como toda persona física o jurídica que resida o tenga su domicilio social en un Estado miembro, tiene derecho a acceder a los documentos de las instituciones, con arreglo a los principios, condiciones y límites que se definen en el Reglamento". En cuanto a quienes no residan ni tengan su domicilio en un Estado miembro, las Instituciones "podrán" conceder el acceso de acuerdo con los mismos principios, condiciones y límites (art. 2.2.). Además, no es necesario acreditar un interés legítimo que justifique el acceso: el artículo 6.1 del Reglamento deja sentado que el solicitante no está obligado a especificar las razones por las que lo solicita. La no necesidad de demostrar o justificar un interés ha sido ya resaltada por el Tribunal de Primera Instancia de las Comunidades Europeas en diversas ocasiones; recientemente en la ya citada sentencia de 8 de noviembre de 2007, Bavarian Lager contra Comisión, epígrafe 92 (también en la STPI de 6 de julio de 2006, Franchet y Byk contra Comisión, Asuntos T-391/03 y T-70/04). La propuesta de reforma del Reglamento va mucho más allá a la hora de reconocer legitimación para la solicitud de acceso. Se pretende, en efecto, extender la legitima-

14 *Proposal for a Regulation of the European Parliament and the Council regarding public access to European Parliament, Council and Commission documents (presented by the Commission)*, Bruselas, 30 de abril de 2008. COM(2008) 229 final. Sobre tal propuesta tiene especial interés la Opinión del Supervisor Europeo de Protección de Datos, de 30 de junio de 2008 (localizable en www.edps.europa.eu).

ción a "toda persona física o jurídica" con independencia de su ciudadanía, residencia o domicilio. Se daría así un gran paso adelante en la configuración del derecho.

Es importante destacar que el acceso se extiende a "todos los documentos que obren en poder de una institución; es decir, los documentos por ella elaborados y que estén en su posesión, en todos los ámbitos de actividad de la Unión Europea" (art. 2.3). Alcanza, pues, a los tres pilares, y no sólo al ámbito propiamente comunitario. De hecho, en el Considerando 17 del Reglamento se afirma que el reconocimiento del derecho de acceso puede exigir que se modifiquen, entre otras disposiciones, "las normas de confidencialidad de los documentos de Schengen" (la propuesta de reforma del Reglamento incorpora una novedad aparentemente menor pero de cierto calado, también en base a la jurisprudencia del Tribunal de Justicia. La expresión "es decir" se sustituye por "en particular", lo que amplía el tipo de documentos respecto de los que cabe solicitar el acceso).

Basándose en lo anterior, es posible hacer algunas consideraciones:

- Primera, que el derecho de acceso se refiere a todos los documentos que obren en poder de las instituciones, es decir, no sólo los que hayan sido elaborados por éstas, sino también los que hayan recibido y estén en su posesión. Es decir, como señala la STPI de 30 de noviembre de 2004, IFAW *Internationaler contra Comisión*, As. T-168/02, el Reglamento 1049/2001 no recoge la llamada "regla del autor" y confirma que, en principio, todos los documentos de las instituciones deben ser accesibles al público. Quizá convenga aclarar que la "regla del autor" se traduce en que "cuando el autor del documento que posea la institución [fuese] una persona física o jurídica, un Estado miembro, otra institución u órgano comunitario, o cualquier otro organismo nacional o internacional, la solicitud [debe] dirigirse directamente al mismo", es decir, al autor del documento. Y que la misma estaba recogida en diversas disposiciones previas a la entrada en vigor del Reglamento (apartado 53 de la Sentencia). Ahora bien, en caso de documentos originarios de terceros, las instituciones deben consultarles antes de conceder el acceso, al objeto de verificar si son o no aplicables las excepciones previstas en el repetido Reglamento.

- Segunda, como antes hemos visto, el derecho de acceso a la información no es del todo equivalente al acceso a documentos. En esta línea, el Reglamento recoge al menos dos previsiones que merece la pena resaltar. Por un lado, la propia definición de documento, referida al "contenido", y no tanto al soporte[15]. Por otro, porque, de acuerdo con la doctrina del Tribunal de Justicia, el Reglamento señala de forma

15 El artículo 3.a) del Reglamento define "documento" como "todo contenido, sea cual fuere su soporte (escrito en versión papel o almacenado en forma electrónica, grabación sonora, visual o audiovisual) referentes a temas relativos a las políticas, acciones y decisiones que sean competencia de la institución".

expresa que cuando se solicite el acceso a un documento y sean aplicables a parte del mismo algunas de las excepciones previstas, deberán divulgarse las demás partes (art. 4.6).

Merecen especial atención las excepciones al derecho de acceso. El artículo 4º del Reglamento distingue entre las que se han llamado excepciones absolutas y excepciones relativas, considerando que las segundas están sujetas al examen de ponderación del interés público en la divulgación de los documentos.

El artículo 4.1 regula las excepciones absolutas: las Instituciones denegarán el acceso a un documento cuya divulgación suponga un perjuicio para la protección de, por un lado, el interés público por lo que respecta a la seguridad pública, la defensa y los asuntos militares, las relaciones internacionales o la política financiera, monetaria o económica de la Comunidad o de un Estado miembro; y, por otro, de la intimidad y la integridad de las personas, en particular de conformidad con la legislación comunitaria sobre protección de los datos personales (art. 4.1 del Reglamento). Excepción esta que es especialmente relevante en el presente documento.

Por su parte, el nº 2 del mismo artículo 4 recoge las excepciones relativas. Señala que las Instituciones denegarán el acceso a un documento cuya divulgación suponga un perjuicio para, a) la protección de los intereses comerciales de una persona física o jurídica, incluida la propiedad intelectual, b) los procedimientos judiciales y el asesoramiento jurídico (sobre ello véase STPI de 23 de noviembre de 2004, Mauricio Turco); o c) el objetivo de las actividades de inspección, investigación y auditoría, salvo que su divulgación revista un interés público superior. Es decir, debe llevarse a cabo una ponderación del perjuicio que pueda suponer el acceso y el interés público que pueda justificarlo.

Sin poder entrar ahora en el análisis de las referidas excepciones al derecho de acceso, señalaré con carácter general que:

- "El acceso del público a los documentos de las instituciones constituye el principio jurídico, y la posibilidad de denegación es la excepción" (STPI de 7 de febrero de 2002, Kuijer contra Consejo*,* As. T-211/00; STPI de 8 de noviembre de 2007, Bavarian Lager).

- Tales excepciones deben interpretarse y aplicarse de forma estricta (STPI de 13 de septiembre de 2000, Denkavit Nederland contra Comisión, As. T-20/99, y de 23 de noviembre de 2004, Mauricio Turco contra Consejo, As. T-84/03, entre otras), de modo que "no frustre el principio general" de acceso.

- Las excepciones deben interpretarse "a la luz del principio del derecho a la información y del principio de proporcionalidad". De ello se desprende que las Instituciones deberán, en su caso, examinar si procede conceder un acceso parcial, limitado a los datos no

amparados por las excepciones; y que "con carácter extraordinario, podría admitirse una excepción a dicha obligación de conceder una acceso parcial cuando la carga administrativa provocada por la disimulación *(sic)* de los datos no comunicables se revelara extraordinariamente gravosa, excediendo así de los límites de lo que puede exigirse razonablemente" (STPI Kuijer, antes citada, apartado 57. En parecidos términos, la STPI de 6 de abril de 2000, también Kuijer contra Consejo, As. T-188/98).

- En particular, y en lo que se refiere a la excepción del derecho a la privacidad, debe traerse ahora a colación el Reglamento nº 45/2001, sobre protección de datos[16]. Pese a que la excepción de la protección de la intimidad es considerada absoluta, lo cierto es que, como la Comisión ha señalado, "la decisión sobre el acceso a los documentos que contengan datos personales debe resultar de una ponderación de los derechos e intereses en juego, a saber, por una parte la información del público y, por otra, la protección de las personas afectadas. Este balance debe hacerse caso por caso, teniendo en cuenta las circunstancias específicas de cada caso"[17].

La propuesta de reforma del Reglamento modifica sustancialmente el régimen de las excepciones. Por un lado abandona la distinción entre excepciones absolutas y relativas, eliminando cualquier referencia a que la divulgación de la información revista un interés público superior. Por otro, lo que nos interesa especialmente, reelabora la excepción relativa a la privacidad, que se reconduce mucho más a la protección de datos, en estos términos: los nombres, títulos y funciones de los cargos públicos, de los empleados públicos y de los representantes de intereses, en relación con sus actividades serán facilitados salvo que, en casos particulares, el acceso pueda afectar a dichas personas. Cualquier otro dato personal será suministrado de acuerdo con las condiciones del tratamiento legítimo de tales datos, tal como se prevé en la legislación de la Comunidad Europea sobre la materia.

3.4 El marco normativo de la transparencia en España

Se considera que, aproximadamente 70 países cuentan con leyes de transparencia y/o acceso a la información. Entre ellos, desde luego, no puede contarse a España.

Como ha señalado T. S. Blanton (2002b:10), la primera ley de acceso a la información es seguramente la *Freedom of the Press Act* aprobada en Suecia en 1766, que permitió la

16 Reglamento (CE) nº 45/2001, del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de esos datos.

17 Informe de la Comisión sobre la aplicación de los principios del Reglamento (CE) nº 1049/2001, relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión, de 30 de enero de 2004, COM (2004) 45 final, pág. 20.

publicación de documentos del gobierno y el acceso público a los mismos. Sin embargo, hubo que esperar casi dos siglos para encontrar leyes semejantes en otros países. En 1951, Finlandia aprueba una ley de acceso a la información, y en 1966, Estados Unidos, la conocida *Freedom of Information Act* (FOIA), una de las leyes más generosas en la implantación del principio de transparencia. En 1978, se aprueba la ley francesa. Aunque no supone una novedad digna de ser tenida en consideración, no está de más señalar que en la vecina Italia recientemente se han aprobado las leyes de 11 de febrero de 2005, nº 15, de 14 de mayo de 2005, nº 80 (por las que, entre otros muchos aspectos, sobre todo en la segunda, se incluyen modificaciones a la Ley de procedimiento de 7 de agosto de 1990, nº 241, en materia de acceso a documentos) y la Ley de Delegación nº 15, de 4 de marzo de 2009, cuyo artículo 4º incorpora alguna referencia a la transparencia[18]. Finalmente, debe señalarse que entre los países de la Comunidad Iberoamericana existe una cada vez más consolidada cultura de transparencia y acceso a la información (el desarrollo en los años ochenta y noventa del pasado siglo fue muy notable), debida sin duda a la influencia de Estados Unidos (ejemplo claro de ello es la muy avanzada Ley Federal Mexicana de Transparencia y Acceso a la Información Pública Gubernamental, de 11 de junio de 2002).

