Pablo Lucas Murillo de la Cueva

José Luis Piñar Mañas

El derecho a la autodeterminación informativa

FUNDACIÓN COLOQUIO JURÍDICO EUROPEO

MADRID

El derecho a la autodeterminación informativa

Pablo Lucas Murillo de la Cueva

José Luis Piñar Mañas

El derecho a la autodeterminación informativa

FUNDACIÓN COLOQUIO JURÍDICO EUROPEO

MADRID

I.S.B.N.: 978-84-613-3470-4

Depósito Legal: M-30430-2009

Imprime: J. SAN JOSÉ, S.A.

Manuel Tovar, 10

28034 Madrid

ÍNDICE

La construcción del derecho a la autodeterminación informativa y las garantías para su efectividad (*Pablo Lucas Murillo de la Cueva*) 11

1. Aclaración previa 11

2. El reconocimiento del derecho fundamental a la protección de datos de carácter personal 13

3. Las principales características del régimen jurídico de la protección de datos en España 26

4. Los retos pendientes 58

5. Consideraciones finales 70

6. Referencias bibliográficas 77

Protección de datos: Origen, situación actual y retos de futuro *(José Luis Piñar)* 81

I. *De los orígenes a la consideración de la protección de datos como derecho fundamental* 81

1. The *right to be let alone*. *Self Determination* y derecho a la autodeterminación informativa. Protección de datos y mercado interior en la Unión Europea..... 82

2. El derecho a la protección de datos como nuevo derecho, autónomo e independiente del derecho a la intimidad 93

3. El Derecho a la privacidad alcanza también a los dispositivos informáticos que utilizamos..... 98

II. *El contenido del derecho fundamental a la protección de datos de carácter personal* 101

1. Principios configuradores del derecho a la protección de datos: una breve referencia 101

2. En particular, el principio de control independiente 104

3. Protección de datos y otros derechos. En particular, protección de datos y libertad de expresión 109

III. *El derecho a la protección de datos en España. Una evolución legislativa* 119

1. De la LORTAD a la LOPD 119

2. La LOPD y alguna legislación sectorial con incidencia en el derecho a la protección de datos 122

3. La legislación autonómica sobre protección de datos. El marco normativo de la distribución competencial 128

4. El desarrollo reglamentario de la LOPD. En particular el Reglamento aprobado mediante Real Decreto 1720/2007. Motivos que hacían necesaria su aprobación .. 136

IV. *Retos actuales y futuros de la protección de datos* 140

1. Protección de datos y nuevas tecnologías 141

2. Protección de datos y seguridad... 148

3. Protección de datos y transparencia 160

4. Garantía del derecho a la protección de datos y globalización 173

LA CONSTRUCCIÓN DEL DERECHO A LA AUTODETERMINACIÓN INFORMATIVA Y LAS GARANTÍAS PARA SU EFECTIVIDAD

Pablo Lucas MURILLO

SUMARIO: 1. Aclaración previa. 2. El reconocimiento del derecho fundamental a la protección de datos de carácter personal. 3. Las principales características del régimen jurídico de la protección de datos en España. 4. Los retos pendientes. 5. Consideraciones finales. 6. Referencias bibliográficas.

1. *Aclaración previa*

Me parece necesario advertir que he preferido utilizar la expresión "derecho a la autodeterminación informativa" en el título de mi intervención porque siempre me ha parecido más expresiva que otras adoptadas por los legisladores y por la doctrina para denominarlo. En efecto, creo que esa fórmula, que tomo de la Sentencia del Tribunal Constitucional Federal de Alemania de 15 de diciembre de 1983 sobre la Ley del Censo, refleja el aspecto más característico de un derecho nuevo que ha ido cobrando cuerpo bajo distintas formas en los ordenamientos de los Estados democráticos: el control que ofrece a las personas

sobre el uso por terceros de información sobre ellas mismas.

Por eso, he seguido utilizándola, aun siendo consciente de que, ciertamente, el Derecho positivo no la recoge. En efecto, tanto el interno, como el europeo hablan del derecho a la protección de datos de carácter personal. Desde luego, nada más lejos de mi intención que entablar una disputa sobre los nombres cuando está claro que cualquiera de los dos mencionados identifica esta figura y es igualmente evidente que lo importante es el contenido que encierra.

A la exposición de sus elementos más significativos se dirigen estas páginas. No obstante, dada su reciente incorporación a la tabla de derechos fundamentales y la manera en que se ha producido, me ha parecido conveniente recordar, antes, algunos rasgos del proceso que ha llevado al reconocimiento de este derecho fundamental porque ayudan a comprender su verdadero alcance. Sólo entonces tendrá sentido repasar las características más señaladas de su régimen jurídico así como apuntar, después, las principales dificultades a las que se enfrenta.

A la luz de todo ello trataré de llegar a algunas conclusiones.

2. *El reconocimiento del derecho fundamental a la protección de datos de carácter personal*

2.1. El derecho a la protección de datos ha encontrado su más solemne reconocimiento en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea. También en el Tratado por el que se establece una Constitución para Europa, pues incorporó como Parte II la Carta en su integridad, y, además lo erigió en principio de la vida democrática en la Unión (artículo I-51). Y en el Tratado de Lisboa, que, como el anterior, asume la Carta de Niza. Ahora bien, no está escrito en nuestro texto fundamental, ni en el Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales.

En realidad, salvo en el caso de Portugal, ha entrado en el ordenamiento jurídico de la mano del legislador ordinario y de pronunciamientos judiciales y sólo recientemente ha recibido el estatuto de derecho fundamental. En España ese rango se lo ha dado el Tribunal Constitucional en su Sentencia 292/2000, de 30 de noviembre, prácticamente al mismo tiempo que se aprobaba la Carta de los Derechos Fundamentales de la Unión Europea y que el Tribunal Europeo de Derechos Humanos dictaba sus Sentencias más significativas

al respecto (casos Amann contra Suiza y Rotaru contra Rumania), ambas de 2000.

Es un *derecho nuevo*, de los que se dice que integran una de las últimas generaciones de derechos, la tercera o la cuarta, según los autores. Es decir, las formadas por aquellos que responden a los retos y dificultades de la sociedad de nuestros días. Principalmente, a los derivados del avance tecnológico, del impacto sobre el medio y de las nuevas formas de desigualdad. Interesa, por tanto, destacar algunos de los pasos más significativos del proceso que ha llevado a su reconocimiento.

2.2. En el origen de los derechos, mejor dicho, en el de su reconocimiento es posible establecer una gradación de etapas o secuencias en las que juegan factores de distinta naturaleza. Ante todo, los de carácter material. Es decir, los que tienen que ver con una aspiración o necesidad individual cuya satisfacción se convierte en una exigencia tan imperiosa que llega a erigirse en condición indeclinable de la convivencia a partir de un momento dado en función de las relaciones sociales. En segundo lugar, la justificación ideológica de la pretensión de ver satisfecha esa necesidad básica y, en estrecha relación con élla, en tercer lugar, su reivindicación frente al poder público a través de distintas formas de acción y expresión. Por último, su

declaración de manera más o menos solemne pero jurídicamente efectiva.

Esos pasos, perceptibles en la génesis de los derechos de cualquiera de las generaciones de las que se viene hablando, se aprecian también en el caso del derecho a la protección de datos.

El elemento determinante de la necesidad o interés esencial sobre el que se construye es el *progreso tecnológico*, principalmente el derivado de los avances que resultan de la combinación de las virtualidades de la informática y de las telecomunicaciones. Aplicadas a la captación, relación, almacenamiento y comunicación de datos personales crean un escenario en el que es posible que terceros, públicos o privados, reúnan tal caudal de información sobre las personas, cualquier clase de personas, que, prácticamente, no queden aspectos de su vida al margen del conocimiento ajeno, a veces inmediato, incluyendo el de su localización y movimientos en cada momento.

En ese contexto, las barreras de protección que podían brindar el tiempo y el espacio o el mismo volumen de datos disponible ya no son operativas, porque es posible recuperar en tiempo real, desde cualquier lugar con acceso a redes de telecomunicaciones, la que se refiere a uno o varios individuos o grupos de

ellos, aunque se halle dispersa en archivos diferentes y sin que sea obstáculo la dimensión que tengan. Además, a partir de los datos obtenidos, cabe extraer, relacionando unos con otros, ulteriores perfiles personales utilizables para los más diversos fines, lícitos o ilícitos, tanto por los poderes públicos como por agentes privados.

La potencialidad de la tecnología ha llegado a tal punto que permite obtener resultados socialmente provechosos. El problema es que, de igual modo, resulta idónea para causar perjuicios de entidad semejante a los beneficios. Por tanto, como en otros aspectos del progreso, se trata de buscar el modo de aprovechar al máximo las ventajas y conjurar, a la vez, las desventajas. Pues bien, en este contexto, la necesidad básica o interés vital a partir del cual surge la demanda de reconocimiento de un derecho es, precisamente, la de poner en manos de los interesados instrumentos que les permitan recuperar, al menos en parte, el control sobre la información personal que les concierne y que está o puede estar en manos de terceros.

Esa pretensión se justifica a partir de la misma dignidad de la persona y guarda estrecha relación con la libertad que le caracteriza. Libertad individual entendida en su más amplio sentido, incluyendo la faceta de manifes-

tarse o conducirse de acuerdo con la propia forma de ser. O sea, según las ideas, gustos y preferencias de cada uno. La libertad concebida en este sentido como identidad también está en juego porque a los riesgos e inconvenientes que depara el uso incontrolado de información personal ajena, se une la tendencia de quienes se saben observados y controlados a comportarse de la forma que creen menos perjudicial para ellos.

2.3. A partir de estos presupuestos, la construcción del derecho que nos ocupa ha sido fruto también de varios factores. No son otros que los vinculados a una suerte de *diálogo entre la doctrina, los legisladores internacional, comunitario y estatal y la jurisprudencia* en esos tres niveles. Sus interacciones nos han llevado a la actual concepción de este derecho. Así, de las iniciales elaboraciones teóricas que buscaban extender los confines del derecho a la intimidad a toda información personal, se pasó a identificar un bien jurídico autónomo —denominado intimidad informativa, *privacy*, libertad informática o autodeterminación informativa— sólo en parte coincidente con aquélla, al menos en la noción que de la misma o de la vida privada ha prevalecido en los distintos ordenamientos.

Bien jurídico consistente en asegurar a las personas el control de la información —de los datos— que les es propia para ponerles al resguardo o, al menos, permitirles protegerse de los perjuicios derivados del uso por terceros, públicos o privados, de ese material. Las ilimitadas posibilidades que ofrece la tecnología de captar, acopiar, asociar, recuperar en tiempo real y conservar indefinidamente datos personales, así como de obtener ulterior información personal mediante su tratamiento, junto a la necesidad creciente de los mismos en todo tipo de relaciones, han hecho imprescindible garantizar a los individuos instrumentos jurídicos que hagan posible ese control.

Adquiere, así, relevancia una nueva situación jurídica o *status* que se ha venido en llamar de *habeas data*, cualificada activamente por los derechos o facultades que aseguran tal dominio y, pasivamente, por los límites opuestos a quienes desde los poderes públicos o desde la sociedad utilizan información de carácter personal. Derechos y deberes que operan en el marco objetivo ofrecido por los principios de calidad de los datos.

2.4. En España, las primeras reflexiones doctrinales, muy escasas, se producen de forma prácticamente simultánea a la elaboración de la Constitución. No obstante, si el

sentido del apartado cuarto de su artículo 18 fue perfectamente comprendido por algunos constituyentes y, en especial, por Miguel Roca Junyent —que propuso la redacción finalmente aprobada— creo que para la mayoría pesó más, a la hora de aprobarla, la influencia del texto portugués de 1976 y el deseo de incorporar las últimas novedades llegadas al constitucionalismo democrático que el convencimiento de su necesidad por tener una clara percepción de los peligros cuya amenaza pretende conjurar ese precepto. O sea, se trata de una manifestación más del carácter extremadamente derivado de nuestro texto fundamental, rasgo en el que pronto se situó, por cierto, su originalidad.

La entrada en vigor de la Constitución no cambió mucho las cosas. De ahí que, cuando las Cortes Generales abordaron la regulación de la protección civil de los derechos al honor, a la intimidad personal y familiar y a la propia imagen por la Ley Orgánica 1/1982, de 5 de mayo, lo único que dijeran al respecto, en una disposición transitoria, fue que mientras no se aprobase la ley a la que se refería este precepto, se aplicarían las reglas previstas para combatir las intromisiones ilegítimas en el ámbito de aquéllos derechos. Era una solución claramente insuficiente porque los problemas derivados del uso de la informática no se manifiestan del mismo modo que las

intromisiones ilegítimas previstas en esa Ley Orgánica.