Sin embargo, España sigue siendo uno de los pocos países europeos que carece de ley de transparencia o ley de acceso a la información pública. El mandato contenido en el artículo 105. b) de la Constitución está todavía sin desarrollar, pese a que el derecho a la transparencia, como ya hemos visto, puede considerarse hoy un derecho fundamental.

En la regulación sobre transparencia y acceso a la información todavía falta mucho camino por recorrer. Camino que es necesario completar cuanto antes, pues de otro modo habremos de conformarnos con una legislación sectorial totalmente insuficiente y con una doctrina del Tribunal Supremo y del Constitucional en relación con el derecho de acceso a la información no muy halagüeña, que parece sentirse siempre obligada a encontrar una conexión con otro derecho o principio[19].

Sin perjuicio de la Ley 4/2006, de 30 de junio, de transparencia y de buenas prácticas en la Administración Pública Gallega, el derecho de acceso hoy está regulado con carácter general en el artículo 37 de la Ley 30/1992, de Bases del Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, modificada por la 4/1999, en cuyo análisis, por suficientemente conocido, no vamos a entrar en este Documento[20]. En

18 Publicada en la *Gazeta Ufficiale* de 6 de marzo de 2009. La Ley añade un inciso al artículo 1º del Decreto Legislativo 196/2003, por el que se aprueba el Texto Único de la Ley de Protección de Datos.

19 Véase STS de 19 de mayo de 2003, clara y desalentadora, STS de 18 de noviembre de 2003, STS de 27 de septiembre de 2002 o STS de 25 de octubre de 2002.

20 Sobre ello hay ya bibliografía conocida. Entre otros véanse Fernández Ramos, Severiano, (1997); Mestre Delgado, Juan Francisco (1998); Pomed Sánchez, Luis Alberto, (1989); Da Silva Ochoa, Juan Carlos (1993, especialmente: 318 y ss.); Embid Irujo, Antonio, (1993a y b); Parada Vázquez (1993, especialmente: 153 y ss.); Rams Ramos, Leonor (2008); Santamaría Pastor, Juan Alfonso (1993, especialmente: 89 y ss.); Villanueva Cuevas, Antonio (1993).

cualquier caso, es indudable que tal precepto no cumple en absoluto las previsiones del artículo 105.b) de la Constitución. Además, se trata de una Ley que da la espalda a la Ley Orgánica de Protección de Datos, lo que es especialmente grave por muchos motivos, pero sobre todo porque la Ley 30/1992 estaba debatiéndose en el Parlamento al mismo tiempo que la vieja Ley Orgánica de Tratamiento Automatizado de Datos de carácter personal, y la Ley 4/1999 coincidió con la LOPD. Y en ambos casos, como digo, los legisladores parecieron no darse cuenta de la necesidad de coordinar los textos finalmente aprobados.

La regulación fragmentaria de la Ley 30/1992 es a todas luces insuficiente. Como lo es la regulación del derecho de acceso en legislaciones sectoriales. No resuelve el problema de la transparencia la que fue "pionera" en la materia, la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español, en particular su artículo 57[21]. Es insuficiente la regulación de la Ley 27/2006, de 18 de julio, por la que se regulan los derechos de acceso a la información, de participación pública y de acceso a la justicia en materia de medio ambiente. Tampoco es suficiente la Ley 4/2007, de 3 de abril, de transparencia de las relaciones financieras entre las Administraciones públicas y las empresas públicas, y de transparencia financiera de determinadas empresas, por la que se traspone la Directiva 2006/111/CE de la Comisión, de 16 de noviembre de 2006, y que pretende garantizar la transparencia de las relaciones financieras entre las Administraciones públicas y las empresas públicas a través del suministro de información sobre la puesta a disposición de fondos, directa o indirectamente, por parte de las primeras a las segundas. A todas luces es insuficiente (por sí sola) la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público. Su artículo 3.2 la convierte casi en papel mojado al establecer que la misma "se aplicará a los documentos elaborados o custodiados por las Administraciones y organismos del sector público, **cuya reutilización sea autorizada por éstos"**. Nada digno de tener en cuenta, pues. Sin olvidar, además, que la restricción a la reutilización que supone la autorización previa por parte de los organismos del sector público no se encuentra recogida en la Directiva 2003/98/CE del Parlamento Europeo y del Consejo de 17 de noviembre de 2003, relativa a la reutilización de la información del sector público, que se ha pretendido transponer mediante la Ley 37/2007.

Tampoco añade apenas nada sustantivo la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los ciudadanos a los Servicios Públicos, pues en ella lo que se reconoce ante todo es el derecho de todos los ciudadanos a relacionarse con las Administraciones por medios electrónicos, pero sin que ello suponga una más generosa regulación del derecho de acceso que contienen las normas que acabo de enumerar. La Ley 30/2007, de 30 de octubre, de Contratos del Sector Público, hace alarde desde sus primeras líneas de sustentarse en el principio de transparencia, pero la regulación que sobre el tema contiene es absolutamente insuficiente: apenas unas referencias genéricas a la transparencia en la

21 Téngase en cuenta el Real Decreto 1401/2007, de 29 de octubre, por el que se regula la composición, funcionamiento y competencias de la Comisión Superior Calificadora de Documentos Administrativos (BOE de 7 de noviembre de 2007), a la que se refiere el artículo 58 de la Ley.

contratación y la previsión de que la misma se hará efectiva mediante el perfil del contratante (artículo 42), y el Registro de Contratos del Sector Público (artículo 308), respecto del cual se establece que "con las limitaciones que imponen las normas sobre protección de datos de carácter personal, facilitará el acceso público a los datos que no tengan el carácter de confidenciales" (art. 308.5).

Peor es la situación en el urbanismo. El Real Decreto Legislativo 2/2008, de 20 de junio, por el que se aprueba el texto refundido de la ley de suelo, es más cicatero aún en la regulación de la transparencia, esencial para la lucha contra la corrupción en el urbanismo. Sólo hay una referencia de pasada en la Exposición de Motivos y en la disposición adicional primera, además de los derechos de acceso a la información y participación que se reconocen a "los ciudadanos" en el artículo 4. Por otra parte, y también relacionado con el mercado inmobiliario, el Real Decreto Legislativo 1/2004, de 5 de marzo, por el que se aprueba el Texto Refundido de la Ley del Catastro Inmobiliario, regula en su Título VI, arts. 50 y ss., el acceso a la información catastral, con notables limitaciones.

En el ámbito de la Administración local la situación no es mejor. Pese al énfasis del artículo 69.1 de la Ley 7/1985, de 2 de abril, reguladora de las Bases de Régimen Local, según el cual "las Corporaciones locales facilitarán la más amplia información sobre su actividad y la participación de todos los ciudadanos en la vida local", lo cierto es que tal precepto al final se traduce en lo siguiente:

- El mismo artículo se apresura a establecer en su apartado 2 que "las formas, medios y procedimientos de participación que las Corporaciones establezcan en ejercicio de su potestad de autoorganización no podrán en ningún caso menoscabar las facultades de decisión que corresponden a los órganos representativos regulados por la Ley".

- El derecho de acceso está en realidad limitado a lo que dispone el artículo 37 de la Ley 30/1992, dado que el artículo 70.3 de la Ley 7/1985 dispone que "todos los ciudadanos tienen derecho a obtener copias y certificaciones acreditativas de los acuerdos de las corporaciones locales y sus antecedentes, así como a consultar los archivos y registros en los términos que disponga la legislación de desarrollo del artículo 105, párrafo b), de la Constitución. La denegación o limitación de este derecho, en todo cuanto afecte a la seguridad y defensa del Estado, la averiguación de los delitos o la intimidad de las personas, deberá verificarse mediante resolución motivada".

Ni siquiera se garantiza plenamente el acceso de los miembros de las corporaciones locales (en particular de los concejales y diputados provinciales) a la totalidad de la información municipal. Por un lado, en la Ley (art. 46.2.b) se prevé que "la documentación íntegra de los asuntos incluidos en el orden del día, que deba servir de base al debate y, en su caso, votación, deberá figurar a disposición de los concejales o diputados, desde el mismo día de la convocatoria, en la Secretaría de la Corporación". Por otro lado, el

artículo 77[22] dispone que "todos los miembros de las corporaciones locales tienen derecho a obtener del alcalde o presidente o de la Comisión de Gobierno cuantos antecedentes, datos o informaciones obren en poder de los servicios de la corporación y resulten precisos para el desarrollo de su función". Pero pese a lo que podría parecer, de ambos preceptos no puede deducirse que se garantice la plena transparencia de las entidades locales ni siquiera respecto de los concejales en el ejercicio de sus funciones. No obstante lo anterior, sí es verdad que el art. 75.7 ha incrementado la transparencia en las entidades locales al exigir la publicación de ciertos datos que pueden afectar a los conflictos de intereses de sus miembros[23].

Llama también la atención el hecho de que en los Estatutos de Autonomía recientemente aprobados apenas hay referencia alguna a la transparencia. Así, el Estatuto catalán tan sólo indica que "La Administración de la Generalitat, de acuerdo con el principio de transparencia, debe hacer pública la información necesaria para que los ciudadanos puedan evaluar su gestión" (apartado 4 del artículo 71, disposiciones generales y principios de organización y funcionamiento –de la Administración de la Generalitat–, del Estatuto, aprobado mediante Ley Orgánica 6/2006, de 19 de julio). Por su parte, el artículo 9º del Estatuto de la Comunidad Valenciana, en la nueva redacción dada por la Ley Orgánica 1/2006, de 10 de abril, establece: "1. Sin perjuicio de lo que dispone la legislación básica del Estado, una Ley de Les Corts regulará el derecho a una buena administración y el acceso a los documentos de las instituciones y administraciones públicas valencianas". No hay en el nuevo Estatuto, sin embargo, alusión alguna a la transparencia.