En el intervalo que media entre la Constitución y la primera regulación de la protección de datos de carácter personal, ya en 1992, siguió sin existir un auténtico debate sobre la cuestión. Sin embargo, en otros países, se fueron produciendo avances importantes. Bien a propósito de los problemas originados por la aplicación de las leyes existentes en algunos de ellos desde principios de los años setenta del pasado siglo —en *Länder* de Alemania, en Suecia y Francia y en la propia República Federal—, bien por su reivindicación donde no las había, se fue creando un caldo de cultivo que, superando las fronteras, llevó al Consejo de Europa a plasmar en su Convenio nº 108, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, los principios sobre los que descansará el régimen jurídico del derecho, después reconocido como fundamental.

Su proyección a las legislaciones, nacionales y comunitaria, y a la jurisprudencia será determinante para su extensión. No obstante, no fue suficiente para que cuajara en España a pesar de que, aunque todavía tímidamente, se hablaba de su necesidad, se intentaban

algunas iniciativas legislativas y algunas asociaciones y entidades comprometidas con los derechos humanos empezaban a reivindicarlo con mayor fuerza. Y a pesar, igualmente, de que la fórmula abierta y transversal con que se redactó el artículo 18.4 de la Constitución facilitaba la recepción y desarrollo del Convenio nº 108. Sin embargo, transcurrieron los años sin que se diera ese paso. Mientras tanto, el Tribunal Constitucional desconocía los problemas relacionados con la protección de datos de carácter personal y el Tribunal Supremo negaba virtualidad al Convenio para sustentar derechos al considerarlo necesitado de desarrollo, ya que, a su entender, se limitaba a afirmar principios que debían concretar los legisladores nacionales, sus únicos destinatarios.

Cuando, por fin, la *Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de datos de carácter personal* (LORTAD), introdujo la regulación que, con pocas modificaciones, permanece en vigor, se sirvió del contenido del Convenio y de las pautas del proyecto de Directiva europea, entonces en gestación. Ahora bien, si los fundamentos de su regulación —y del derecho al que da cuerpo— se elevaban, en última instancia, a la dignidad humana y se vinculaban a la personalidad individual, fueron motivos más prosaicos los que impulsaron la

aprobación de este texto legal: la puesta en marcha de los Acuerdos de Schengen.

La LORTAD fue sustituida por la *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD)*, actualmente vigente, cuyo Reglamento ha sido recientemente aprobado por el Real Decreto 1720/2007, de 21 de diciembre.

Me parece interesante subrayar que la LORTAD encuadró la disciplina que establecía bajo la idea de "privacidad". Su exposición de motivos concluía así:

> "En este caso, al desarrollar legislativamente el mandato constitucional de limitar el uso de la informática, se está estableciendo un *nuevo y más consistente derecho a la privacidad de las personas* (s.n.)".

Y su artículo 1 decía:

> "La presente Ley Orgánica, en desarrollo de lo previsto en el apartado 4 del art. 18 de la Constitución, tiene por objeto limitar el uso de la informática y otras técnicas y medios de tratamiento automatizado de los datos de carácter personal para garantizar el honor, la intimidad personal y familiar de las personas físicas y el pleno ejercicio de sus derechos".

De este modo, el legislador, mediante ese barbarismo y la reiteración del apartado cuarto del artículo 18 de la Constitución, procuraba mantener una cierta ambigüedad en torno a la trascendencia del paso que estaba dando. Por su parte, la LOPD resolvió el problema prescindiendo de exposición de motivos —a pesar de que las vicisitudes que atravesó su elaboración y los escasos pero significativos cambios que introdujo en el texto hasta entonces vigente la hacían necesaria— y estableciendo en su artículo 1 que su objeto es el siguiente:

> "La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar".

Es importante el cambio de planteamiento que refleja este último precepto. No se sitúa en el marco de la limitación del uso de la informática, ni siquiera en el del artículo 18.4 de la Constitución, como sí hacía la LORTAD, pese a que la nueva Ley Orgánica recoge su contenido en sus propios términos salvo escasas novedades aunque sean llamativas, como ya se ha dicho. La adaptación de la LORTAD a la Directiva 95/46/CE, razón que estuvo en el origen de lo que iba a ser una reforma puntual

de aquélla, no obligaba a dar esos pasos. Desde luego, no mencionar el artículo 18.4 de la Constitución no impide establecer una conexión con él ya reconocida por el legislador de forma rotunda en 1992. Y, si se pensaba que con el texto de 1999 se supera el marco de la limitación del uso de la informática para una normativa que va más allá de tal objetivo, además de que se podía haber dicho sin ninguna dificultad, sucede que ese propósito es igualmente perseguible desde el mismo precepto constitucional que se preocupa de la garantía del pleno ejercicio de los derechos de los ciudadanos, de todos sus derechos. Al fin y al cabo, no cuesta trabajo ver en ese último apartado del artículo 18 la voluntad de protegerlos de los peligros derivados de las tecnologías de la información, ya estrechamente vinculadas, por otra parte, a las de las comunicaciones.

Un año después el Tribunal Constitucional, con sus Sentencias 292 y 290, ambas de 30 de noviembre, a las que se hace referencia más adelante, lo demostraría.

A partir de ese momento, al margen de la aprobación de algunas disposiciones especiales a las que luego se aludirá, el acontecimiento más relevante que se ha producido a nivel normativo ha sido la inclusión de este derecho entre los que algunos de los nuevos Estatutos

de Autonomía han recogido. Así, además de referirse a él, a propósito de la distribución competencial a la protección de datos, lo proclaman, en el momento de escribir estas líneas, los de Cataluña (artículo 31), Andalucía (artículo 32), Islas Baleares (artículo 28), Aragón (artículo 16.3) y Castilla y León (artículo 12 d)).

No es un hecho menor que se haya producido esa incorporación, dada la significación de los estatutos de autonomía. Buena prueba de la trascendencia que tiene la inclusión en él de derechos sustantivos la ofrece el debate político, académico y judicial que se ha producido al respecto, cuya entidad explica las características de las Sentencias del Tribunal Constitucional 247 y 249/2007 y sobre el que se pronunciará, sin duda, nuevamente a propósito del Estatuto de Autonomía de Cataluña. Ahora bien, para el derecho a la autodeterminación informativa tal vez lo único significativo de su recepción estatutaria sea la confirmación que supone de su carácter autónomo. En lo demás, no representa ninguna novedad.

3. *Las principales características del régimen jurídico de la protección de datos en España*

No me propongo adentrarme en una exposición minuciosa de su regulación. No es el momento adecuado para hacerlo. Pero sí me parece importante identificar algunos de sus rasgos más destacados que tienen que ver con la fuerza de los principios y la demanda de especificación de las reglas generales derivada de la enorme variedad de supuestos en los que surge la necesidad de proteger los datos personales.

3.1. Los elementos principales del sistema de protección de datos personales son los que ya encontramos formulados como principios en el Convenio nº 108 del Consejo de Europa. A su vez, las facultades que se confieren a las personas son las que se habían reconocido en la práctica norteamericana de protección frente a los informes de solvencia patrimonial desde los años sesenta del siglo XX.

Este régimen presupone que la disposición por terceros de datos personales solamente es lícita cuando han sido obtenidos con el *consentimiento inequívoco de los afectados, debidamente informados, o con autorización legal explícita*. Consentimiento y autorización que se circunscriben a la utilización de

esa información —exacta, puesta al día y proporcionada— para finalidades lícitas y determinadas. La autodeterminación se quiere garantizar, además, mediante una serie de *derechos regulados en la* LOPD (información, acceso, rectificación, cancelación y oposición). Buscan brindar a los afectados medios para conocer qué información manejan sobre ellos terceros, de donde procede y con qué finalidad la tienen y usan y a quien la transmiten y para qué, así como a obtener su rectificación cuando sean inexactos o su cancelación si no deben ser objeto de tratamiento. Y para oponerse a que sean tratados aquellos que se obtuvieron sin consentimiento o a que se utilicen en su perjuicio perfiles procedentes de tratamientos de esos datos.

Evidentemente, estos derechos y los *principios de protección de datos*, expresados por la LOPD, se erigen en límites impuestos por el legislador al tratamiento de los datos por terceros y van acompañados de normas sancionadoras, penales y administrativas, dirigidas a asegurar su respeto. Los *deberes* que pesan sobre quienes pretendan tratar información personal, contrapartida de los derechos y de las exigencias de los principios, comportan, junto a su estricto respeto, la observancia de formas y procedimientos imprescindibles para hacer efectivas las garantías del derecho a la autodeterminación informativa. Es lo que

sucede con los pasos a dar en la creación de ficheros, con su inscripción o notificación, con la manera de almacenar los datos y las medidas de seguridad que han de establecerse y aplicarse o con el deber de secreto de quienes tratan los datos personales.

Además, se han erigido unos *entes públicos, dotados de una posición de independencia*, con potestades de informe, inspección y sanción, entre otras, que velan por el respeto de todo este conjunto normativo. Tales organismos, en nuestro caso Agencias, cuentan con registros públicos en los que se inscriben los ficheros y tratamientos de datos personales sometidos a su vigilancia.

Por lo demás, el vigente *Reglamento* (Real Decreto 1720/2007) se distingue no sólo porque se ajusta directamente a la LOPD —el anterior se elaboró vigente la LORTAD— y aborda una ejecución global de sus disposiciones sino también porque lo hace mediante preceptos dotados de una gran densidad normativa, en buena medida expresivos de la experiencia generada previamente y de la tarea realizada por la Agencia Española de Protección de Datos. Densidad que, cuando menos, justifica decir que efectúa un verdadero desarrollo de la Ley Orgánica, tal como reconoce el preámbulo del Real Decreto que lo aprueba.

También se van franqueando los obstáculos a la utilización de datos biométricos para distintas finalidades legítimas. Así, además de la digitalización de las huellas dactilares y de la imagen del rostro, a efectos de la expedición del documento nacional de identidad (artículo 9.1 de la Ley Orgánica 1/1992, de 21 de febrero, sobre Protección de la Seguridad Ciudadana, y artículos 5.3 y 11 del Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica) y del pasaporte (artículos 10 de la citada Ley Orgánica 1/1992 y 10 del Real Decreto 896/2003, de 11 de julio, por el que se regula la expedición del pasaporte ordinario y se determinan sus características), se ha previsto legalmente el tratamiento de datos genéticos por la policía para la investigación de los delitos y la identificación de víctimas o de personas desaparecidas (Ley Orgánica 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN).

Asimismo se ha reconocido judicialmente que no es lesivo del derecho a la autodeterminación informativa, por ejemplo, la utilización a efectos de control laboral de un algoritmo elaborado a partir de una imagen parcial de la mano [Sentencia de la Sala Tercera del

Tribunal Supremo de 2 de julio de 2007 (casación 5017/2003)], en el bien entendido que tal uso se hace conforme a las exigencias de los principios de respeto a la finalidad y de seguridad de los datos.

En definitiva, el ordenamiento jurídico dedica a la protección de datos de carácter personal una disciplina general —en la que el Reglamento tiene una gran importancia— cuyo núcleo está bien definido.

Por otra parte, diversos textos legales han *extendido explícitamente los principios de protección de datos a ámbitos específicos*. Así, lo hace el artículo 230.5 de la Ley Orgánica del Poder Judicial, tras su reforma de 1994, y también las normas sobre firma digital (Ley 59/2003, de 19 de diciembre), telecomunicaciones (Ley 32/2003, de 3 de noviembre) o sobre los servicios de la sociedad de la información y el comercio electrónico (Ley 34/2002, de 11 de julio, con su modificación por la Ley 52/2007, de 28 de diciembre, de Impulso de la Sociedad de la Información). Otro tanto ha hecho la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos. También se han establecido algunas reglas especiales en las recientes Leyes orgánicas 4/2007 y 2/2006, sobre Universidades o Educación, respectivamente y en la Ley 30/2007, de

Contratos del Sector Público. Lo mismo hizo la anterior Ley 41/2002, sobre autonomía del paciente.

Ahora bien, las especialidades son pocas y muy concretas y las remisiones a la LOPD no suponen más que explicitar algo que por sí mismo ya resulta del propio imperio de la Constitución y de la LOPD. Esto significa que, en realidad, el régimen jurídico del derecho a la autodeterminación informativa es exclusivamente el que resulta de esa Ley Orgánica y de la interpretación que viene recibiendo. Y la aplicación de normas de carácter general a los problemas que plantean los tratamientos de datos de carácter personal en ámbitos singulares muy definidos no siempre es fácil. Eso ha hecho que se reclamen reglas especiales para sectores concretos de particular importancia. Por ejemplo, el de los datos relativos a la salud, en parte regulado por la Ley 41/2002, o el de los que son objeto de tratamiento por los órganos judiciales o en el marco de las relaciones laborales que tienen lugar en la empresa.

3.2. Según se ha visto, el *Tribunal Constitucional* no se manifestó sobre este derecho hasta relativamente tarde. Y, cuando lo hizo, no todas sus primeras sentencias siguieron la misma línea en lo que se refiere a la identificación del derecho cuyo amparo estaba dis-

pensando. Así, la STC 254/1993, que abre la serie, es consciente de que, tras el artículo 18.4 de la Constitución subyace algo que no es exactamente igual al derecho a la intimidad, pero mantiene la misma línea de relativa ambigüedad que caracteriza la exposición de motivos de la LORTAD y su opción por el término "privacidad" en un intento de eludir la toma de postura en el debate sobre el bien jurídico subyacente.

En la posterior STC 143/1994 deshará esa indefinición y razonará desde el punto de vista del derecho a la intimidad para pronunciarse sobre el régimen del Número de Identificación Fiscal. No obstante, en las SSTC 11, 33, 35, 45, 60, 77, 94, 104, 105, 106, 123, 124, 125, 126, 158, 198, 223 de 1998 y en las SSTC 30, 44, 45 y 202 de 1999, preparará el camino que conduce a las de 30 de noviembre de ese año.

Como dice la Sentencia 202/1999, el previsto por el artículo 18.4 de la Constitución

> "Se trata, por tanto, de un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecaniza-

do de datos (SSTC 254/1993, fundamento jurídico 6º y 11/1998, fundamento jurídico 4º)".

Y añade:

> "la garantía de la intimidad adopta hoy un entendimiento positivo que se traduce en un derecho de control sobre los datos relativos a la propia persona; la llamada «libertad informática» es así el derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención (SSTC 254/1993, fundamento jurídico 7º; 11/1998, fundamento jurídico 4º; 11/1998, fundamento jurídico 4º y 94/1998, fundamento jurídico 4º). 3".

A partir de aquí, *la STC 292/2000*, despeja ya las ambigüedades y establece rotundamente que lo que ya había considerado anteriormente "un instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute de los restantes derechos de los ciudadanos" constituye, también, "un derecho o libertad fundamental". Es, prosigue la sentencia, "lo que se ha dado en llamar «libertad informática», la cual, precisa, posee "una dimensión positiva que excede el ámbito propio del derecho fundamental a la intimidad

(…) y (…) se traduce en un derecho de control sobre los datos relativos a la propia persona".

Seguidamente, habla ya del *derecho fundamental a la protección de datos* y se preocupa de diferenciarlo del derecho a la intimidad, señalando que, si bien comparte con él "el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar", se distingue del mismo porque "atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos cuya concreta regulación debe establecer la Ley". No cualquier Ley, sino aquella que "conforme al art. 18.4 CE debe limitar el uso de la informática, bien desarrollando el derecho fundamental a la protección de datos (art. 81.1 CE), bien regulando su ejercicio (art. 53.1 CE)". Añade que la peculiaridad de este derecho fundamental respecto del derecho a la intimidad radica en la distinta función que cumplen, diferencia que se proyecta sobre su objeto y contenido respectivos.

Nos dice el Tribunal Constitucional que la *función del derecho a la intimidad* es la de protegernos frente a cualquier invasión del ámbito de la vida personal y familiar que deseamos excluir del conocimiento ajeno y de

las intromisiones de terceros en contra de nuestra voluntad, mientras que *el derecho a la protección de datos persigue garantizarnos un poder de control sobre nuestros datos personales*, sobre su uso y destino, a fin de impedir su tráfico ilícito y lesivo para nuestra dignidad y derechos.

Y que, si el derecho a la intimidad permite excluir ciertos datos personales del conocimiento ajeno, "es decir, el poder de resguardar su vida privada de una publicidad no querida", por su parte, el derecho a la protección de datos "garantiza a los individuos un poder de disposición sobre esos datos". De él deriva la prohibición de que los poderes públicos se conviertan en fuentes de esa información sin las debidas garantías, así como el deber de prevenir los riesgos que puedan derivarse del acceso o divulgación indebidas a la misma. Ahora bien, advierte que "ese poder de disposición sobre los propios datos personales nada vale si el afectado desconoce qué datos son los que se poseen por terceros, quiénes los poseen, y con qué fin".

Por tanto, va concluyendo la sentencia, *la singularidad del derecho a la protección de datos* viene, de una parte, de la mayor amplitud de su objeto en comparación con el del derecho a la intimidad, ya que "extiende su garantía no sólo a la intimidad en su dimen-

sión constitucionalmente protegida por el art. 18.1 CE, sino a lo que en ocasiones este Tribunal ha definido en términos más amplios como esfera de los bienes de la personalidad que pertenecen al ámbito de la vida privada, inextricablemente unidos al respeto de la dignidad personal (…), como el derecho al honor, (…) e igualmente, en expresión bien amplia del propio art. 18.4 CE, al pleno ejercicio de los derechos de la persona". De esta manera, el derecho fundamental a la protección de datos "amplía la garantía constitucional a aquellos de esos datos que sean relevantes o tengan incidencia en el ejercicio de cualesquiera derechos de la persona, sean o no derechos constitucionales y sean o no relativos al honor, la ideología, la intimidad personal y familiar o cualquier otro bien constitucionalmente amparado".

La sentencia precisa esta peculiaridad material del derecho examinado aclarando que el *objeto por él protegido no se reduce a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales*. De ahí que alcance también a "aquellos datos personales públicos" ya que, por el hecho de serlo, "por ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado". Su derecho a la

protección de datos lo impide. En realidad, cubre "todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo".

Hay otro rasgo que, para el Tribunal Constitucional, singulariza a este nuevo derecho fundamental frente al derecho a la intimidad personal y familiar del art. 18.1 CE. En efecto, a diferencia de este último, "que confiere a la persona el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima de la persona y la prohibición de hacer uso de lo así conocido, el derecho a la protección de datos atribuye a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio *impone a terceros deberes jurídicos, que no se contienen en el derecho fundamental a la intimidad*, y que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer".

Se trata del derecho del afectado a que se *solicite su previo consentimiento para recoger y usar sus datos personales, del derecho a saber y ser informado sobre el destino y uso de esos datos y de los derechos a acceder, rectificar y cancelar dichos datos*. Es decir, de los instrumentos que hacen posible su poder de disposición sobre sus datos personales.

Ese poder de disposición y de control sobre los datos personales se concreta 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 "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"*. Completan los elementos característicos de la definición constitucional de este derecho fundamental la facultad del afectado de ser informado de quién posee sus datos personales y con qué fin, a la que corresponde el deber del responsable de informarle de qué datos posee sobre su persona y de qué destino han tenido, lo que alcanza también a posibles cesionarios. Todo ello además de rectificar o cancelar los que proceda.

Reconoce el Tribunal Constitucional que estas conclusiones sobre el significado y el contenido el derecho a la protección de datos personales se ven *confirmadas por los instrumentos internacionales* que se refieren a este derecho fundamental a los que ha tenido que acudir en cumplimiento del artículo 10.2 de la Constitución. Se trata de la Resolución 45/95 de la Asamblea General de las Naciones Unidas que recoge la versión revisada de los Principios Rectores aplicables a los Ficheros Computadorizados de Datos Personales. Naturalmente, del Convenio para la Protección de las Personas respecto al Tratamiento Automatizado de Datos de Carácter Personal hecho en Estrasburgo el 28 de enero de 1981 y de la Directiva 95/46, sobre Protección de las Personas Físicas en lo que respecta al Tratamiento de Datos Personales y la Libre Circulación de estos datos. En fin, la Carta de Derechos Fundamentales de la Unión Europea completa esta relación. Subraya la Sentencia que todos estos textos coinciden en el establecimiento de un régimen jurídico para la protección de datos personales basado en la predisposición de un haz de garantías para los afectados, semejante al que ha descrito, que hace posible su respeto.

Sobre los *límites de este derecho fundamental* recuerda que el artículo 105 b) de la Constitución encarga a la ley regular 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" y que, en numerosas ocasiones, el Tribunal Constitucional 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, los cuales encuentran reconocimiento en los artículos. 10.1 y 104.1 de la Constitución. Lo mismo sucede con la distribución equitativa del sostenimiento del gasto público y las actividades de control en materia tributaria (artículo 31) como bienes y finalidades constitucionales legítimas capaces de restringir los derechos del artículo 18.1 y 4 del texto fundamental.

Precisamente, advierte la Sentencia, el Convenio europeo de 1981 también ha tenido en cuenta estas exigencias en su artículo 9. Al igual que el Tribunal Europeo de Derechos Humanos. Este último, al hablar de la garantía de la intimidad individual y familiar, aplicable al tráfico de datos de carácter personal, reconoció que puede tener límites como la seguridad del Estado (caso Leander, 1987), o la persecución de infracciones penales (casos Z, 1997, y Funke, 1993). Y ha exigido que tales limitaciones estén previstas legalmente y sean las indispensables en una sociedad de-

mocrática. Esto significa que la ley que las establezca sea accesible al individuo concernido por ella, que resulten previsibles las consecuencias que para él pueda tener su aplicación y que respondan a una necesidad social imperiosa, además de ser adecuados y proporcionados para el logro de su propósito (caso X e Y, 1985; caso Leander; caso Gaskin, 1989; caso Funke; caso Z).

El resumen anterior muestra que el Tribunal Constitucional ha querido trazar un completo dibujo de este derecho fundamental. No sólo indica su singularidad sobre los otros que reconoce el artículo 18.1 sino que lo diferencia expresamente del derecho a la intimidad y, pese al silencio de la LOPD, sitúa su sede en el apartado cuarto de ese precepto, sin extraer ninguna consecuencia relevante de tal actitud del legislador. Además, expone su contenido y límites y reconoce la virtualidad interpretativa que para precisarlos ofrecen los textos internacionales y comunitarios, incluida la Carta de los Derechos Fundamentales de la Unión Europea.

Desde esas premisas, *resuelve el recurso de inconstitucionalidad del Defensor del Pueblo* y declara inconstitucionales la comunicación de datos entre ficheros de las Administraciones Públicas cuando carezca de consentimiento del afectado o de previsión legal

(artículo 21 LOPD) y, también, las limitaciones del artículo 24.2 al ejercicio de los derechos de acceso, rectificación y cancelación en los ficheros de titularidad pública, así como la previsión del primer apartado de ese mismo artículo que excluía el deber de informar al afectado en la recogida de datos para esos mismos ficheros cuando "impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones públicas» y cuando afecte a la persecución de infracciones administrativas.

Por su parte, la *STC 290/2000*, de la misma fecha que la anterior, confirmó la constitucionalidad de la opción realizada por la LORTAD y mantenida por la LOPD de atribuir la competencia exclusiva sobre los ficheros de titularidad privada a la Agencia Española de Protección de Datos.

Después de estos pronunciamientos, el Tribunal Constitucional no ha vuelto a dictar otros significativos en la materia a excepción del que luego se mencionará sobre la publicación de sus Sentencias y resoluciones.

Visto retrospectivamente, no puede evitarse la impresión de que el supremo intérprete de la Constitución empezó a moverse en la dirección que le condujo a las Sentencias de 30 de noviembre de 2000 a medida que lo

hacían el legislador, la Unión Europea y el Tribunal Europeo de Derechos Humanos. En efecto, es llamativo que la primera Sentencia sobre el derecho a la protección de datos —la STC 254/1993— no se dicte sino pocos meses después de la entrada en vigor de la LORTAD y que la 11/1998 y las que componen la serie que ésta encabeza surjan cuando se discute la transposición de la Directiva 46/95/CEE. En fin, las de 30 de noviembre de 2000, no sólo cuentan ya con el referente de destacadas decisiones del Tribunal de Estrasburgo, sino que aparecen casi a la par que la Carta de los Derechos Fundamentales de la Unión Europea. En cambio, en su día, en 1981, el Convenio nº 108 del Consejo de Europa pasó prácticamente inadvertido.

Estas circunstancias son las que me han llevado a subrayar la importancia del diálogo e interacción a los que aludía antes. Al final, ha sido la confluencia de factores de distinta naturaleza (legislativa, judicial, política) y ámbito (estatal, comunitario, internacional) la que explica la decisión de nuestro Tribunal Constitucional de reconocer un nuevo derecho fundamental a la protección de datos de carácter personal como categoría autónoma y distinta del derecho a la intimidad, sirviéndose, ahora sí, para ello de aportaciones doctrinales anteriores que venían propugnando ese paso.

3.3. No es extraño que la experiencia inicial se haya caracterizado por una *gran ignorancia* de las exigencias que comporta el reconocimiento de este derecho. Ignorancia que no es contradictoria con la relevancia que posee, sino que refleja lo insidioso de las amenazas que quiere conjurar: no se perciben directamente pues están ocultas a los ojos de quienes las padecen. Eso es lo que sucede cuando no se obtiene un crédito, un alquiler o un trabajo a causa de informes sobre la persona del interesado de los que éste no tiene noticia y de los que, por tanto, no puede defenderse.