Tampoco existe entre nosotros una norma de rango adecuado que acierte a regular el alcance y contenido de la publicación de las sentencias de los tribunales. Desgraciadamente, el Tribunal Constitucional ha dejado sentadas unas bases más que discutibles en su sentencia 114/2006, de 5 de abril de 2006.

Para finalizar, incluso el Tribunal Supremo admite la existencia de acuerdos "secretos", no publicados, en virtud de los cuales se aprueban medidas de acceso a los edificios judiciales y demás instalaciones pertenecientes a la Administración de Justicia, como ya sabemos (STS de 29 de enero de 2008). Medidas que se aplican a los ciudadanos sin que éstos sepan en qué consisten. Algo contra lo que ha reaccionado el Tribunal de Justicia de las Comunidades Europeas en relación con las medidas que se han adoptado a nivel europeo para preservar la seguridad en los vuelos (Sentencia de 10 de marzo de 2009, Asunto C-345/06, Gottfried Heinrich*,* antes citada). En Francia acaba de aprobarse el

22 Así, por ejemplo, la Agencia Española de Protección de Datos ha señalado en el Informe Jurídico 0172/2008 que la fotocopia del IBI de un supermercado, cuya propiedad pertenece a otro concejal, no puede facilitarse por impedirlo la legislación tributaria (el Informe puede consultarse en www.agpd.es).

23 Sobre dicho artículo véase el Informe 0212/2008 de la Agencia Española de Protección de Datos (localizable en www.agpd.es).

Decreto núm. 2008-1281 de 8 de diciembre de 2008 relativo a las condiciones de publicación de las instrucciones y circulares, según el cual las dirigidas por los ministros a los servicios y establecimientos del Estado deben ponerse a disposición del público en un sitio Internet del primer ministro. Deberán clasificarse para facilitar su consulta y se entenderá que en tanto no se publiquen no son aplicables. Incluso las ya aprobadas, si no son publicadas, se entenderán derogadas.

En conclusión, pues, resulta ineludible aprobar una ley de transparencia cuanto antes. Instituciones como *Transparency International* o el *Centre for Promotion of Freedom of Expression and Access to Information (Access Info)* han denunciado la ausencia de legislación sobre este tema en España.

3.5 Sobre una futura y necesaria ley de transparencia y acceso a la información

En este escenario, resulta imprescindible reflexionar sobre los posibles contenidos de una futura y necesaria ley de transparencia y acceso a la información pública, que tenga en cuenta los límites que pueden suponer la seguridad y la protección de datos.

A) El escaso debate político y las razones que exigen aprobar una ley de transparencia

Este debate, sin embargo, apenas se ha planteado todavía entre las fuerzas políticas. Debo decir que de modo absolutamente incomprensible; no sólo porque está todavía incompleto el mandato incluido en el artículo 105 de la Constitución, sino porque, como ya he señalado, España es ya uno de los pocos países occidentales que carecen de ley de transparencia o acceso a la información. Sin entrar ahora en las referencias que de una u otra manera y en diversos foros se han hecho por parte de muy diversos representantes políticos a la necesidad de incrementar la transparencia en la vida pública (y en los mercados), me limitaré tan sólo a exponer las propuestas que han presentado formalmente algunos partidos.

El Partido Socialista Obrero Español, en su Programa Electoral para las elecciones de 2008, es el que en principio parece más comprometido con tal iniciativa, pero de un modo sumamente genérico. En efecto señala: “Impulsaremos una Ley sobre el derecho al libre acceso a la información, que garantice que todos los poderes, autoridades públicas y entidades sostenidas con fondos públicos faciliten, en tiempo útil, el libre acceso a toda información o documento oficial, con la única excepción de lo que atente a la legislación de protección de datos o de secretos oficiales. La autoridad requerida deberá motivar, en su caso, su negativa a la información o documentación. La garantía del derecho a la libre información la ejercerá una autoridad independiente elegida por el Congreso de los

Diputados, por mayoría cualificada, con facultades para obligar a las Administraciones Públicas a la entrega inmediata de la información o datos solicitados"[24]. En la Ponencia del 37 Congreso, celebrado en julio de 2008, no se encuentra referencia expresa a la ley de transparencia. Parte, sin embargo, de un principio general de reconocimiento de la importancia de la transparencia en la democracia: "La mejor garantía para que los poderes públicos cumplan su función de protección y promoción de la libertad individual es la conformación democrática y responsable de sus decisiones. La participación ciudadana en los procesos de reflexión y decisión, la transparencia y veracidad en la información, la claridad y amplitud en su divulgación pública y el derecho al acceso a la misma, así como la rendición de cuentas, son factores que garantizan una mejor calidad de las decisiones de las instituciones públicas. Y si esos rasgos democráticos deben impregnar las instituciones, más aún la actuación de los partidos políticos como principales sujetos constitucionales de la acción política en democracia".

Así, en las páginas 1-2 de la Ponencia, además de otras alusiones más genéricas a la transparencia, puede leerse lo siguiente: "La reforma de la Administración debe centrarse, también, en la mejora de la transparencia y de la responsabilidad… Los y las socialistas creemos que hay un derecho y un deber cívico a la buena administración. La ciudadanía tiene derecho a una buena administración, a una acción de gobierno que promueva y respete el interés general y que aporte eficacia, eficiencia, **transparencia**, responsabilidad y rendición de cuentas. Pero ha cambiado muy significativamente la naturaleza de los problemas que la acción de gobierno tiene que enfrentar y los modos de intervención. Ya no es sólo un estado productor y proveedor de servicios. También debe ser un estado catalizador. Catalizador de crecimiento y catalizador de equidad. La economía actual requiere ser regulada –impidiendo además los abusos que el mercado pueda implicar–, pero la regulación debe ser sólo la necesaria y siempre evitando los costes de la hiperregulación. Para las y los socialistas, un instrumento fundamental para conseguir estos objetivos es la transparencia de las Administraciones públicas. La discusión y el diálogo bien informado son esenciales en una democracia, pero para ello necesitamos gobiernos abiertos que aporten información y se sometan al escrutinio público. El único remedio contra el abuso de poder público por personas privadas yace en la esfera pública misma, en la luz con la que muestra cada acto realizado dentro de sus límites, en la visibilidad a la que expone a todos los que se sitúan en ella. De ahí la conexión casi constante de corrupción y opacidad, de abuso y secreto. Todos los estudios recientes sobre calidad de la democracia señalan la transparencia como uno de los indicadores clave. Los beneficios de la transparencia de las Administraciones y la buena información para la democracia son muy numerosos, pues, para empezar, previenen contra el abuso de poder, la discriminación y la corrupción, y para continuar, favorecen discusiones sensatas y racionales mejorando la toma de decisiones públicas. Por ello debemos reforzar la transparencia en la información sobre la actuación de las Administraciones, así como el dere-

24 Pág. 259 del Programa Electoral para las Elecciones 2008.

cho de los ciudadanos a recibirla. En este sentido recomendamos la publicación anual de memorias de sostenibilidad y responsabilidad social de empresas públicas, agencias, hospitales, universidades y Administraciones públicas en general. También somos partidarios de que los altos cargos y cargos electivos de todas las Administraciones presenten declaraciones de bienes y actividades, públicas y privadas, así como de la máxima transparencia sobre ellas".

Por su parte, en su Programa de Gobierno 2008, el Partido Popular señala que "La libertad de elección del ciudadano, la fijación de objetivos, la transparencia y la necesidad de auditorías siguen siendo retos a los que deben responder las Administraciones públicas" (pág. 57 del Programa de Gobierno 2008), y asume el compromiso de crear "una Carta de Transparencia con el Ciudadano que permita a los españoles conocer detalladamente el importe de los impuestos y cotizaciones sociales que aportan anualmente al conjunto de Administraciones y el coste de los principales servicios individualizados que reciben" (pág. 58). En cuanto a la Ponencia Política del 16 Congreso del PP, tan sólo hay una doble referencia a la transparencia en el mercado (puntos 95 y 248), pero ninguna a una posible ley sobre la materia.

Izquierda Unida incluye numerosas referencias a la transparencia en su Programa Electoral para 2008, pero no lleva a cabo propuestas concretas a favor de la aprobación de una ley de transparencia. Se compromete a llevar a cabo una reforma de la Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, en aquellos aspectos que limitan la participación e información de los ciudadanos. Un aspecto fundamental a cambiar es la filosofía restrictiva con que se contempla el concepto de "interesado", figura que otorga la posibilidad de actuar ante las Administraciones Públicas" (Programa Electoral. Elecciones Generales 2008, Apartado 4.1.3). Señala, por ejemplo, su compromiso de "desarrollar medidas para fomentar la transparencia en las Administraciones tributarias y financieras" (pág. 41), o de impulsar el "establecimiento en el ámbito de la UE, de una Carta de los Servicios Públicos, donde se establezca su sujeción al interés general, sus principios caracterizadores (igualdad de acceso, universalidad, continuidad, transparencia, calidad, eficacia económica, ecológica y social, simplificación de procedimientos, participación y control público) y los derechos de los ciudadanos" (pág. 73), así como "avanzar en la transparencia pública de los criterios empleados para la política de subvenciones, adquisición y contrataciones" (pág. 95).

Quizá Ciudadanos es el partido que ha elaborado una propuesta más detallada. Propone la aprobación de una Ley de Acceso a la Información y Transparencia Pública en la que se reconozca el derecho de todos los ciudadanos a acceder a la información en poder de las Administraciones públicas. Las excepciones al acceso serían las derivadas de la seguridad nacional, prevención e investigaciones criminales, derecho a la intimidad, secretos industriales, o los derechos de partes sometidas a un proceso judicial, así como el respeto a la confidencialidad en las deliberaciones previas a la toma de una decisión. Todas ellas, siem-

pre que no exista interés público mayor. El plazo para la respuesta sería de 15 días y se crearía la Agencia Nacional de Acceso a la Información (ANAINFO), como instancia de recurso para los ciudadanos. También se establecería la obligación de las Administraciones de publicar información sobre su regulación y el ejercicio de sus competencias[25].

Por su parte, Convergencia i Unió apoya la aprobación de una Ley que regule el derecho de acceso a la información pública, reconocido a todos los ciudadanos en relación con la información de entidades públicas y privadas que realicen funciones pública[26].

Vemos, pues, que la propuesta expresa de acometer la aprobación de una Ley de Transparencia sólo es asumida en casos contados, aunque sí se aprecia una preocupación generalizada por la importancia de la transparencia y la participación ciudadana. Sin embargo, parece ya llegada la hora de aprobar una ley de transparencia y acceso a la información. No por razones de simple oportunidad, sino por mandato constitucional. Las razones que exigen aprobar esa ley son muy diversas:

- Primero, y ante todo, porque así lo prescribe el artículo 105.b) de la Constitución. que debe ponerse en relación, cuando menos, con los artículos 9.2 y 3, 10, 20 y 23 del propio texto constitucional. En efecto, la transparencia, además de ser en sí un derecho fundamental autónomo (art. 105), es requisito imprescindible para la efectividad del derecho de participación que reconocen los artículos 9 y 23. Lo es también para el ejercicio del derecho a la libertad de expresión y de información (art. 20) y se trata de un derecho fundamental que debe ser interpretado de acuerdo con los tratados y acuerdos internacionales sobre la materia, así como la jurisprudencia de los tribunales que los apliquen (art. 10.2).

Ya sólo la anterior consideración es por sí sola más que suficiente para justificar la imperiosa necesidad de aprobar una ley de transparencia. Pero hay más motivos.

- Segundo, porque la regulación del artículo 37 de la Ley 30/1992 es notoriamente insuficiente y, en mi opinión, inconstitucional por restringir claramente el derecho de acceso.

- Tercero, porque la inexistencia de una ley de transparencia y acceso a la información está produciendo como efecto no deseado que en virtud de la Ley Orgánica de Protección de Datos se esté restringiendo notablemente el acceso a la información pública, por no existir una ley que ampare la cesión de datos en que consiste dicho acceso. En efecto, la puesta a disposición de información a quien la solicite puede suponer una cesión de datos personales prevista y regulada en el artículo 11 de la

25 Fuente, http://www.access-info.org/.
26 Fuente, http://www.access-info.org/.

LOPD. Este precepto requiere que la cesión se ampare con carácter general en el consentimiento de los afectados, si bien permite la comunicación "cuando esté autorizada en una ley". En consecuencia, será necesario que tal ley exista para permitir el acceso, lo cual hoy nos reconduce al repetido artículo 37 de la Ley 30/1992 y en su caso a otras leyes sectoriales que puedan ser de aplicación (por ejemplo el acceso a la información ambiental recogida en la Ley 27/2006, de 18 de julio).

- Cuarto, porque el uso de nuevas tecnologías de la información por parte de las Administraciones públicas hace posible el acopio y tratamiento de una ingente cantidad de información, mucha de ella referida a personas, lo que exige la adopción de medidas legislativas que eviten la opacidad y el oscurantismo.

- Quinto, porque como ya ha quedado suficientemente resaltado, la transparencia es consustancial a un Estado democrático y participativo como el nuestro. Mientras no se apruebe la ley seguiremos teniendo una deuda pendiente con la democracia, que poco a poco nos va diferenciando del resto de países europeos en los que tal ley ya existe. Existe Ley de transparencia y/o autoridad independiente de tutela y garantía del derecho de acceso en numerosos países. En Europa, en los siguientes: Albania, Alemania, Bélgica, Bosnia y Herzegovina, Croacia, Dinamarca, Eslovaquia, Eslovenia, Estonia, Finlandia, Francia, Holanda, Hungría, Irlanda, Islandia, Kosovo, Macedonia, Noruega, Polonia, Portugal, Reino Unido, República Checa, Rumania, Serbia, Suecia, Suiza, así como en Turquía. En este escenario, ¿puede España seguir siendo un país sin ley de transparencia y acceso a la información? Parece, pues, que la ley se impone.

B) Posible contenido de una ley de transparencia y acceso a la información

Blanton (2002b:18) señala que los principios que deben informar la legislación de transparencia deben ser:

a) La información pertenece a los ciudadanos, no a los gobiernos.

b) Las excepciones al principio anterior deben ser muy limitadas y deben estar expresamente previstas en la ley.

c) Las excepciones deben basarse en daños identificables en relación con específicos intereses públicos (no con abstractos intereses generales).

d) Incluso cuando exista un daño identificable, éste debe ser superior al interés público que se atiende mediante la aportación de información.

e) La garantía de la transparencia debe atribuirse a los jueces o a una autoridad independiente.

El Estado tiene competencia para aprobar dicha ley en virtud de los títulos contenidos en el artículo 149.1, apartados 1 y 18, de la Constitución, pues es evidente que hablamos de una materia que afecta a un derecho fundamental y forma parte de las bases del régimen jurídico de las Administraciones públicas, cuya regulación le corresponde en exclusiva al Estado. En cuanto manifestación del derecho a la libertad de expresión e información (art. 20 de la Constitución) y del derecho a la participación en asuntos públicos (art. 23.1) también el Estado ostenta el título competencial que le atribuye el artículo 149.1.1 de la Constitución.

La Ley debería regular al menos los siguientes extremos:

• Objeto

El objeto de la Ley no debe ser sólo el acceso a documentos administrativos entendidos en sentido estricto. No debe tratarse de una ley que tan sólo amplíe o mejore el actual artículo 37 de la Ley 30/1992 en el ámbito del procedimiento administrativo. No es, pues, una ley que única y estrictamente desarrolle el artículo 105.b) de la Constitución. Debe ser una ley de transparencia y acceso a la información pública. No estaría pues, por ejemplo, en línea con las recientes modificaciones legislativas llevadas a cabo en Italia (donde, como ya vimos más atrás, se ha regulado de nuevo en 2005 –leyes números 15 y 80– el derecho de acceso a documentos administrativos en términos muy limitados), sino más cercana a una *Freedom of Information Act*. Por eso debe tratarse de una ley de acceso a la información, en la que es evidente que el concepto de documento ocupa un lugar central, pero entendiendo por tal no el soporte en que se encuentre la información sino su contenido mismo. Sin que obste al ejercicio del derecho el soporte, que puede ser de cualquier tipo.

• Ámbito subjetivo

Debe aplicarse a todas las Administraciones públicas territoriales (Estado, comunidades autónomas y entidades locales), pero también a las entidades de la Administración institucional y corporativa. Y no sólo a ellas, sino, cuando menos, a cualquier entidad que integre el sector público[27]. Además, debería aplicarse a todos los poderes públicos y a los órganos constitucionales.

Sólo si se garantiza el acceso respecto de tales entidades podrá entenderse plenamente reconocido este derecho, que, como vemos, no debe tomar como referencia el de acceso a **documentos administrativos**, sino el derecho a la transparencia en una sociedad democrática.

27 En los términos del artículo 3 de la Ley 30/2007, de Contratos del Sector Público.

• Sujetos legitimados

En línea con el artículo 42 de la Carta de los Derechos Fundamentales de la Unión Europea, podría limitarse la legitimación para el ejercicio del derecho de acceso sólo a los ciudadanos. Planteamiento que, además, sería acorde con los arts. 23.1 y 105.b) de la Constitución (no así con el artículo 20.1.d). En cualquier caso, el concepto de ciudadano está sujeto a debate y no es fácil definirlo con precisión. Por ejemplo, el Anexo de la Ley 11/2007, de acceso electrónico de los ciudadanos a los servicios públicos define ciudadano como "cualesquiera personas físicas, personas jurídicas y entes sin personalidad que se relacionen, o sean susceptibles de relacionarse, con las Administraciones públicas".

La configuración del derecho de acceso a la información como un derecho fundamental aconseja extender la legitimación a cualquier persona. Como ya hemos visto, la propuesta de reforma del Reglamento 1049/2001 va en esta línea, de modo que en el futuro se reconocerá el derecho de acceso a "cualquier persona física o jurídica". Tampoco debe requerirse que el solicitante justifique un interés legítimo que le habilite a ello.

• Excepciones

Es este sin duda el aspecto más importante y más complicado de definir en una ley de transparencia. En lo que interesa al presente documento debe hacerse una especial referencia a la legislación de secretos oficiales y a la de protección de datos. Pero en cualquier caso han de recordarse algunas consideraciones que ya he adelantado previamente y que deben ser tenidas en cuenta:

- El acceso a la información debe ser la regla, que puede estar sujeta a excepciones.

- Las excepciones deben interpretarse y aplicarse de forma estricta.

- La decisión sobre el acceso a la información que contengan datos personales debe tener en cuenta los principios que configuran el derecho a la protección de datos. La decisión debe adoptarse caso a caso, teniendo en cuenta las circunstancias específicas de cada supuesto concreto. El uso que se haga de la información obtenida debe siempre respetar el principio de finalidad. La ley, en efecto, deberá establecer que la información a que se tenga acceso está protegida por lo dispuesto en la legislación de protección de datos.

- También debe señalarse que las excepciones deben estar expresamente previstas en la ley, sin que quepa hacer remisiones a normas reglamentarias que deslegalicen la reserva de ley que deriva de los artículos 105.b), 20 y 23 de la Constitución.

• Procedimiento

Deberá establecerse un procedimiento ágil, sencillo y gratuito en virtud del cual las personas puedan solicitar y obtener el acceso a la información. Para ello deberá establecerse un plazo razonablemente breve para la resolución de la solicitud, plazo que en mi opinión no debería superar el mes. Por supuesto, la resolución denegatoria del acceso deberá ser motivada. Pasado el plazo debería entenderse que se ha desestimado la solicitud (silencio negativo), al objeto de dejar abierta la vía para reclamar ante la Autoridad Independiente de Control.

• Sanciones y responsabilidad

En caso de no contestar a la solicitud o no atender el acceso inicialmente reconocido, podrá exigirse responsabilidad disciplinaria al responsable y, en su caso, podrá imponerse la correspondiente sanción, en los términos que a continuación señalaré.

• Autoridad independiente de supervisión y tutela del derecho.

Por otra parte, uno de los elementos esenciales de un sistema de transparencia o acceso a la información es la existencia de una autoridad pública independiente que garantice o tutele el derecho. Dos son los sistemas posibles:

- La existencia de una autoridad *ad hoc*. Tal es el caso, por ejemplo, de la Comisión de Acceso a los Documentos Administrativos (CADA) en Francia o la Comisión de Acceso a Documentos Administrativos de Portugal.