En esta fase, las Agencias de Protección de Datos han tenido, primero, que constituirse y asentarse allí donde se han creado. Luego, han debido concentrar gran parte de sus esfuerzos en una suerte de pedagogía dirigida a los ciudadanos y a las instituciones, a veces más ajenas que aquellos a la existencia de un régimen jurídico de protección de datos. No son sólo anécdotas que un Alcalde de Madrid se preguntara si la Agencia de Protección de Datos era una agencia de viajes, ni el retraso con el que el Consejo General del Poder Judicial notificó al Registro General de Protección de Datos sus ficheros o la existencia al margen de las previsiones legales de ficheros de diversa naturaleza en distintos órganos jurisdiccionales. O que aparezcan en papele-

ras o contenedores de basura historias clínicas o informes sobre entrevistas de trabajo, por no hablar de los innumerables registros de datos personales en poder de las empresas cuya existencia no ha sido notificada y carecen de todo control.

Es verdad, sin embargo, que la Agencia Española, creada en 1994, y la de la Comunidad de Madrid, constituida en 1997 (Ley 13/1995, de 21 de abril, modificada por la Ley 8/2001, de 13 de julio, de Protección de Datos en la Comunidad de Madrid, y Decreto 67/2003, de 22 de mayo), están realizando un importante esfuerzo para cumplir las funciones que les han encomendado los legisladores. Así, despliegan tareas informativas, incluso, educativas, junto a sus cometidos consultivo, inspector y sancionador. Las Agencias catalana (Ley 5/2002, de 19 de abril, y Decreto 48/2003, de 20 de febrero) y vasca (Ley 2/2004, de 25 de febrero y Decretos 308 y 309/2005, de 18 de octubre) son más recientes y no han tenido tiempo de realizar una labor prolongada aunque desde el primer momento han emprendido su actuación con la misma intensidad que las anteriores. Sin embargo, el trabajo que tienen por delante es inmenso.

3.4. Por su parte, los Tribunales de Justicia confirman, en general, la actuación de estas instituciones especializadas que constituyen una primera línea de defensa para los afectados, e interpretan las normas de la forma más favorable a la efectividad del derecho fundamental.

3.4.1. En efecto, sus decisiones se ven en su mayor parte *confirmadas judicialmente*. Sean las Salas de los Tribunales Superiores de Justicia, sea la Audiencia Nacional o el Tribunal Supremo, en líneas generales, ratifican la legalidad de la actuación de esas instituciones y llevan a cabo una interpretación de la LOPD y demás normas de aplicación a la protección de datos de carácter personal directamente dirigida a restringir el alcance de las previsiones restrictivas de derechos del afectado, a ampliar sus facultades de autodeterminación informativa y a potenciar las reglas objetivas sobre calidad de los datos de carácter personal. Labor a la que contribuyen en sus esferas de actuación el Tribunal Constitucional y los Tribunales de Justicia de las Comunidades Europeas y el de Estrasburgo.

Ha de tenerse en cuenta, igualmente, que junto a las normas e instituciones especialmente establecidas para asegurar el respeto de este derecho fundamental, el conjunto de los mecanismos del Estado de Derecho juega en

su favor. Especialmente, cuando de actuaciones administrativas se trata, ya que deben observar las reglas sobre el procedimiento y respetar los límites que vinculan la actuación de los poderes públicos. Reglas y límites que hacen valer los tribunales.

Así, además de recordar la Sentencia del Tribunal Constitucional 292/2000, cabe señalar la Sentencia de la Sala Tercera del Tribunal Supremo de 28 de marzo de 2007 (recurso 76/2005), que declaró la nulidad de los artículos 323.1 y 2 y 324 del Reglamento del Registro Mercantil (Real Decreto 685/2005) sobre publicidad vía *Internet* de resoluciones judiciales sobre deudores concursados por *falta de dictamen del Consejo de Estado* sobre la redacción finalmente aprobada. O, en el Derecho Comunitario, la Sentencia del Tribunal de Justicia de las Comunidades Europeas de 30 de mayo de 2006, que anuló el Acuerdo entre la Comunidad Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de los datos de los expedientes de los pasajeros por las compañías aéreas al Departamento de Seguridad Nacional porque *el artículo 95 del Tratado constitutivo de la Comunidad Europea no habilitaba a la Comisión* para convenir ese Acuerdo.

Ya en el campo específico de la protección de datos de carácter personal, el Tribunal de

Justicia ha dictado Sentencias relevantes, como la de 6 de noviembre de 2003 (caso Linqvist) o, más recientemente, la de 29 de enero de 2008 (caso Promusicae/Telefónica de España). Ambas tienen en común *proyectar su tutela en el ámbito de Internet*, si bien en relación con problemas diferentes. En efecto, la primera considera tratamiento de datos personales la referencia a ellos en una página *web*. La segunda, en cambio, establece que la defensa de los derechos de propiedad intelectual en los intercambios de archivos P2P no conlleva la obligación de los operadores de las redes de desvelar la identidad de quienes los realizan.

Por su parte, el Tribunal Europeo de Derechos Humanos, en su Sentencia de 3 de abril de 2007 (caso Copland contra el Reino Unido) ha precisado que la navegación por Internet y los archivos temporales que se guardan de los lugares visitados están protegidos por el artículo 8 del Convenio Europeo.

Volviendo al Tribunal Supremo, es importante subrayar que su Sala Tercera circunscribió el concepto de interesado que franquea el *acceso a las resoluciones judiciales* a quienes fueran parte o tuvieran un interés concreto en el litigio [Sentencia de 3 de marzo de 1995 (recurso 1218/1991], abriendo el camino a que se eliminen, de las que se

publican en las bases de datos, las referencias que permiten identificar a las personas afectadas (artículo 266.1 de la Ley Orgánica del Poder Judicial). Camino éste que, sin embargo, no ha seguido el Tribunal Constitucional respecto de sus propias resoluciones (STC 114/2006).

Asimismo, ha negado el *acceso a ficheros judiciales* de litigantes que pretendían hacerse con la información personal de la parte contraria que constaba en ellos y correspondía a otros procesos [STS de 18 de septiembre de 2006 (recurso 274/2002]. Y, en general, ha delimitado el derecho de acceso a los *archivos y registros públicos*, previsto en el artículo 105 b) de la Constitución y regulado en el artículo 37 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, en lo que ahora importa, además de en atención al derecho a la intimidad, en razón de la existencia de un interés legítimo y del respeto al principio de proporcionalidad [STS de 19 de mayo de 2003 (casación 3193/1999)].

También ha negado virtualidad al artículo 39.3 de la Ley 7/1996, de Ordenación del Comercio Minorista, para hacer accesibles los *datos del censo electoral*, cuya prohibición de tratamiento mantiene en tanto la Ley

Orgánica del Régimen Electoral General no disponga otra cosa [STS de 7 de marzo de 2006 (casación 1728/2002), que recoge otras anteriores a partir de la STS de 18 de octubre de 2000].

Asimismo, en extremos estrechamente relacionados con el tratamiento de datos por sujetos privados, la jurisprudencia está siendo especialmente rigurosa.

Es lo que sucede en cuanto a la *exigencia del consentimiento*, que no permite entenderlo concedido por la falta de manifestación del afectado en sentido contrario tras la comunicación de un sujeto privado de que se propone tratar sus datos de no recibir comunicación en contra [STS de 18 de marzo de 2005 (casación 7707/2000)]; y a propósito de la *finalidad determinada*, que excluye la validez de las formuladas en términos genéricos [STS de 11 de abril de 2005 (casación 4209/2001)]. O cuando limita a sus estrictos términos legales el concepto de *fuente accesible al público* [STS de 20 de febrero de 2007 (casación 732/2003)] y exige que los responsables de los ficheros y tratamientos velen por la *calidad de los datos*, depurando los inexactos y no puestos al día [STS de 18 de julio de 2006 (casación 322/2005)].

Lo mismo puede decirse de pronunciamientos sobre el tratamiento por particulares de *datos sensibles* sin pedir el necesario consentimiento, como los relativos a la afiliación política [STS de 25 de enero de 2006 (casación 7396/2001)] o a las creencias [STS de 17 de abril de 2007 (casación 3755/2003)].

En cuanto a la utilización de *datos biométricos*, ya se ha dicho que la Sentencia de la Sala Tercera del Tribunal Supremo de 2 de julio de 2007 (casación 5017/2003) no consideró lesivo de derecho fundamental a la protección de datos un sistema de control laboral basado en la digitalización de una imagen de la mano en los términos de finalidad y seguridad allí contemplados. Tampoco apreció exceso en el recurso a este procedimiento a la vista de los argumentos planteados en el proceso.

Y, en el orden social, la Sentencia de 26 de septiembre de 2007 (unificación de doctrina 966/2006), siguiendo la doctrina del Tribunal Europeo de Derechos Humanos (caso Copland contra el Reino Unido) y, a propósito de la información derivada del seguimiento del uso personal de Internet por los trabajadores desde los ordenadores de la empresa, consideró que ésta no podía efectuarlo sin previa advertencia sobre las condiciones de utilización y

control de los mismos, en la línea de lo establecido por el Garante italiano de la Privacy en su Instrucción de 1 de mayo de 2007 sobre *Lavoro*: *le linee guida del Garante per posta elettronica e internet*.

La Audiencia Nacional y los Tribunales Superiores de Justicia están dictando Sentencias de indudable importancia para la más plena eficacia de este derecho fundamental. Interpretación que supera algunos de los extremos conflictivos del texto legal. Esos pronunciamientos se apoyan en los principios de la protección de datos del artículo 4 para despejar dudas o evitar contradicciones. Veamos.

1) Por ejemplo, en lo relativo a la *utilización de los datos para finalidades no incompatibles con la que justificó su recogida*. La LOPD modificó en este punto la LORTAD de manera que si aquella prohibía su uso para fines distintos de los que motivaron la captación de los datos personales, ahora el alcance de esa prohibición es mucho más reducido: llega solamente a las finalidades incompatibles con la original. Pues bien, la Audiencia Nacional ha dictado varias Sentencias [de 11 de febrero de 2004 (recurso 119/2002) y de 8 de febrero de 2002 (recurso 1067/2000)] en las que sostiene que la nueva redacción, recogida en el artículo 4.2 de la LOPD no puede

tener un sentido distinto de la que ese mismo precepto de la LORTAD imponía.

Razonó la Audiencia Nacional que en castellano la palabra incompatible entraña repugnancia entre dos cosas o términos y que si se pretendiera limitar esta cláusula solamente a los supuestos en que se diera esa contradicción, eso equivaldría a dejarla sin efecto porque en muy pocos supuestos existiría una contradicción de tal naturaleza. Por eso, llegó a la conclusión de que por fines incompatibles había que entender fines distintos, ya que, además, esa solución era la que mejor se ajustaba a los principios de la ley y a la relevancia que atribuye al consentimiento que, interpretando el artículo.6.2, entiende necesario cuando se pretenda usar esos datos para finalidades diferentes de las iniciales.

Línea esta en la que también se encuentran Sentencias de Tribunales Superiores de Justicia, como la de la Sala de lo Contencioso-Administrativo de la Comunidad Valenciana 1901/2002, de 27 de noviembre. O la del de Madrid 90/2003, de 29 de enero.

2) O que el principio de calidad de los datos obliga a quien los trata a velar por su veracidad, exactitud y actualidad, lo que, entre otras cosas, hace ilegítimo el mantenimiento en ficheros de solvencia patrimonial

del *saldo cero* porque no refleja la situación real del afectado, que no tiene ningún saldo deudor [Sentencias de 12 de agosto de 2004 (recurso 599/2002) y, antes, Sentencias de 15 de mayo, de 6 de junio y de 3 de marzo, todas ellas de 2002 (dictadas en los recursos 656 y 711 de 2001 y en el recurso 388/2002, respectivamente)].

3) Ha dicho, igualmente la Audiencia Nacional que la cancelación de la inscripción en uno de estos ficheros de solvencia patrimonial no depende —ni puede depender— del momento en que se contabiliza el pago de la deuda. Así, el *mantenimiento de la condición de moroso con posterioridad a la satisfacción de la obligación* supone incumplir el deber que la LOPD impone a quien trata datos personales de que sean veraces, exactos y de que estén actualizados [Sentencia de 18 de febrero de 2004 (recurso 209/2002)].

4) O convierte en culpable de infracción al responsable del fichero que mantiene *datos erróneos* y los cede a terceros [Sentencias de 16 de junio, 24 de abril, 3 de marzo y 21 de enero, todas ellas de 2004 (recursos 865, 445, 346, de 2002 y 1937/2001)].