- La atribución de dicha competencia a la Autoridad de Protección de Datos Personales. Es el caso de Reino Unido (*Information Commissioner's Office)*, Alemania[28] o Hungría, en Europa, o México el (Instituto Federal de Acceso a la Información Pública, IFAI)[29].

Hay que resaltar que la tendencia actual es atribuir las competencias a la Autoridad de Protección de Datos. De hecho, los modelos recientes inglés y alemán, se han mostrado sumamente eficaces.

En mi opinión, esta sería la solución más conveniente para nuestro país. La estrecha relación existente entre transparencia y protección de datos justifica e incluso aconseja que

28 En virtud de la Ley Federal de 5 de septiembre de 2005.

29 El caso del IFAI es diferente, pues sus competencias principales se refieren a la garantía del derecho de acceso a la información, aunque también tiene reconocidas competencias en cuanto a la tutela del derecho a la protección de datos en poder de entidades públicas federales.

sea una misma autoridad la que tutele ambos derechos, aportando así una perspectiva de conjunto que se pierde, sin duda, al atribuir las funciones a entidades distintas[30].

Dicho lo anterior, debe hacerse una matización, referida al sistema de distribución de competencias entre el Estado y las comunidades autónomas. La ley de transparencia podría atribuir la competencia, en el ámbito estatal, a la Agencia Española de Protección de Datos, pero en virtud de las facultades de auto-organización que corresponden a las comunidades autónomas, deben ser éstas las que definan el diseño organizativo que consideren oportuno. Es decir, podría atribuirse la competencia de tutela y control a las Agencias de Protección de Datos (existentes hasta el momento sólo en Madrid, Cataluña y País Vasco), o a otras entidades. En caso de que no se creasen tales entidades o no se atribuyesen las funciones a las Agencias (ni a otro organismo), correspondería al Estado la tutela del derecho de acceso, en términos semejantes a lo que ocurre en la actualidad con la protección de datos, tal como ha confirmado el Tribunal Constitucional en su Sentencia 290/2000, de 30 de noviembre.

Las autoridades de control tendrán como función esencial la de garantizar el derecho de acceso, sin perjuicio, por supuesto, del control posterior de sus decisiones por parte de los tribunales del orden contencioso-administrativo. A tal fin recibirán, tramitarán y resolverán las reclamaciones derivadas de la denegación expresa o presunta del acceso. Tras el correspondiente procedimiento podrán, en su caso, requerir a la entidad pública de que se trate para que atienda el derecho de acceso, pudiendo imponer las sanciones que al efecto se hayan previsto. Para ello la Autoridad debe gozar de una total independencia, y de potestad para imponer sus resoluciones. Podría preverse, como ya ocurre con las Agencias de Protección de Datos, que dé traslado de sus resoluciones al Defensor del Pueblo u órgano autonómico equivalente.

C. Repercusión para el gasto público de la aprobación de una ley de transparencia

No es posible obviar que la aprobación de una ley de transparencia y acceso a la información que quiera cumplir las exigencias que es posible requerir a la regulación de tan importante derecho ha de tener repercusión en el gasto público. Por un lado, porque todos los sujetos públicos obligados deberán implantar procedimientos rápidos y efectivos al objeto de atender a las peticiones de información que se planteen. Por otro, porque debe evaluarse el coste de la creación de una autoridad independiente de tutela o de la reestructuración de la Agencia Española de Protección de Datos, dirigida a asumir tales competencias. Al objeto de tener una idea aproximada del volumen de trabajo que puede representar (sólo en cuanto a posibles reclamaciones presentadas), puede tomarse en consideración el hecho de

30 La autoridad de control (la Agencia) debería, por supuesto, modificar su estructura y régimen jurídico, siempre considerada como una de las llamadas administraciones independientes a las que se refiere la disposición adicional décima de la Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado.

que la Comisión de Acceso a los Archivos Administrativos (CADA) de Francia fue constituida en 1979, año en que atendió unas 500 reclamaciones, mientras que desde 2005 viene atendiendo cada año más de 5.000[31]. Por su parte, el *Information Comissioner's Office* del Reino Unido recibió en el período 2007-2008 un total de 2.646 reclamaciones[32].

Podría pensarse que, en lo que se refiere a los sujetos públicos obligados, la repercusión económica no debería ser notable por cuanto las funciones en materia de acceso a la información podrían ser asignadas a unidades ya existentes, por ejemplo a las de atención a los ciudadanos. Pero una conclusión de este tipo puede tergiversar la realidad. Primero, porque los servicios de atención al ciudadano no siempre cuentan con las competencias necesarias para determinar qué información o documentos pueden facilitarse y cuáles no. Debería, pues, preverse la asignación de la competencia a unidades u órganos con capacidad suficiente de decisión y evaluación de las peticiones, con muy directa relación con los órganos directivos. Segundo, porque es de prever que la puesta en marcha de una ley de transparencia genere en un primer momento un importante número de solicitudes de información del más variado tipo, en un proceso además de incremento constante, lo que podría desbordar totalmente a los órganos o unidades que realicen funciones u ostenten competencias de otro tipo.

En cuanto a la autoridad independiente de control, la situación será muy diferente si se opta por la creación de un nuevo organismo o si se atribuyen las funciones a la Agencia Española de Protección de Datos (o a las autoridades de control existentes en las comunidades autónomas). En el primer caso es evidente que el gasto público se verá afectado mucho más que en el segundo. De hecho, si se opta por una sola autoridad con funciones en materia de protección de datos y transparencia (que es lo que propongo en este documento), la repercusión en términos de incremento del gasto público, para el Estado, no para las comunidades autónomas, será prácticamente nula dado el sistema de financiación de la Agencia de Protección de Datos. Ésta, en efecto, se financia con cargo a los Presupuestos Generales del Estado (artículo 35.4 de la LOPD[33]), integrándose a tales efectos en el Ministerio de Justicia. Pero en realidad no genera apenas gasto alguno al tesoro público, pues la Agencia se financia con cargo a una transferencia presupuestaria del Ministerio de Justicia, pero además, y fundamentalmente, con cargo al remanente de tesorería generado en su mayoría por las sanciones impuestas en el ejercicio de su actividad. Así, el presupuesto de la Agencia para el 2009 es de 15,32 millones de euros, mientras que su remanente supera con creces los 20 millones.

31 Memoria de Actividades de 2007. http://www.cada.fr/fr/rapport/rapport2007.pdf.

32 Datos tomados del Informe 2007-2008, que puede consultarse en la dirección. http://www.ico.gov.uk/upload/documents/library/corporate/detailed_specialist_guides/annual_report2007_08.pdf.

33 Además de otros medios económicos de cuantía casi simbólica, a los que también se refiere el citado artículo.

4. Conclusiones y propuestas

El presente Documento de Trabajo desarrolla una reflexión de futuro acerca de la necesidad de encontrar un equilibrio adecuado entre el derecho a la protección de datos, la transparencia y la garantía de seguridad pública, y, teniendo en cuenta que en España no contamos todavía con una ley de transparencia, ofrece propuestas sobre su posible contenido.

4.1 La protección de datos como derecho fundamental imprescindible en la sociedad contemporánea

Pese a que el derecho a la protección de datos puede considerarse consolidado en España, es imprescindible continuar con la labor de lo que en otras ocasiones he denominado la "normalización de la cultura de la protección de datos".

Varios son los factores que aconsejan no bajar la guardia en el fortalecimiento de la protección de datos. Por un lado, el hecho de que la evolución imparable de las nuevas tecnologías permite recabar información de todo tipo en cualquier lugar y a cualquier hora. El ser humano va dejando constantemente rastros de su actividad y conducta, rastros que son fácilmente detectables y almacenables, lo que permite someter a tratamiento una información de gran valor que se mueve en el marco de una sociedad constantemente vigilada. Por otro lado, los atentados a la privacidad pasan en la mayoría de las ocasiones totalmente desapercibidos, lo que permite la impunidad de los transgresores, y genera en las personas una sensación de despreocupación que en la mayoría de las ocasiones no coincide con la realidad. Stefano Rodota ha hablado de las "microviolaciones" de la protección de datos. Microviolaciones que son en la mayoría de las ocasiones las que perciben las personas, sin darles la importancia que merecen, y que ocultan otras más graves que pasan desapercibidas.

Por ello debe insistirse en la necesidad de considerar el derecho a la protección de datos como pieza clave del sistema democrático. Derecho que además es esencial para el desarrollo efectivo de otros derechos, como el de no discriminación, libertad de residencia y circulación, igualdad, derecho al trabajo, etc., y, en definitiva, para el respeto a la dignidad humana.

4.2 Sobre la necesidad de identificar los verdaderos riesgos para la seguridad y la plena aplicación del derecho a la protección de datos

En el debate entre libertad y seguridad, el respeto a la protección de datos tiene asimismo una importancia que debe ser convenientemente resaltada. No se trata de colocarnos en el dilema que ya apuntó Benjamin Franklin: "El que sacrifica la libertad en aras de la seguridad no merece ninguna de las dos". Se trata de reconocer que la sociedad actual está sometida a amenazas hasta ahora no conocidas, que tienen mucho que ver con el uso de nuevas y sofisticadas tecnologías, y que permiten a muy bajo costo generar riesgos reales para la seguridad ciudadana.

El derecho a la seguridad es un derecho fundamental. Ahora bien, es imprescindible ser conscientes del alcance real de las amenazas que recibe y adoptar las medidas que sean necesarias para combatirlas. Pero siempre con pleno respeto a los derechos fundamentales y, en particular, por lo que ahora nos interesa, a la protección de datos de carácter personal. Ello se debe a que no pocas de las medidas que, sobre todo a partir de los execrables atentados del 11-S, se vienen adoptando no siempre respetan el contenido esencial de los derechos y son claramente desproporcionadas en relación con la situación que se pretende atajar. En este sentido es imprescindible hacer un claro análisis de la situación real, de la necesidad de las medidas que se adopten, de la finalidad perseguida al aprobarlas y adoptarlas y de su proporcionalidad. Respetando siempre, por supuesto, los principios constitucionales y del Estado de derecho.

4.3 Por la urgente aprobación de una ley de transparencia y acceso a la información

Las medidas para garantizar la seguridad y/o para preservar el derecho a la protección de datos de carácter personal pueden hacer que la sociedad tienda a volverse opaca, lo que es contrario a cualquier democracia avanzada. El principio de transparencia, no ya de las Administraciones públicas, sino de la sociedad y los mercados es básico para la democracia. El acceso a la información es un derecho fundamental de todas las personas que requieren una regulación adecuada. Es imprescindible, pues, que se apruebe cuanto antes una ley de transparencia y acceso a la Información que acabe con la insostenible situación que hoy padecemos en España.

Quizá hasta no hace mucho no se ha considerado la urgencia de contar con una norma que por fin desarrolle el mandato del artículo 105.b) de la Constitución, pero es evidente que las Administraciones públicas españolas, y principalmente las entidades locales, están asumiendo un modo de actuar opaco, limitando el derecho de acceso e intentando amparar su

secretismo en la legislación de protección de datos. Ello ha incrementado notablemente los supuestos de corrupción y ha alejado la gestión de lo público de los ciudadanos.

Dicha ley es más necesaria si cabe, dado que en España contamos con un marco normativo muy desarrollado en materia de protección de datos. Por ello es necesario aclarar los supuestos en los que el derecho a la transparencia puede considerarse título habilitante para acceder a información que incluso contenga datos de carácter personal, y definir las excepciones que pueden oponerse frente al ejercicio del derecho de acceso. Excepciones entre las que ha de considerarse sin duda el respeto a la protección de datos. No se trata ni de vaciar de contenido este derecho ni de eclipsar la transparencia. Se trata de encontrar el justo equilibrio entre ambos. Equilibrio que, por definición, no existe si falta una ley de transparencia.

La ley, para cuya aprobación el Estado es competente en virtud de los títulos contenidos en los apartados 1 y 18 del artículo 149.1 de la Constitución, debe determinar los sujetos obligados. Desde luego, ha de alcanzar cuando menos a todas las entidades del sector público, tanto del Estado como de las comunidades autónomas y entidades locales, así como a otros poderes y órganos constitucionales.

Definido el ámbito subjetivo de aplicación, debe establecerse quién ostenta legitimación para ejercer el derecho de acceso. En este sentido, la tónica del Derecho comparado es la de reconocer el derecho a cualquier persona física o jurídica y no exigir la acreditación de interés para ejercitarlo. En cualquier caso, en el uso que se haga de la información obtenida deberá respetarse el principio de finalidad, de acuerdo con lo dispuesto en la legislación de protección de datos.

Contenido medular de la ley de transparencia ha de ser la regulación de las excepciones al acceso, entre las que sin duda ha de incluirse la información amparada por la legislación de protección de datos.

Debe fijarse un procedimiento, rápido, eficaz, sencillo y gratuito para el ejercicio de este derecho. En todos los sujetos obligados deberán establecerse unidades de atención del derecho de acceso y aprobarse protocolos de actuación.

La Ley debe prever la existencia de una autoridad independiente de garantía del derecho. En mi opinión, entre las posibles soluciones, la más acertada sería la de constituir una autoridad independiente con competencias tanto en materia de tutela de la protección de datos, como del derecho a la información. Quizá el modelo del *Information Commissioner's Office* inglés sea el más recomendable. Deberían constituirse tanto una autoridad a nivel del Estado como en las diferentes comunidades autónomas.

En fin, debe establecerse un régimen sancionador que permita hacer realmente efectivo el derecho de acceso previsto en la Ley.

Asimismo, debe valorarse la necesidad de regular (en la norma adecuada para ello, que seguramente no es la ley de transparencia) el modo en que deben hacerse públicas las sentencias de los tribunales, tanto de los ordinarios como del Tribunal Constitucional, al objeto de determinar qué datos personales pueden incorporarse a las versiones públicas de las sentencias.

Bibliografía

Blanton, T. S. (2002a). The World's Right to Know. En Foreign Policy, julio-agosto 2002, págs. 50 y ss.

(2002b), The Openness Revolution. The Rise of a Global Movement for Freedom of Information. en Development dialogue, 2002, nº 1, pág 10.

Bowyer, K.W. (2004) Face recognition technology: security versus privacy. Technology and Society Magazine, IEEE, Primavera de 2004, Volumen 23, páginas 9 y ss.

Brandeis, L.B. (1932), Other Peoples's Money. Puede consultarse en http://library.louisville.edu/law/brandeis/opm-ch5.html.

Castells (2005), La era de la información. Vol. 1, La sociedad red. Alianza Editorial, Madrid, 3ª ed.

Castillo Vázquez (2007), Protección de datos: cuestiones constitucionales y administrativas. El derecho a saber y la obligación de callar. Thomson Civitas-Agencia de Protección de Datos de la Comunidad de Madrid, Cizur Menor.

Clippinger (2007), A Crowd of one. The Future of Individual Identity, Public Affaires, New York.

Colombo (2008), Sulle Regole. Feltrinelli, Milán,

Comisionado para los Derechos Humanos del Consejo de Europa (2008), Perotecting the Right to Privacy in the Fight Against Terrorism. CommDH/Issue Paper (2008) 3, Strasburgo, 4 de diciembre de 2008.

Da Silva Ochoa, J. C. (1993), Derechos de los ciudadanos, con especial referencia a lenguas y acceso a registros. En Pendas García (Coordinador), Administraciones Públicas y ciudadanos (Estudio sistemático de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común), Ed. Praxis, Barcelona.

Embid Irujo, A. (1993a), El derecho de acceso a los archivos y registros administrativos. Algunas reflexiones en las vísperas de su consagración legislativa, en La protección jurídica del ciudadano. Estudios en homenaje al Profesor Jesús González Pérez, Civitas, Madrid, Vol. I, pp. 727 y ss.

(1993b) El derecho de acceso a los archivos y registros administrativos. En Leguina Villa y Sánchez Morón (Directores), La nueva Ley de régimen jurídico de las Administraciones Públicas y del procedimiento administrativo común, Tecnos, Madrid, 1993, pp. 99 y ss.

Etzioni, A. (2004), How Patriotic is the Patriot Act? Freedom versus Security in the Age of Terrorism, Routledge, New York.

Faull, J. (2008), Intimidad y seguridad, en Datospersonales.org. Nº 35 - 30 septiembre 2008.

Fernández Ramos, S. (1997), El derecho de acceso a los documentos administrativos. Pons, Madrid.

Foerstel, H. N. (1999), Freedom of Information and the Right to Know. Greenwood Press, Westport, CT.

Guerrero, J.P. (2005), Transparencia: de la abstracción a la operación de un concepto, en Merino, M. (Coord.) (2005). Transparencia: libros, autores e ideas, IFAI-CIDE, México.

Kinsley, M. (2008), Inherited Properties. The U.S. Congress voted to ban genetic discrimination. But how much equality do Americans Really want? En Time, 19 de mayo de 2008, pág. 60.

Krauthamer, Ch. (2004), Democratic Realism. An American Foreign Policy for a Unipolar World. Conferencia pronunciada el 12 de febrero de 2004 en el American Enterprise Institute for Public Policy Research. Publicada por AEI Press (Washington), 2004. Puede también consultarse en la dirección http://www.aei.org/publications/pubID.19912,filter.all/pub_detail.asp.

Krugman, P. (2008), Después de Bush. El fin de los "neocons" y la era de los demócratas. Ed. Crítica, Barcelona.

Lavilla Rubira, J. J. (1991), La participación pública en el procedimiento de elaboración de los reglamentos en los Estados Unidos de América. Civitas, Madrid.

Lindblom, Ch. (1990), Inquiry and Change: the troubled attempt to understand and shape society. Yale University Press, New Haven.

Maugüe, Ch. (2004), La portée de l'obligation de transparence dans les contrats publics, en VVAA Mouvement du droit public. Du droit administratif au droit constitutionnel. Du droit français aux autres droits. Mélanges en l'honneur de Frank Moderne, Dalloz, Paris.

Merino, M. (Coord.) (2005), Transparencia: libros, autores e ideas. IFAI-CIDE, México.

Mestre Delgado, J. F. (1998), El derecho de acceso a archivos y registros administrativos (Análisis del artículo 105. b) de la Constitución). Civitas, Madrid, 2ª ed.

Moore, G. (1965), Cramming more components onto integrated circuits. Electronics, Volumen 38, Número 8, 19 de Abril de 1965.

Parada Vázquez, R. (1993), Comentarios a la Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. Pons, Madrid.

Piñar Mañas (2003), El derecho a la protección de datos de carácter personal en la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas. En Cuadernos de Derecho Público, nº 19-20, monográfico sobre Protección de datos., págs. 61 y ss.

(2005), El derecho fundamental a la protección de datos personales. Algunos retos de presente y futuro. En Asamblea. Revista Parlamentaria de la Asamblea de Madrid, nº 13, diciembre, págs. 21 y ss.

(2007) Revolución tecnológica, Derecho Administrativo y Administración Pública. Notas provisionales para una reflexión. En VVAA, La autorización Administrativa. La Administración Electrónica. La enseñanza del Derecho Administrativo hoy. Publicaciones de la Asociación Española de Profesores de Derecho Administrativo, Thomson Aranzadi, Cizur Menor, págs. 54 y ss.

(2008 a), El derecho fundamental a la protección de datos personales. Contenido esencial y retos actuales. En torno al nuevo Reglamento de Protección de Datos, Estudio Introductorio, en Piñar Mañas y Canales Gil, Legislación de Protección de Datos. Iustel, Madrid, págs. 90 y ss.

(2008 b) ¿Existe la privacidad? CEU Ediciones, Madrid.

Pomed Sánchez, L. A. (1989), El derecho de acceso de los Ciudadanos a los archivos y registros administrativos. INAP, Madrid.

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

Rodota, S. (2003), Democracia y protección de datos. En Cuadernos de Derecho Público, nº 19-20, monográfico sobre Protección de datos, págs.15 y ss.

(2006) La vita e le regole. Tra diritto e non diritto. Feltrinelli, Milan.

(2008) Innovación, nuevas tecnologías, participación política y protección de datos. Un equilibrio para mejorar la democracia. Conferencia impartida en los Cursos de Verano de la Universidad del País Vasco, en el marco del Seminario El acceso a la Información Parlamentaria, impartida el 28 de julio de 2008. He utilizado el texto original que amablemente me ha facilitado el autor.

Sainz Moreno, F., (2004) Secreto y transparencia. En VVAA Estudios para la reforma de la Administración Pública, INAP, Madrid, págs. 166 y ss.