5) Igualmente, ha dicho que en las cesiones de datos es el cedente el que debe lograr

el consentimiento del afectado cuando sea preceptivo. No obstante, precisa que esto no exime de *responsabilidad al cesionario* por el incumplimiento de su deber de desplegar una actividad razonable y diligente encaminada a comprobar que aquél lo obtuvo [Sentencias de 30 de junio de 2004 (recurso 619/2002) y de 15 de septiembre de 2001 (recurso 1120/1999)].

6) Otro de los extremos que ha merecido su atención es el que se refiere a la *información en el momento de la recogida de los datos*, respecto de la que ha dicho que ha de ser completa, clara e inequívoca sobre los destinatarios de esos datos y de la finalidad perseguida. La falta de alguno de estos requisitos determina la responsabilidad de quien lo hubiere omitido [Sentencia de 21 de abril de 2004 (recurso 480/2002)].

7) La *carencia de las medidas de seguridad* necesarias llevó a la anulación de la Orden del Ministerio de Sanidad y Consumo de 18 de diciembre de 2000 que creaba un fichero de datos, gestionado por ese departamento, relativos al Sistema de Información sobre Nuevas Infecciones (SINIVIH). La Audiencia Nacional, en Sentencia de 24 de marzo de 2004 (recurso 226/2001), falló en ese sentido tras comprobar que era posible la identificación de los afectados con un alto

grado de evidencia y que también podían producirse confusiones.

8) Respecto de los *ficheros no automatizados* dijo que sus responsables debían cumplir los deberes que la LOPD impone a quienes tratan información personal y afectan a los derechos fundamentales de las personas sin que el plazo de doce años que concedía para que se adaptaran a ella significase que estuvieran exentos de ellos. En concreto, la Audiencia Nacional entendió que la cesión a terceros de datos personales que constaban en uno de estos ficheros sin obtener el consentimiento del afectado era una infracción punible, pues suponía la inobservancia del deber de guardar secreto sobre los datos sensibles [Sentencia de 19 de mayo de 2004 (recurso 754/2002)].

3.4.2. Claro que, al igual que sucede con el Tribunal Constitucional y su antes mencionada Sentencia 114/2006, hay pronunciamientos recientes que parecen encajar mal en esa línea.

Por ejemplo, el de la Sentencia 236/2008, de 9 de mayo, de la Sala Segunda del Tribunal Supremo, para la cual quien utiliza "un programa P2P, en nuestro caso EMULE, asume que muchos de los datos se convierten en públicos para los usuarios de Internet, cir-

cunstancia que conocen o deben conocer los internautas, y tales datos conocidos por la policía, datos públicos en Internet, no se hallaban protegidos por el art. 18-1º ni por el 18-3 C.E.". Posición ésta que suscita dudas desde la perspectiva que ofrece, por ejemplo, la Sentencia del Tribunal Europeo de Derechos Humanos dictada en el caso Copland contra el Reino Unido, que considera contrario al derecho al respeto de la vida privada la captación y almacenamiento de información personal sin conocimiento del afectado de sus correos electrónicos y del uso que hace de Internet.

O la que ha dictado la Sala Tercera el 19 de septiembre de 2008 (casación 6031/2007) que, en contra del criterio de la Agencia Española de Protección de Datos y de la Audiencia Nacional, mantiene que los libros de bautismos parroquiales no son ficheros de datos personales y que no están sujetos a la LOPD. Sentencia a la que acompaña un voto particular discrepante que sostiene que debió plantearse la cuestión prejudicial ante el Tribunal de Justicia de las Comunidades Europeas sobre el alcance de las previsiones de la Directiva 95/46 sobre los conceptos de fichero de datos de carácter personal y de tratamiento al objeto de establecer si comprenden a los libros de bautismos parroquiales.

Seguramente, las circunstancias concretas contempladas en cada uno de los litigios en los que se han producido estos pronunciamientos ofrecen argumentos que explican la posición expresada en las sentencias. En cualquier caso, lo cierto es que no guardan sintonía con una cada vez más larga serie de fallos judiciales que, en distintos niveles —internacionales, europeos, internos— y contextos jurisdiccionales, hacen valer el derecho fundamental a la protección de datos de carácter personal, sea frente a la actuación de los poderes públicos, sea en las relaciones entre particulares.

4. *Los retos pendientes*

4.1. Ahora bien, a propósito de su efectividad nos encontramos con que, sin haber salido todavía de la etapa de desconocimiento del derecho a la autodeterminación informativa, nos estamos adentrando en otra en la que su contenido se ve en parte comprimido en un proceso que parece avanzar con cierta fuerza a impulsos de los cada vez más grandes intereses que se mueven en torno a la utilización de datos personales. Así, *al peligro procedente del poder, se añade el que surge del valor económico de esta información*.

En los debates parlamentarios que llevaron a la aprobación de la LOPD se advierten los

ecos de las presiones de los grupos de interés en las normas sobre el consentimiento, el censo promocional o los ficheros de las aseguradoras. Y algo parecido puede decirse de las llamadas listas de exclusión de envíos publicitarios (artículos 31 de la LOPD y 49 del Reglamento) o de la presunción del consentimiento tácito para tratar datos en todos los casos en que la Ley Orgánica no exija que sea expreso.

En efecto, me parece llamativo que el artículo 15 del Reglamento lo de por prestado siempre que, tras haberle comunicado el responsable del tratamiento que va a tratar sus datos personales, con la información que exigen los artículos 5 de la LOPD y 12.2 del Reglamento, el afectado no manifieste su negativa dentro de los treinta días siguientes a la recepción de la comunicación en cuestión. Teniendo en cuenta que la Ley Orgánica requiere que el consentimiento sea inequívoco (artículo 6.1) me parece difícilmente compatible con ella la solución reglamentaria.

Esta evidente flexibilización puede responder a la idea de que mantener con carácter general una posición estricta o rigurosa sobre la forma de prestar el consentimiento en los casos en que la LOPD no requiere explícitamente que sea expreso no es eficaz debido al todavía amplio desconocimiento que existe en

torno a este derecho y a la dificultad de hacer efectivo su cumplimiento en la práctica. Consideración a la que acompañaría la de que son más eficaces, a la hora de salvaguardar este derecho en las condiciones actuales, las iniciativas encaminadas a asegurar la calidad de los datos y, particularmente, el respeto a la finalidad y al principio de proporcionalidad.

De ser así, hay que reconocer que se trata de un planteamiento respetable aunque, insisto, difícilmente compatible con la regulación legal a la que está sometido el reglamento y en contraste con los criterios que ha ido sentando la jurisprudencia en torno al consentimiento a los que se ha hecho referencia. Criterios que, no debe olvidarse, se apoyan en el carácter inequívoco que la Ley Orgánica ha querido atribuirle para que sea válido. Por lo demás, al margen del juicio que se mantenga sobre su legalidad, parece claro que esta opción reglamentaria, más que un desarrollo que potencie las posibilidades ofrecidas por la LOPD apunta, so pretexto de un realismo pragmático, a su interpretación menos ambiciosa, actitud que contrasta con principios como el de *favor libertatis* que vienen presidiendo la de los derechos fundamentales.

4.2. En otro plano, la difusión de dispositivos que captan la imagen en espacios públicos, en establecimientos comerciales, en cen-

tros de trabajo, zonas comunes de comunidades de propietarios y en otros lugares semejantes, hace posible que quienes controlan esos mecanismos tengan cada vez más información sobre más personas con lo que, potencialmente, se abren nuevos frentes de peligro de difícil control. Se añaden a los instrumentos que están en poder de cualquier persona y permiten hacerse con la imagen y la voz de otros con suma facilidad.

La llamada videovigilancia se está generalizando en todos los ámbitos dándose la circunstancia de que su rápida implantación se está llevando a cabo en la mayor parte de los casos sin observar las normas de la LOPD que, sin duda, son aplicables, ya que la imagen, al igual que el sonido, es un dato personal sometido a su imperio desde el momento en que identifica o permite identificar a aquél a quien pertenece. Y esto ocurre con un medio técnico de enorme capacidad agresiva no sólo para la información personal sino también para la intimidad e, incluso, la propia libertad individual.

Sucede, además, que este acelerado proceso de instalación de dispositivos idóneos para hacerse con la imagen se está haciendo sin que se haya establecido una regulación precisa que adapte a sus peculiaridades las normas generales sobre protección de los derechos

del artículo 18 de la Constitución. En efecto, aparte de la 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, que solamente se ocupa de las cámaras situadas en el exterior para usos policiales, únicamente una Instrucción de la Agencia Española de Protección de Datos, la 1/2006, de 8 de noviembre, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras, ha sentado hasta el momento algunos criterios al respecto.

Son interesantes las consideraciones que hace en su preámbulo. Así, dice que, conforme al principio de proporcionalidad, siempre que resulte posible, deben preferirse otros medios menos agresivos para las personas a fin de prevenir interferencias injustificadas en los derechos y libertades fundamentales. De ahí que sostenga que el uso de cámaras o videocámaras no deba ser el medio inicial para llevar a cabo funciones de vigilancia. Asimismo, desde un punto de vista objetivo, subraya que la utilización de estos sistemas debe ser proporcional al fin perseguido, que en todo caso deberá ser legítimo. E indica que el respeto a ese principio exige evitar abusos como, por ejemplo, sucedería con la instalación de sistemas de vigilancia en espacios comunes o en aseos del lugar de trabajo o de

dispositivos que permitan una observación permanente y omnipresente ya que hace vulnerable a la persona.

Parece claro que estos son criterios razonables que han de respetarse siempre que se pretenda la utilización de estos medios técnicos en espacios interiores como los que se han mencionado antes. No obstante, en lo relativo a la preferencia de otros medios no parece realista pensar, ante la tendencia cada vez más extendida a la instalación de sistemas de videovigilancia en todo tipo de establecimientos, que se vaya a respetar. La apelación a la seguridad es difícil de objetar y no parece exagerado considerar que la preocupación por incrementarla conducirá a un creciente recurso a estos instrumentos técnicos, por otra parte, cada vez más baratos, sencillos y manejables e idóneos para lograr con menos personal una más amplia supervisión y control.

Esto, ciertamente nos afectará a todos pero tendrá una incidencia especial en quienes trabajan en esos establecimientos, ya que estarán permanentemente expuestos a las cámaras o aparatos semejantes. Aquí sí es donde deberá hacerse plenamente efectiva la exigencia de proporcionalidad en la que insiste la Agencia Española de Protección de Datos y donde se deberá velar por el cumplimiento de

todas las garantías de información y salvaguardia de los derechos de los afectados previstas en la LOPD.

Para ello, me parece que sería conveniente sentar normas específicas a través de fuentes apropiadas.

4.3. Naturalmente, *Internet* y, en general, las tecnologías de la información y las telecomunicaciones no sólo potencian la dimensión mercantil de los datos personales, sino que han provocado nuevas preocupaciones relacionadas, unas con la *dimensión universal de las redes*, que dificulta la aplicación de normas circunscritas a ámbitos territoriales limitados. Otras con los mecanismos que permiten seguir la navegación a través de ellas. En fin, están las vinculadas a la *seguridad pública* ante la utilización de estos instrumentos con fines delictivos, como, por ejemplo, las que han dado lugar a la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a comunicaciones electrónicas y redes públicas de comunicaciones, la cual trae causa, a su vez, de la Directiva 2006/24/CE, en cuya elaboración influyeron notablemente los atentados de Londres de julio de 2005.

En este horizonte hay que tener en cuenta que la Ley 11/2007, de acceso electrónico de los ciudadanos a los servicios públicos, prevé

que, a partir del 31 de diciembre de 2009, podremos ejercer nuestro *derecho a relacionarnos electrónicamente con la Administración* (disposición final tercera). Obviamente, la generalización de esa forma de comunicación facilitará el acopio por los poderes públicos de mucha más información personal y su tratamiento. Ese proceso se unirá a los que ya están en marcha en la esfera privada en los campos del *comercio electrónico* y, en general, de los servicios de lo que ha venido en llamarse *sociedad de la información*, en los que los datos personales que se manejan alcanzan cantidades ingentes.

El desarrollo de estos fenómenos comportará cambios cualitativos sin duda, en general, beneficiosos pero también traerá nuevas fuentes de problemas para la garantía del derecho a la autodeterminación informativa, precisamente por el enorme caudal de información personal que circulará, que está circulando ya, en esas relaciones públicas y privadas y la creciente tensión que originan a propósito de ella las demandas de seguridad pública y de beneficio privado.

De este modo, el derecho a la autodeterminación informativa y otros derechos fundamentales se ven enfrentados a retos de gran calado. Desde luego, la protección de los datos de carácter personal se hace más difícil.

No ya porque haya leyes que, sea por razones de seguridad, sea por exigencias del mercado, la restrinjan, sino porque las magnitudes a que ascienden los tratamientos de información personal relativizan extraordinariamente las posibilidades reales de control.

El escenario, mejor dicho, los escenarios que surgen de estas circunstancias no son los más favorables para el derecho que nos ocupa. Parecería, incluso, que, antes de haber tenido la posibilidad de desplegar sus efectos defensivos, estuviera siendo objeto de una progresiva reducción de la mano de los intereses económicos, por un lado, y de las necesidades de la lucha contra la criminalidad organizada, particularmente, contra el terrorismo, del otro. Precisamente, ambas perspectivas hacen acto de presencia en las relaciones de la Unión Europea con los Estados Unidos a propósito de las transferencias de datos personales a ese país, dotado de un menor régimen de protección que el europeo pero que, sin embargo, ha logrado hacer valer sus pretensiones tanto en materia de seguridad como, en general, de circulación de la información personal. Razones de poder político y económico lo explican.

4.4. Las dificultades, por grandes que sean, no deben impedir la aplicación de las normas jurídicas que garantizan un derecho funda-

mental. Al fin y al cabo, vincula a todos los poderes públicos y, además de su vertiente subjetiva, tiene una dimensión objetiva en tanto se integra en el orden de principios y valores sobre el que se asienta la convivencia. El derecho a la autodeterminación informativa, como los demás derechos fundamentales, posee esta doble condición. Tal vez sea la fallida Constitución Europea, me refiero al Tratado por el que se establece una Constitución para Europa, la que mejor lo ha expresado cuando, antes de reconocer el derecho a la protección de datos de carácter personal (artículo II-68), lo proclamaba dentro del Título VI, "De la vida democrática en la Unión" (artículo 1-51), como uno de los elementos que la conforman.

Por tanto, se trata de sacar las consecuencias debidas de esa posición. Consecuencias que llevan a promover la acción de todos los poderes públicos para que, cada uno en su ámbito de actuación, no sólo ajusten su proceder a las exigencias de este derecho, sino que, además, promuevan positivamente su respeto e, incluso, remuevan los obstáculos que dificultan su efectividad.

Está claro que decirlo es más fácil que hacerlo. No obstante, *la tecnología también favorece el ejercicio de la vigilancia y el control sobre los tratamientos de información*

personal. En términos positivos porque permite extender la vigilancia y, negativamente, porque —prohibiendo a los fabricantes y distribuidores la instalación en los aparatos que sirven para acceder y moverse en las redes, de dispositivos que lo hacen posible— se puede impedir o, cuando menos dificultar notablemente seguir la pista a quienes los utilizan.

Al mismo tiempo, en la *sociedad mediática* de nuestros días las decisiones sancionadoras de las autoridades de control —de las Agencias de Protección de Datos— e, incluso, las meramente inspectoras, y las decisiones judiciales que las confirman, pueden alcanzar un eco amplísimo que potencie sus efectos preventivos y contribuya a crear una cultura de defensa de la autodeterminación informativa.

Por lo demás, sea en el ámbito del Consejo de Europa y de las convenciones que ha promovido sobre derechos fundamentales y sobre la protección de datos de carácter personal, sea en el ámbito de la Unión Europea, tenemos instrumentos para *aproximar las legislaciones y la jurisprudencia* surgida de su interpretación de manera que, al menos regionalmente, se construya un espacio amplio de respeto de este derecho. Y, desde luego, el carácter informador de los principios y valores ha de orientar la actuación de

los poderes públicos que tienen confiada la dirección política de los Estados en el sentido de hacer tratados y convenios internacionales que extiendan progresivamente a escala universal los beneficios de este derecho fundamental así como en el de propiciar su respeto tanto en la práctica de las Administraciones que dirigen o en los proyectos normativos que elaboran.

La posibilidad de lograr progresos razonables se ve confirmada a la vista de la *actuación de las Agencias* españolas y de los organismos de control que desempeñan tareas semejantes en otros países y en el ámbito de la Unión Europea. Es la suya una labor, en buena medida, callada pero que, poco a poco, va avanzando en la creación de conciencia en los afectados y de responsabilidad en quienes tratan información personal. Cuantos más medios se pongan a su disposición y a medida que se complete la red territorial todavía apenas iniciada entre nosotros mayor será el rendimiento que lograrán.

Pueden resultar, igualmente, efectos saludables para la protección de los datos de carácter personal, de las *normas y prácticas sobre la competencia*.

La experiencia demuestra que, más a menudo de lo que parece, principios y normas

ideados con otros propósitos revierten en beneficio de los afectados por el uso por terceros de sus datos personales. Ya ha sucedido con los derechos de los trabajadores, con los de los consumidores y usuarios y con la defensa del medio ambiente y ocurre, también, con el mercado y las reglas encaminadas a garantizar su buen funcionamiento: pueden producir el efecto indirecto de contribuir a la efectividad de este derecho fundamental.

Claro está que en este punto es importante no olvidar que la lógica del mercado no es la misma que la de los derechos fundamentales y que, en ocasiones, estos, por motivos ajenos a la funcionalidad económica, pueden exigir restricciones al desenvolvimiento de las relaciones mercantiles. Me parece importante tenerlo presente ante la preocupación creciente por facilitar la circulación de datos personales, objetivo, no lo olvidemos, de la Directiva europea.

5. *Consideraciones finales*

5.1. El proceso que lleva al reconocimiento del derecho a la autodeterminación informativa recuerda al que arranca de los planteamientos de Samuel Warren y Louis Brandeis para enunciar el derecho a la intimidad. La lectura de las páginas de su trabajo "The right to privacy" revela que buscaron en el fondo

del *common law* los medios para combatir las agresiones a la vida privada procedentes de la prensa en las condiciones propias de la sociedad de fines del siglo XIX. Y es de los viejos principios de ese ordenamiento de donde extraen las reglas que definen ese derecho a que nos dejen en paz que preconizaron: *the right to be let alone*. Tal construcción doctrinal acabará fructificando en la jurisprudencia norteamericana y pasará a la legislación federal y estatal a la vez que ha acabado alcanzando estado en los sistemas democráticos.

La búsqueda de protección frente al uso incontrolado de información personal ha seguido unos pasos parecidos. En general, se ha hecho a partir de reflexiones académicas sobre los medios jurídicos que permitirían asegurarla. En España, con la ayuda que ofrece la perspectiva abierta por el artículo 10.2 de la Constitución, ha sido posible construirlo a partir de las previsiones de su artículo 18.4.

El reconocimiento del derecho a la autodeterminación informativa es el caso más claro de afirmación por el Tribunal Constitucional de una nueva figura o variedad de derecho fundamental. No se trata de la expresión del contenido implícito de otro derecho, ni del resultado de la combinación de dos o más ya declarados, sino de su identificación en el

seno de la Constitución y de su construcción con los materiales a los que ésta se abre.

5.2. Este derecho se ha convertido en una categoría transversal. Su carácter instrumental ha hecho que, a la postre, se cumpla el artículo 18.4 en la medida en que se preocupa por garantizar a los ciudadanos el pleno ejercicio de sus derechos, de todos sus derechos y no sólo de los previstos en su apartado primero. En efecto, la protección de los datos personales está redundando en la salvaguardia del derecho al honor, a la intimidad personal y familiar y a la propia imagen. También de la libertad ideológica y del secreto de las comunicaciones, así como del derecho a la salud o al trabajo o al desarrollo de la carrera administrativa. Basta repasar las resoluciones de las Agencias o las sentencias dictadas por los tribunales en asuntos relacionados con la protección de datos para comprobarlo.

5.3. Por lo demás, en la pugna entre las pretensiones de tratamiento de información personal y de su protección, sin perjuicio de la predisposición de ulteriores regulaciones en nuevos sectores cuando sean necesarias, ni del desarrollo de las ya establecidas, los principios han de jugar un papel decisivo. La versatilidad de las amenazas hace que sean especialmente útiles para afrontarlas

por su carácter abierto. Hay que volver la vista, pues, especialmente, al principio de finalidad, estrechamente vinculado al consentimiento y a la habilitación legal, y a las exigencias relacionadas con la calidad de los datos: veracidad, exactitud, proporcionalidad, actualidad, seguridad.

5.4. Es razonable pensar que una más completa regulación del derecho de acceso a los archivos y registros públicos al que se refiere el artículo 105 b) de la Constitución, que supere la que actualmente rige, en tanto precise con más claridad los límites de ese acceso, beneficiará la protección de datos de carácter personal. No obstante, creo que los efectos positivos que esa eventual modificación legislativa pueda comportar para el derecho a la autodeterminación informativa serán limitados porque los principales problemas se sitúan en otros frentes.

5.5. Desde luego, el fomento de códigos tipo y de buenas prácticas es muy importante. Ahora bien, esa relevancia no debe llevar a pensar que en la iniciativa privada se encuentra la solución a los principales problemas de la protección de datos personales. Como en otros derechos, la información, educación y formación facilitan su respeto, pero la experiencia pone de relieve que sin una autoridad dispuesta a aplicar con eficacia las normas y

a sancionar con rigor a quienes las ignoran la efectividad del derecho al que sirven queda esencialmente comprometida.

5.6. No obstante, esto no supone desconocer que solamente se lograrán resultados verdaderamente eficaces si, a partir de un marco jurídico claro y de una actuación firme y decidida de las autoridades públicas encargadas de velar por su observancia, se establece una suerte de cooperación con los sujetos privados que están presentes tanto en la creación y gestión de redes de comunicaciones como en la producción de terminales y *software*.

En este sentido se mueven propuestas como la de Yves Poullet y Jean Marc Dinant, que han hablado al respecto de co-regulación. Una idea que enlaza con la que, desde otros presupuestos, se ha propugnado, por ejemplo, por Colin Bennet, hablando de la gobernanza de la *privacy* o de la autodeterminación informativa entendiendo por tal el resultado de la acción de los poderes públicos y de los propios ciudadanos a través de sus organizaciones y asociaciones y de otras entidades comprometidas con la defensa de los derechos humanos o con los de los consumidores y usuarios.

5.7. La realidad tiende a imponer sus dictados. Frente a ello, es preciso redoblar los esfuerzos a todos los niveles para, con los medios que el ordenamiento jurídico ha puesto a nuestra disposición, luchar por el Derecho. De nuevo, la lucha por el Derecho, y por los derechos, se nos presenta como la forma natural de vivirlos, ya que, precisamente, su reconocimiento presupone su negación y reacciona contra ella. El que descansa en el artículo 18.4 de la Constitución no es una excepción.

REFERENCIAS BIBLIOGRÁFICAS

Colin Bennet, *The Privacy Advocates*, MIT Press, 2008.

Colin Bennet, *The Governance of Privacy,* escrito con Charles Raab. MIT Press, 2006.

Isabel Cecilia del Castillo Vázquez, *Protección de datos: cuestiones constitucionales y administrativas. El derecho a saber y la obligación de callar*. Thomson/Civitas, Madrid, 2007.

Manuel Fernández Salmerón, *La protección de datos personales en las Administraciones Públicas*. Thomson/Civitas, Madrid, 2003.

Emilio Guichot, *Datos personales y Administración Pública*. Thomson/Civitas, Madrid, 2005.

Carlos Lesmes Serrano (coordinador). *La Ley de Protección de Datos. Análisis y comen-*

tario de su jurisprudencia. Lex Nova, Valladolid, 2008.

Pablo Lucas Murillo de la Cueva, *El derecho a la autodeterminación informativa*. Tecnos; Madrid, 1990.

Pablo Lucas Murillo de la Cueva, *Informática y protección de datos*. Centro de Estudios Constitucionales, Madrid, 1993.

Pablo Lucas Murillo de la Cueva, «Las vicisitudes del Derecho de la protección de datos personales», en *Revista Vasca de Administración Pública*, nº 58-II/2000, págs. 211 y sigs.

Pablo Lucas Murillo de la Cueva, "La Constitución y el derecho a la autodeterminación informativa", en *Cuadernos de Derecho Público*, nº 19-20/2003, págs. 27 y sigs.

Ricard Martínez Martínez, U*na aproximación crítica a la autodeterminación informativa*. Thomson/Civitas, Madrid, 2004.

Jesús Alberto Messía de la Cerda Ballesteros, *La cesión o comunicación de datos de carácter personal*. Thomson/Civitas, Madrid, 2003.

Antonio Enrique Pérez Luño, *La tercera generación de derechos humanos*. Aranzadi, Pamplona, 2006.

Yves Poullet, Jean Marie Dinant y María Verónica Pérez-Asinari, *Rapport sur l'application des principes de protection des donnees aux reseaux mondiaux de telecommunications. L'autodétermination informationnelle à l'ère de l'Internet. Eléments de réflexion sur la Convention n° 108 destinés au travail futur du Comité consultatif.*

Rodrigo Tascón López, *El tratamiento por la empresa de los datos personales de los trabajadores. Análisis del estado de la cuestión*. Thomson/Civitas, Madrid, 2005.