Sánchez Morón, M. (2008), Derecho Administrativo. Parte General. Tecnos, Madrid, 3ª edición.

Santamaría Pastor, J. A. (1993), De los interesados: derechos y obligaciones. En el libro colectivo Comentarios a la Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, Comunidad de Madrid, Consejería de Hacienda, Madrid.

Solove (2002), Conceptualizing Privacy. En California Law Review, nº 1087, págs. 90 y ss.

(2004), The Digital Person. Technology and Privacy in the Information Age. New York University Press.

Supervisor europeo de protección de datos (2005), Public acces to documents and data protection. Background Paper Series nº 1, Julio 2005.

Sorace, D. (2007), Diritto delle Amministrazioni Publiche. Una introduzione. Il Mulino, 3ª edición, Bologna.

Stanley, J. y Steinhardt, B. (2004), Face-Recognition Technology Threatens Individual Privacy. Opposing Viewpoints: Civil Liberties. Ed. Tamara L. Roleff. San Diego: Greenhaven Press. Ver http://www.enotes.com/civil-liberties-article/41394.

Villanueva Cuevas, A. (1993), El derecho de acceso a archivos y registros. En Revista Jurídica de Castilla-La Mancha, nº 18, monográfico dedicado a Comentarios a la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, pp. 109 y ss.

Weiser, M. (1988), The Computer for the 21st Century. http://www.ubiq.com/hypertext/weiser/SciAm Draft3.html

Westin, A. F. (1967), Privacy and Freedom. Atheneum, New York.

Documentos de trabajo publicados

1/2003. **Servicios de atención a la infancia en España: estimación de la oferta actual y de las necesidades ante el horizonte 2010.** María José González López.

2/2003. **La formación profesional en España. Principales problemas y alternativas de progreso.** Francisco de Asís de Blas Aritio y Antonio Rueda Serón.

3/2003. **La Responsabilidad Social Corporativa y políticas públicas.** Alberto Lafuente Félez, Víctor Viñuales Edo, Ramón Pueyo Viñuales y Jesús Llaría Aparicio.

4/2003. **V Conferencia Ministerial de la OMC y los países en desarrollo.** Gonzalo Fanjul Suárez.

5/2003. **Nuevas orientaciones de política científica y tecnológica.** Alberto Lafuente Félez.

6/2003. **Repensando los servicios públicos en España.** Alberto Infante Campos.

7/2003. **La televisión pública en la era digital.** Alejandro Perales Albert.

8/2003. **El Consejo Audiovisual en España.** Ángel García Castillejo.

9/2003. **Una propuesta alternativa para la Coordinación del Sistema Nacional de Salud español.** Javier Rey del Castillo.

10/2003. **Regulación para la competencia en el sector eléctrico español.** Luis Atienza Serna y Javier de Quinto Romero.

11/2003. **El fracaso escolar en España.** Álvaro Marchesi Ullastres.

12/2003. **Estructura del sistema de Seguridad Social. Convergencia entre regímenes.** José Luis Tortuero Plaza y José Antonio Panizo Robles.

13/2003. **The Spanish Child Gap: Rationales, Diagnoses, and Proposals for Public Intervention.** Fabrizio Bernardi.

13*/2003. **El déficit de natalidad en España: análisis y propuestas para la intervención pública.** Fabrizio Bernardi.

14/2003. **Nuevas fórmulas de gestión en las organizaciones sanitarias.** José Jesús Martín Martín.

15/2003. **Una propuesta de servicios comunitarios de atención a personas mayores.** Sebastián Sarasa Urdiola.

16/2003. **El Ministerio Fiscal. Consideraciones para su reforma.** Olga Fuentes Soriano.

17/2003. **Propuestas para una regulación del trabajo autónomo.** Jesús Cruz Villalón.

18/2003. **El Consejo General del Poder Judicial. Evaluación y propuestas.** Luis López Guerra.

19/2003. **Una propuesta de reforma de las prestaciones por desempleo.** Juan López Gandía.

20/2003. **La Transparencia Presupuestaria. Problemas y Soluciones.** Maurici Lucena Betriu.

21/2003. **Análisis y evaluación del gasto social en España.** Jorge Calero Martínez y Mercè Costa Cuberta.

22/2003. **La pérdida de talentos científicos en España.** Vicente E. Larraga Rodríguez de Vera.

23/2003. **La industria española y el Protocolo de Kioto.** Antonio J. Fernández Segura.

24/2003. **La modernización de los Presupuestos Generales del Estado.** Enrique Martínez Robles, Federico Montero Hita y Juan José Puerta Pascual.

25/2003. **Movilidad y transporte. Opciones políticas para la ciudad.** Carme Miralles-Guasch y Àngel Cebollada i Frontera.

26/2003. **La salud laboral en España: propuestas para avanzar.** Fernando G. Benavides.

27/2003. **El papel del científico en la sociedad moderna.** Pere Puigdomènech Rosell.

28/2003. **Tribunal Constitucional y Poder Judicial.** Pablo Pérez Tremps.

29/2003. **La Audiencia Nacional: una visión crítica.** José María Asencio Mellado.

30/2003. **El control político de las misiones militares en el exterior.** Javier García Fernández.

31/2003. **La sanidad en el nuevo modelo de financiación autonómica.** Jesús Ruiz-Huerta Carbonell y Octavio Granado Martínez.

32/2003. **De una escuela de mínimos a una de óptimos: la exigencia de esfuerzo igual en la Enseñanza Básica.** Julio Carabaña Morales.

33/2003. **La difícil integración de los jóvenes en la edad adulta.** Pau Baizán Muñoz.

34/2003. **Políticas de lucha contra la pobreza y la exclusión social en España: una valoración con EspaSim.** Magda Mercader Prats.

35/2003. **El sector del automóvil en la España de 2010.** José Antonio Bueno Oliveros.

36/2003. **Publicidad e infancia.** Purificación Llaquet, Mª Adela Moyano, María Guerrero, Cecilia de la Cueva, Ignacio de Diego.

37/2003. **Mujer y trabajo.** Carmen Sáez Lara.

38/2003. **La inmigración extracomunitaria en la agricultura española.** Emma Martín Díaz.

39/2003. **Telecomunicaciones I: Situación del Sector y Propuestas para un modelo estable.** José Roberto Ramírez Garrido y Juan Vega Esquerrá.

40/2003. **Telecomunicaciones II: Análisis económico del sector.** José Roberto Ramírez Garrido y Álvaro Escribano Sáez.

41/2003. **Telecomunicaciones III: Regulación e Impulso desde las Administraciones Públicas.** José Roberto Ramírez Garrido y Juan Vega Esquerrá.

42/2004. **La Renta Básica. Para una reforma del sistema fiscal y de protección social.** Luis Sanzo González y Rafael Pinilla Pallejà.

43/2004. **Nuevas formas de gestión. Las fundaciones sanitarias en Galicia.** Marciano Sánchez Bayle y Manuel Martín García.

44/2004. **Protección social de la dependencia en España.** Gregorio Rodríguez Cabrero.

45/2004. **Inmigración y políticas de integración social.** Miguel Pajares Alonso.

46/2004. **TV educativo-cultural en España. Bases para un cambio de modelo.** José Manuel Pérez Tornero.

47/2004. **Presente y futuro del sistema público de pensiones: Análisis y propuestas.** José Antonio Griñán Martínez.

48/2004. **Contratación temporal y costes de despido en España: lecciones para el futuro desde la perspectiva del pasado.** Juan J. Dolado y Juan F. Jimeno.

49/2004. **Propuestas de investigación y desarrollo tecnológico en energías renovables.** Emilio Menéndez Pérez.

50/2004. **Propuestas de racionalización y financiación del gasto público en medicamentos.** Jaume Puig-Junoy y Josep Llop Talaverón.

51/2004. **Los derechos en la globalización y el derecho a la ciudad.** Jordi Borja.

52/2004. **Una propuesta para un comité de Bioética de España.** Marco-Antonio Broggi Trias.

53/2004. **Eficacia del gasto en algunas políticas activas en el mercado laboral español.** César Alonso-Borrego, Alfonso Arellano, Juan J. Dolado y Juan F. Jimeno.

54/2004. **Sistema de defensa de la competencia.** Luis Berenguer Fuster.

55/2004. **Regulación y competencia en el sector del gas natural en España. Balance y propuestas de reforma.** Luis Atienza Serna y Javier de Quinto Romero.

56/2004. **Propuesta de reforma del sistema de control de concentraciones de empresas.** José Mª Jiménez Laiglesia.

57/2004. **Análisis y alternativas para el sector farmacéutico español a partir de la experiencia de los EE UU.** Rosa Rodríguez-Monguió y Enrique C. Seoane Vázquez.

58/2004. **El recurso de amparo constitucional: una propuesta de reforma.** Germán Fernández Farreres.

59/2004. **Políticas de apoyo a la innovación empresarial.** Xavier Torres.

60/2004. **La televisión local entre el limbo regulatorio y la esperanza digital.** Emili Prado.

61/2004. **La universidad española: soltando amarras.** Andreu Mas-Colell.

62/2005. **Los mecanismos de cohesión territorial en España: un análisis y algunas propuestas.** Ángel de la Fuente.

63/2005. **El libro y la industria editorial.** Gloria Gómez-Escalonilla.

64/2005. **El gobierno de los grupos de sociedades.** José Miguel Embid Irujo, Vicente Salas Fumás.

65(I)/2005. **La gestión de la demanda de electricidad Vol. I.** José Ignacio Pérez Arriaga, Luis Jesús Sánchez de Tembleque, Mercedes Pardo.

65(II)/2005. **La gestión de la demanda de electricidad Vol. II (Anexos).** José Ignacio Pérez Arriaga, Luis Jesús Sánchez de Tembleque, Mercedes Pardo.

66/2005. **Responsabilidad patrimonial por daño ambiental: propuestas de reforma legal.** Ángel Manuel Moreno Molina.

67/2005. **La regeneración de barrios desfavorecidos.** María Bruquetas Callejo, Fco. Javier Moreno Fuentes, Andrés Walliser Martínez.

68/2005. **El aborto en la legislación española: una reforma necesaria.** Patricia Laurenzo Copello.

69/2005. **El problema de los incendios forestales en España.** Fernando Estirado Gómez, Pedro Molina Vicente.