Antonio Troncoso Reigada, "Introduction and presentation" en *An aproach to data protection in Europe*. APDCM/Thomson-Civitas, Madrid, 2007, págs. 9-58.

III. Congreso Internet, Derecho y Política (IDP). Nuevas perspectivas. IDP. Revista de Internet, Derecho y Política, nº 5/ 2007. Universitat Oberta de Catalunya. Monográfico coordinado por Agustí Cerrillo, Jordi García y Mónica Vilasau, con contribuciones de Miquel Peguera Poch, Pablo Lucas Murillo de la Cueva, Yves

Poullet, Ricard Martínez, Martínez, Antonio López, Maite Casado Cadalso, Elisenda Bru Cuadrada e Isabel García Noguera.

PROTECCIÓN DE DATOS: ORIGEN, SITUACIÓN ACTUAL Y RETOS DE FUTURO

José Luis PIÑAR

Sumario: I.- De los orígenes a la consideración de la protección de datos como derecho fundamental. 1.- The *right to be let alone*. *Self Determination* y derecho a la autodeterminación informativa. Protección de datos y mercado interior en la Unión Europea. 2.- El derecho a la protección de datos como nuevo derecho, autónomo e independiente del derecho a la intimidad. 3.- El Derecho a la privacidad alcanza también a los dispositivos informáticos que utilizamos. II.- El contenido del derecho fundamental a la protección de datos de carácter personal. 1.- Principios configuradores del derecho a la protección de datos: una breve referencia. 2.- En particular, el principio de control independiente. 3.- Protección de datos y otros derechos. En particular, protección de datos y libertad de expresión. III.- El derecho a la protección de datos en España. Una evolución legislativa. 1.- De la LORTAD a la LOPD. 2.- La LOPD y alguna legislación sectorial con incidencia en el derecho a la protección de datos. 3.- La legislación autonómica sobre protección de datos. El marco normativo de la distribución competencial. 4.- El desarrollo reglamentario de la LOPD. En particular el Reglamento aprobado mediante Real Decreto 1720/2007. Motivos que hacían necesaria su aprobación IV.- Retos actuales y futuros de la protección de datos. 1.- Protección de datos y nuevas tecnologías. 2.- Protección de datos y seguridad. 3.- Protección de datos y transparencia. 4.- Garantía del derecho a la protección de datos y globalización.

I. *De los orígenes a la consideración de la protección de datos como derecho fundamental*

1.- The *right to be let alone*. *Self Determination* y derecho a la autodeterminación informativa. Protección de datos y mercado interior en la Unión Europea.

Como ya he tenido ocasión de señalar en otras ocasiones[1], el derecho a la protección de datos surge como tal, seguramente, en la década de los sesenta del pasado siglo. No obstante, no es posible olvidar las espectaculares construcciones doctrinales anteriores, entre las que destaca sin duda alguna Thomas Cooley que en 1888 habló ya de «the right to be let alone»[2] y el tantas veces citado (que no

---

[1] A ello me he referido ya en «ECJ Case-Law on the Right to Protection of Personal Data», *BNA International. World Data Protection Report*. Parte 1 y Parte 2, enero y febrero de 2006, respectivamente. También en «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. 45 y ss.; *¿Existe la Privacidad?*, Ediciones CEU, Madrid, 2008. Alguna de las reflexiones que expongo a continuación están asimismo tomadas de mi artículo «La mirada europea», en la Revista *Nexos*, México, Vol XXIX, núm. 353, mayo 2007, págs. 29 y ss.

[2] *A Treatise on the Law of Torts or the Wrongs which arise independent of contract*, Callaghan 2ª ed., Chicago, 1888, p. 29.

siempre leído) artículo de Warren y Brandeis «The Right to Privacy», publicado en la *Harvard Law Review*[3]. «Los cambios políticos, sociales y económicos –expusieron entonces– traen consigo el reconocimiento de nuevos derechos, y el *common law*, en su eterna juventud, acierta a satisfacer las nuevas demandas de la sociedad». El derecho a la vida ha pasado a significar derecho a disfrutar de la vida, que incluye el derecho a que te dejen estar solo. El derecho debe preservarnos frente a las invasiones de los «sagrados límites de nuestra vida privada y doméstica». El derecho a la privacidad supone, pues, el derecho a poder estar solo, con el alcance que cada uno desee, incluso completamente solo, sin sufrir ingerencias no deseadas y sin interferir en el derecho de los demás[4]. Tal concepto, aunque todavía digno de ser tenido muy en cuenta, ha sido desde luego superado[5]. En

---

[3] *Harvard Law Review*, Vol. IV, 15 de diciembre de 1890, núm. 5. Ha sido reeditado por la Oficina del *Garante per la Protezione dei dati personal,* Edición bilingüe, anglo-italiana, Roma-Verona, 2005.

[4] Ver Amitai Etzioni, *The limits of Privacy*, Basic Books, New York, 1999, pág. 190.

[5] Véase Stefano Rodota, *La vita e le regole. Tra diritto e non diritto*, Feltrinelli, Milán, 2006, pág. 100. William Prosser es incluso muy crítico con el artículo de Warren y Brandeis: «Privacy (A legal Análisis)», *California Law Review*, nº 48, 1960, pág. 338. El trabajo de Prosser puede asimismo consultarse en Schoeman, *Philosophical Dimensions of Privacy: an Anthology*,

este sentido, las aportaciones de Westin son sin duda de capital importancia[6]. A él se debe precisamente la definición de privacidad en términos de autodeterminación, de «*self determination*»[7], concepto éste que más tarde fue expresamente asumido por el Tribunal Constitucional Federal Alemán en su conocida sentencia de 15 de diciembre de 1983 sobre el Censo, y que también ha sido utilizado por nuestro Tribunal Constitucional[8], como más adelante veremos.

Pero lo cierto es que hasta la segunda mitad de los años sesenta del pasado siglo no se ponen las bases del derecho a la protección de datos tal como hoy lo entendemos. En efecto,

---

Cambridge University Press, 1984 (reedición de 2007), págs. 104 y ss. A todo ello me he referido en *¿Existe la Privacidad?*, op. cit., pág. 7.

[6] Alan F. Westin, *Privacy and Freedom*, Atheneum, New York, 1967. Hay edición de 1970.

[7] Como ha recordado Jan Holvast, «History of privacy», en Karl De Leeuw y Jan Bergstra (eds.), *The History of Information Security. A Comprehensive Handbook*, Elsevier, Amsterdam, 2007, págs. 737 y ss.

[8] Sobre el concepto, vid., por todos, Pablo Lucas Murillo de la Cueva, *El derecho a la autodeterminación informativa*, Tecnos, Madrid, 1990 y, más recientemente, «La Constitución y el derecho a la autodeterminación informativa», en *Cuadernos de Derecho Público*, nº 19-20 (2003), monográfico sobre *Protección de Datos*, págs. 27 y ss. También Ricard Martínez, *Una aproximación crítica a la autodeterminación informativa*, Civitas, Madrid, 2004.

en 1967 se constituyó en el seno del Consejo de Europa una Comisión Consultiva para estudiar las tecnologías de la información y su potencial agresividad hacia los Derechos de las personas, especialmente en relación con su Derecho a no sufrir ingerencias en la vida privada (Derecho éste que se había ya recogido en la Declaración Universal de Derechos Humanos[9] o el Pacto Internacional de Derechos Civiles y Políticos de 1966[10]), y de ella surgió la Resolución 509 de la Asamblea del Consejo Europa sobre *«los Derechos humanos y los nuevos logros científicos y técnicos»*, que se considera el origen del movimiento legislativo que desde entonces recorrerá Europa en materia de protección de datos.

Es lugar común citar la conocida Ley del Land de Hesse, en Alemania, pionera en la

---

[9] El artículo 12 dispone: «Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene Derecho a la protección de la ley contra tales injerencias o ataques».

[10] En términos prácticamente iguales, el art. 17 del Pacto dispone:

«1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación.

2. Toda persona tiene Derecho a la protección de la ley contra esas injerencias o esos ataques».

materia, así como la propia Ley Federal alemana de 1977. Pero no debe olvidarse que ya en 1973 el Departamento de Salud, Educación y Bienestar de Estados Unidos elaboró un Informe sobre las bases de datos telemáticas del Gobierno[11] y propuso un Código de buenas prácticas que recogería los principios que habrían de regir el uso de información por parte del Gobierno (*Fair Information Practices* o *Fair Information Principles*): no deben existir bases de datos secretas, se ha de reconocer el derecho de acceso y rectificación de los datos personales, ha de respetarse el principio de finalidad, debe respetarse el principio de calidad y han de adoptarse medidas de seguridad. Un año más tarde, y en base a tal Informe, se aprueba la *Privacy Act* de Estados Unidos, y van poniéndose las bases de los principios esenciales configuradores del núcleo esencial del derecho a la privacidad. Como se ha señalado, de los *privacy principles* se pasa a las *privacy laws*[12]. Veremos que tales principios fueron en parte el embrión de los

---

[11] U.S. Department of Health , Education & Welfare, *Records, Computeres and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data System*. Vid. Solove, Rotenberg y Schwartz, *Information Privacy Law*, págs. 35-36 y 577-578.

[12] Bennett y Raab, *The Governance of Privacy. Policy Instruments in Global Perspective*, The Mit Press, Cambridge-Londres, 2006, pág. 121.

que más tarde se recogerían en textos internacionales y en normas europeas y nacionales. Volviendo a Europa, en 1978 se aprueba la Ley francesa de Informática, Ficheros y Libertades, sustancialmente modificada, al objeto de adaptarla a la Directiva 95/46/CEE, por la Ley nº 2004-801, de 6 de agosto de 2004, relativa a la protección de las personas físicas en relación con el tratamiento de datos de carácter personal. El 8 de mayo de 1979 el Parlamento Europeo aprueba una Resolución sobre «*La tutela de los Derechos del individuo frente al creciente progreso técnico en el sector de la informática*». En junio de 1978 se aprobaron en Dinamarca dos leyes, una sobre registros privados y otra sobre registros públicos. En 1978 se aprueba en Austria la Ley de Protección de Datos, que consagra el Derecho fundamental de todo ciudadano a exigir la confidencialidad del tratamiento y comunicación de los datos que le conciernan, y en marzo de 1979 se aprueba en Luxemburgo la Ley sobre utilización de datos en tratamientos informáticos.

En los años ochenta, desde el Consejo de Europa se dará un respaldo definitivo a la protección de la intimidad frente a la informática mediante el Convenio nº 108 para la Protección de las Personas con respecto al tratamiento automatizado de los datos de carácter personal (1.981), en el que se estable-

cen los principios y Derechos que cualquier legislación estatal debe recoger a la hora de proteger los datos de carácter personal.

En fin, también la OCDE publica dos importantes Recomendaciones en esta materia: la Recomendación sobre *«Circulación internacional de datos personales para la protección de la intimidad»* y la Recomendación relativa a la *«Seguridad de los sistemas de información»*.

La perspectiva de entonces es clara: se pretende resolver la tensión existente entre el uso cada vez más generalizado de la informática y el riesgo que el mismo puede suponer para la vida privada. Informática *versus* intimidad: éste es el gran dilema. Esta es también la lógica de la Constitución española de 1978 en su artículo 18.4.

Unos años más tarde, el 15 de diciembre 1983, el Tribunal Constitucional Alemán dicta su capital Sentencia sobre el Censo en el que, como ya he apuntado más atrás, se reflejan las aportaciones que desde la doctrina (principalmente norteamericana y en particular de la mano de Westin) se habían producido en orden a destacar el papel capital que tiene el control sobre la propia información en la configuración del derecho a la privacidad y a la protección de datos. El Tribunal Constitu-

cional Alemán completó los derechos constitucionales de la personalidad a pesar de la inexistencia en la Ley Fundamental de 1.949 de un derecho específico. Sobre la base del derecho a la dignidad humana y al libre desarrollo de la personalidad el Tribunal garantizó la continuidad de las libertades básicas, consagradas con anterioridad, con la formulación de un nuevo derecho, el derecho a la autodeterminación informativa[13]. En la clave de bóveda del ordenamiento de la Ley Fundamental, dice el Tribunal, se encuentra la dignidad de la persona, que actúa con libre autodeterminación como miembro de una sociedad libre. El derecho general de la personalidad abarca la facultad del individuo, derivada de la autodeterminación, de decidir básicamente por sí mismo cuándo y dentro de qué límites procede revelar situaciones referentes a la propia vida, protegiéndole contra la recogida, el almacenamiento, la utilización y la transmisión ilimitada de los datos concernientes a la persona. Se garantiza así la facultad del individuo de decidir básicamente por sí sólo sobre la difusión y utilización de sus datos personales. El tratamiento automatizado de datos ha incrementado en una medida

---

[13] Sobre ello, como ya he señalado más atrás, es esencial la lectura de Pablo Lucas Murillo de la Cueva, *El derecho a la autodeterminación informativa*, Tecnos, Madrid, op. cit.

hasta ahora desconocida las posibilidades de incidir sobre la conducta del individuo. El que no pueda percibir con seguridad suficiente qué informaciones relativas a su persona son conocidas en determinados sectores de su entorno social y no pueda saber en consecuencia qué se sabe de él, puede coartar substancialmente su libertad de planificar o decidir. Por ejemplo, quien sepa de antemano que su participación en una reunión o iniciativa ciudadana va a ser registrada por las autoridades y que podrán derivarse riesgos para él por este motivo renunciará presumiblemente a lo que supone un ejercicio de sus derechos fundamentales. De modo que un dato carente en sí mismo de interés puede cobrar un nuevo valor de referencia y, en esta medida, concluye el Tribunal, ya no existe, desde la perspectiva del tratamiento automatizado de datos, ninguno «sin interés».