70/2005. **Estatuto de laicidad y Acuerdos con la Santa Sede: dos cuestiones a debate.** José M.ª Contreras Mazarío, Óscar Celador Angón.

71/2005. **Posibilidades de regulación de la eutanasia solicitada.** Carmen Tomás-Valiente Lanuza.

72/2005. **Tiempo de trabajo y flexibilidad laboral.** Gregorio Tudela Cambronero, Yolanda Valdeolivas García.

73/2005. **Capital social y gobierno democrático.** Francisco Herreros Vázquez.

74/2005. **Situación actual y perspectivas de desarrollo del mundo rural en España.** Carlos Tió Saralegui.

75/2005. **Reformas para revitalizar el Parlamento español.** Enrique Guerrero Salom.

76/2005. **Rivalidad y competencia en los mercados de energía en España.** Miguel A. Lasheras.

77/2005. **Los partidos políticos como instrumentos de democracia.** Henar Criado Olmos.

78/2005. **Hacia una deslocalización textil responsable.** Isabel Kreisler.

79/2005. **Conciliar las responsabilidades familiares y laborales: políticas y prácticas sociales.** Juan Antonio Fernández Cordón y Constanza Tobío Soler.

80/2005. **La inmigración en España: características y efectos sobre la situación laboral de los trabajadores nativos.** Raquel Carrasco y Carolina Ortega.

81/2005. **Productividad y nuevas formas de organización del trabajo en la sociedad de la información.** Rocío Sánchez Mangas.

82/2006. **La propiedad intelectual en el entorno digital.** Celeste Gay Fuentes.

83/2006. **Desigualdad tras la educación obligatoria: nuevas evidencias.** Jorge Calero.

84/2006. **I+D+i: selección de experiencias con (relativo) éxito.** José Antonio Bueno Oliveros.

85/2006. **La incapacidad laboral en su contexto médico: problemas clínicos y de gestión.** Juan Gervas, Ángel Ruiz Téllez y Mercedes Pérez Fernández.

86/2006. **La universalización de la atención sanitaria. Sistema Nacional de Salud y Seguridad Social.** Francisco Sevilla.

87/2006. **El sistema de servicios sociales español y las necesidades derivadas de la atención a la dependencia.** Pilar Rodríguez Rodríguez.

88/2006. **La desalinización de agua de mar mediante el empleo de energías renovables.** Carlos de la Cruz.

89/2006. **Bases constitucionales de una posible política sanitaria en el Estado autonómico.** Juan José Solozábal Echavarría.

90/2006. **Desigualdades territoriales en el Sistema Nacional de Salud (SNS) de España.** Beatriz González López-Valcárcel y Patricia Barber Pérez.

91/2006. **Agencia de Evaluación: innovación social basada en la evidencia.** Rafael Pinilla Pallejà.

92/2006. **La Situación de la industria cinematográfica española.** José María Álvarez Monzoncillo y Javier López Villanueva.

93/2006. **Intervención médica y buena muerte.** Marc-Antoni Broggi Trias, Clara Llubià Maristany y Jordi Trelis Navarro.

94/2006. **Las prestaciones sociales y la renta familiar.** María Teresa Quílez Félez y José Luis Achurra Aparicio.

95/2006. **Plan integral de apoyo a la música y a la industria discográfica.** Juan C. Calvi.

96/2006. **Justicia de las víctimas y reconciliación en el País Vasco.** Manuel Reyes Mate.

97/2006. **Cuánto saben los ciudadanos de política.** Marta Fraile.

98/2006. **Profesión médica en la encrucijada: hacia un nuevo modelo de gobierno corporativo y de contrato social.** Albert J. Jovell y María D. Navarro.

99/2006. **El papel de la financiación público-privada de los servicios sanitarios.** A. Prieto Orzanco, A. Arbelo López de Letona y E. Mengual García.

100/2006. **La financiación sanitaria autonómica: un problema sin resolver.** Pedro Rey Biel y Javier Rey del Castillo.

101/2006. **Responsabilidad social empresarial en España.** Anuario 2006.

102/2006. **Problemas emergentes en salud laboral: retos y oportunidades.** Fernando G. Benavides y Jordi Delclòs Clanchet.

103/2006. **Sobre el modelo policial español y sus posibles reformas.** Javier Barcelona Llop.

104/2006. **Infraestructuras: más iniciativa privada y mejor sector público.** Ginés de Rus Mendoza.

105/2007. **El teatro en España: decadencia y criterios para su renovación.** Joaquín Vida Arredondo.

106/2007. **Las alternativas al petróleo como combustible para vehículos automóviles.** José Antonio Bueno Oliveros.

107/2007. **Movilidad del factor trabajo en la Unión Europea y coordinación de los sistemas de pensiones.** Jesús Ferreiro Aparicio y Felipe Serrano Pérez.

108/2007. **La reforma de la casación penal.** Jacobo López Barja de Quiroga.

109/2007. **El gobierno electrónico: servicios públicos y participación ciudadana.** Fernando Tricas Lamana.

110/2007. **Sistemas alternativos a la resolución de conflictos (ADR): la mediación en las jurisprudencias civil y penal.** José-Pascual Ortuño Muñoz y Javier Hernández García.

111/2007. **El sector de la salud y la atención a la dependencia.** Antonio Jiménez Lara.

112/2007. **Las revistas culturales y su futuro digital.** M.ª Trinidad García Leiva.

113/2007. **Mercado de vivienda en alquiler en España: más vivienda social y más mercado profesional.** Alejandro Inurrieta Beruete.

114/2007. **La gestión de la demanda de energía en los sectores de la edificación y del trasporte.** José Ignacio Pérez Arriaga, Xavier García Casals, María Mendiluce Villanueva, Pedro Miras Salamanca y Luis Jesús Sánchez de Tembleque.

115/2007. **Aseguramiento de los riesgos profesionales y responsabilidad empresarial.** Manuel Correa Carrasco.

116/2007. **La inversión del minoritario: el capital silencioso.** Juan Manuel Barreiro, José Ramón Martínez, Ángeles Pellón y José Luis de la Peña.

117/2007. **¿Se puede dinamizar el sector servicios? Un análisis del sector y posibles vías de reforma.** Carlos Maravall Rodríguez.

118/2007. **Políticas de creación de empresas y su evaluación.** Roberto Velasco Barroetabeña y María Saiz Santos.

119/2007. **La reforma del acceso a la carrera judicial en España: algunas propuestas.** Alejandro Saiz Arnaiz.

120/2007. **Renta y privación en España desde una perspectiva dinámica.** Rosa Martínez López.

121/2007. **La inversión pública en España: algunas líneas estratégicas.** Rafael Myro Sánchez.

122/2007. **La prensa ante el reto en línea. Entre las limitaciones del modelo tradicional y las incógnitas de su estrategia digital.** Xosé López y Xosé Pereira.

123/2007. Genéricos: medidas para el aumento de su prescripción y uso en el Sistema Nacional de Salud. Antonio Iñesta García.

124/2007. **Laicidad, manifestaciones religiosas e instituciones públicas.** José M.ª Contreras Mazarío y Óscar Celador Angón.

125/2007. **Las cajas de ahorros: retos de futuro.** Ángel Berges Lobera y Alfonso García Mora.

126/2007. **El Informe PISA y los retos de la educación en España.** Olga Salido Cortés.

127/2007. **Propuesta de organización corporativa de la profesión médica.** Juan F. Hernández Yáñez.

128/2008. **Urbanismo, arquitectura y tecnología en la ciudad digital.** José Carlos Arnal Losilla.

129/2008. **La televisión digital terrestre en España. Por un sistema televisivo de futuro acorde con una democracia de calidad.** Enrique Bustamante Ramírez.

130/2008. **La distribución y dispensación de medicamentos en España.** Ricard Meneu.

131/2008. **Nuevos mecanismos de fraude fiscal. Algunas propuestas para un modelo de investigación.** Juan Manuel Vera Priego.

132/2008. **Radio digital en España: incertidumbres tecnológicas y amenazas al pluralismo.** Rosa Franquet Calvet.

133/2008. **Dinámica emprendedora en España.** M.ª Jesús Alonso Nuez, Carmen Galve Górriz, Vicente Salas Fumás y J. Javier Sánchez Asín.

134(I)/2008. **Negociación colectiva, adaptabilidad empresarial y protección de los derechos de los trabajadores vol. I.** Joaquín García Murcia y María Antonia Castro Argüelles.

134(II)/2008. **Negociación colectiva, adaptabilidad empresarial y protección de los derechos de los trabajadores vol. II (Anexos).** Joaquín García Murcia y María Antonia Castro Argüelles.

135/2008. **El sindicalismo en España.** Andrew J. Richards.

136/2008. **La Genómica de plantas: una oportunidad para España.** Pere Arús y Pere Puigdomènech.

137/2008. **Planes y fondos de pensiones: propuestas de reforma.** José Luis Monereo Pérez y Juan Antonio Fernández Bernat.

138/2008. **Modelos de desarrollo de centros hospitalarios: tendencias y propuestas.** Óscar Moracho del Río.

139/2008. **La frontera de la innovación: la hora de la empresa industrial española.** Emilio Huertas Arribas y Carmen García Olaverri.

140/2008. **Propuestas para mejorar la calidad de vida en las ciudades.** María Cifuentes, Rafael Córdoba, Gloria Gómez (coord.), Carlos Hernández Pezzi, Marcos Montes, Raquel Rodríguez, Álvaro Sevilla.

141/2008. **La evolución de la productividad en España y el capital humano.** Rafael Doménech.

142/2008. **Los sindicatos en España frente a los retos de la globalización y del cambio tecnológico.** Holm-Detlev Köhler.

143/2009. **La creación del Sistema Nacional de Dependencia: origen, desarrollo e implicaciones económicas y sociales.** Elisa Díaz, Sara Ladra y Néboa Zozaya.

144/2009. **Biotecnología para una química verde, respetuosa con el medio ambiente.** José Luis García López.

145/2009. **Reinterpretando la rendición de cuentas o *accountability*: diez propuestas para la mejora de la calidad democrática y la eficacia de las políticas públicas en España.** Eduard Jiménez Hernández.

146/2009. **Análisis económico de los efectos de la inmigración en el sistema educativo español.** Javier Salinas Jiménez y Daniel Santín González