A partir de esta sentencia, que incorpora a los principios esenciales del derecho a la privacidad el del consentimiento, tal derecho y el derecho a la protección de datos ya no fueron lo mismo en Europa. Aunque todavía faltaba mucho por andar.

En la década de los noventa se incorpora un elemento fundamental al debate. La construcción europea, que requiere ineludiblemente la constitución del mercado interior, exige que

se garantice la libre circulación de los datos personales, dado el valor económico que los mismos tienen en las transacciones comerciales, sobre todo en el marco de una economía cada vez más globalizada y transfronteriza. En este escenario se mueve la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Los tres primeros considerandos de la Directiva son de una importancia capital y centran perfectamente el sentido de la norma[14].

---

[14] «(1) Considerando que los objetivos de la Comunidad definidos en el Tratado, tal y como quedó modificado por el Tratado de la Unión Europea, consisten en lograr una unión cada vez más estrecha entre los pueblos europeos, establecer relaciones más estrechas entre los Estados miembros de la Comunidad, asegurar, mediante una acción común, el progreso económico y social, eliminando las barreras que dividen Europa, fomentar la continua mejora de las condiciones de vida de sus pueblos, preservar y consolidar la paz y la libertad y promover la democracia, basándose en los Derechos fundamentales reconocidos en las constituciones Y leyes de los Estados miembros y en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales;

(2) Considerando que los sistemas de tratamiento de datos están al servicio del hombre; que deben, cualquiera que sea la nacionalidad o la residencia de las personas físicas, respetar las libertades y Derechos fundamentales de las personas físicas y, en particular, la intimidad, y

Al par de conceptos intimidad-informática, se añade ahora uno más: el valor económico de los datos personales en relación con el respeto a los Derechos y en particular al Derecho a la intimidad. La construcción europea pasa por la creación del mercado interior en el respeto a los Derechos fundamentales, y en este marco la libre circulación de los datos con respeto al Derecho a la intimidad se considera de primera importancia. A ese fin responde la Directiva 95/46/CEE, de la que deriva la legislación de los países europeos en materia de protección de datos, y en particular, en España, la Ley Orgánica 15/1999, de 13 de diciembre[15].

---

contribuir al progreso económico y social, al desarrollo de los intercambios, así como al bienestar de los individuos;

(3) Considerando que el establecimiento Y funcionamiento del mercado interior, dentro del cual está garantizada, con arreglo al artículo 7 A del Tratado, la libre circulación de mercancías, personas, servicios y capitales, hacen necesaria no sólo la libre circulación de datos personales de un Estado miembro a otro, sino también la protección de los Derechos fundamentales de las personas»

[15] La protección de datos es tomada en consideración, además de en la citada Directiva 95/46, en otras tales como la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, también conocida como «Directiva sobre la privacidad y las comunicaciones electrónicas», que ha

2.- El derecho a la protección de datos como nuevo derecho, autónomo e independiente del derecho a la intimidad.

En el año 2000 la situación experimenta un giro copernicano tanto en Europa como en España. Se abre una nueva etapa, en la que nos encontramos, que se basa en la consideración de la protección de datos de carácter personal como un verdadero Derecho fundamental autónomo e independiente del Derecho a la intimidad. Tan radical innovación deriva fundamentalmente de la Carta de los Derechos Fundamentales de la Unión Europea, proclamada en la Cumbre de Niza de 7 de diciembre de 2000, que de forma lacónica, pero tajante dispone, en su artículo 8, dentro del Capítulo relativo a las Libertades, que *«Toda persona tiene Derecho a la protección de los datos de carácter personal que la conciernan»*. Ninguna referencia a la intimidad o privacidad; ninguna a la informática. Sí una previsión expresa, de suma importancia,

---

sustituido a la Directiva 97/66/CE, relativa al tratamiento de los datos personales y protección de la intimidad en el sector de las telecomunicaciones. Además de las normas sobre protección de datos existen otras dos Directivas que complementan a las anteriores en el campo del comercio electrónico, a saber, la Directiva 2000/31/CE, de comercio electrónico, y la 1999/93/CE, sobre firma electrónica, aunque en ningún caso sustituyen a aquellas en lo relativo a la protección de datos personales.

al hecho de que «*El respeto de estas normas* [sobre protección de datos] *quedará sujeto al control de una autoridad independiente*». Además, en el artículo 7º, de forma separada, se recoge el derecho a la vida privada y familiar. Hay, pues, una clara diferenciación entre ambos derechos, el derecho a la privacidad y el derecho a la protección de datos, que merecen, en consecuencia, dos preceptos distintos. Por su parte, el Tribunal Europeo de Derechos Humanos dicta las importantes Sentencias Amann contra Suiza, de 16 de febrero de 2000, y Rotaru contra Rumanía, de 4 de mayo del mismo año. En ambas el Tribunal aboga por una interpretación amplia del derecho a la vida privada reconocido en el artículo 8º del Convenio Europeo de Derechos Humanos, y considera que tal derecho comprende también el derecho a establecer y desarrollar relaciones con otros seres humanos, al tiempo que hace una referencia al Convenio 108 y al concepto de dato personal[16].

En España, ese cambio hacia la consideración del Derecho a la protección de datos como un verdadero Derecho autónomo e independiente viene de la mano de dos importantísimas sentencias del Tribunal Cons-

[16] § 65 de la primera y § 43 de la segunda.

titucional: las números 290 y 292 de 2000, ambas de 30 de noviembre. La segunda, que consolida una evolución jurisprudencial constitucional que ha ido configurando el Derecho a la protección de datos, desde el reconocimiento del Derecho a la intimidad y privacidad, pasando por el llamado Derecho a la autodeterminación informática o informativa[17], es la que definitivamente ha reconocido que el Derecho fundamental a la protección de datos personales deriva directamente de la Constitución y debe considerarse como un Derecho autónomo e independiente. El Fundamento

---

[17] Merece la pena recordar ahora las Sentencias constitucionales 110/84, 254/93, 143/94, 94/98, 11/98, 144/99 y 202/99. En particular, la STC 254/1993 señala que la Constitución de 1978 ha incorporado el «Derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona proveniente de un uso ilegítimo del tratamiento automatizado de datos». Añade que no es posible aceptar que «el Derecho fundamental a la intimidad agota su contenido en facultades puramente negativas, de exclusión. Las facultades precisas para conocer la existencia, los fines y los responsables de los ficheros automatizados… son absolutamente necesarias para que los intereses protegidos por el artículo 18 de la Constitución, y que dan vida al Derecho fundamental a la intimidad, resulten real y efectivamente protegidos». La bibliografía sobre la jurisprudencia constitucional en materia de protección de datos es ya abundante. Puede verse por todos Antonio Troncoso Reigada, «La protección de datos personales. Una reflexión crítica de la jurisprudencia constitucional», en *Cuadernos de Derecho Público*, nº 19-20, monográfico sobre *Protección de Datos*, págs. 231 y ss.

Jurídico Séptimo es sin duda esencial, y pese a que es de sobra conocido merece la pena transcribirlo una vez más:

«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».

Reconoce, pues, la existencia del Derecho a la protección de datos como Derecho autónomo e independiente del Derecho a la intimidad; determina su contenido esencial; lo relaciona no sólo con el artículo 18.4 de la Constitución, sino también con el 10.2. Además, en el Fundamento Jurídico 8º cita de forma expresa diversos instrumentos internacionales y en particular, pese a no estar todavía en vigor (apenas había sido adopta-

da), la Carta Europea de Derechos Fundamentales.

3.- El Derecho a la privacidad alcanza también a los dispositivos informáticos que utilizamos.

Se consolida así el concepto de Derecho a la protección de datos, frente a la noción de Derecho a la autodeterminación informativa, cuya construcción tanto debe al Tribunal Constitucional alemán a través de su conocida Sentencia de 15 de diciembre de 1983 sobre la Ley del Censo, a la que antes me he referido. Pero el derecho está en constante evolución. Y una vez más debemos al Tribunal alemán la aportación de una construcción tan importante como novedosa en la definición del alcance de la protección de datos en relación con las nuevas tecnologías. Me refiero a su Sentencia de 27 de febrero de 2008[18]. La sentencia es fruto del recurso interpuesto contra la reforma de la ley de los servicios de inteligencia

[18] A esta Sentencia me he referido en *¿Existe la Privacidad?*, op. cit., págs. 35-36. También, recientemente, Rodota, «Innovación, nuevas tecnologías participación política y protección de datos. Un equilibrio para mejorar la democracia», Conferencia impartida en los Cursos de Verano del 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.

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 ordenadores de cualquier sospechoso: penetran en los ordenadores 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 (en 1983 como ya sabemos) y más tarde del derecho a la protección absoluta de la zona nuclear del comportamiento privado. 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»[19]. Los sistemas de información protegidos por este nuevo dere-

[19] Epígrafe 181 de la Sentencia.

cho son todos aquellos (ordenadores personales, PDAs, teléfonos móviles...) que solos o interconectados con otros pueden contener datos personales del afectado de modo que el acceso al sistema permite hacerse una idea sobre aspectos relevantes del comportamiento vital de una persona o incluso obtener una imagen representativa de su personalidad[20]. 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 online. 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 central de la vida privada («*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

[20] Epígrafe 203.

inmediato sin que puedan ser utilizados en ningún caso.

Es decir, el derecho a la privacidad alcanza también a los dispositivos informáticos que utilizamos y que forman parte ya de nuestra propia vida, que contienen información que nos identifica y que puede dar una imagen de nuestra personalidad. Lo que supone para tal derecho, para la protección de datos, un desarrollo espectacular.

II. *El contenido del derecho fundamental a la protección de datos de carácter personal*

1.- Principios configuradores del derecho a la protección de datos: una breve referencia.

La cuestión estriba entonces en determinar cuál es el contenido esencial de tal derecho; los principios y características que lo definen y que no pueden ser desconocidos so pena de desconocer y en consecuencia violentar el propio derecho.

En otras ocasiones he señalado que tales principios pueden reconducirse a los siguientes: consentimiento, información, finalidad, calidad de los datos, con especial referencia a la proporcionalidad, seguridad. Principios todos ellos recogidos en la Ley Orgánica de Protección de Datos, artículos 4 y ss., a los

que puede añadirse el de utilización leal de los datos y el de minimización en el uso de los datos (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 (regulados, en nuestro caso, en los artículos 15 y ss. de la LOPD).

Debe señalarse que los anteriores principios alcanzan pleno significado desde el reconocimiento de que el derecho fundamental a la protección de datos se fundamenta en el poder de disposición de los datos personales por su titular, y en que tales datos son sometidos a tratamiento. Lo que se traduce en que por definición quien trata datos personales trata datos ajenos, no propios, que debe utilizar con estricto respeto a los derechos del interesado. Esta construcción nos reconduce al respeto a la dignidad de la persona, base fundamental de la protección de datos. Y explica perfectamente los principios que antes he mencionado.

En efecto, si los datos sometidos a tratamiento son datos ajenos y su utilización ha de hacerse en el marco del respeto a la dignidad de la persona y a su poder de disposición sobre los datos, es lógico que cuando se recaben datos deba informarse al interesado (arts. 10

y 11 de la Directiva 95/46/CE; art. 5º de la LOPD y arts. 18 y 19 del Reglamento de desarrollo de la Ley Orgánica, aprobado por Real Decreto 1720/2007, de 21 de diciembre[21]). Que el tratamiento deba estar amparado en un título que habilite su utilización, siendo esencial el consentimiento del titular de los datos (art. 7 de la Directiva y art. 8 de la Carta Europea de Derechos Fundamentales; arts. 6, 7 y 11 de la LOPD; arts. 12 a 17 del Reglamento). Que los datos sólo puedan utilizarse para la o las finalidades legítimas para las que fueron recabados (art. 6.1.a de la Directiva; art. 4 de la LOPD; arts. 8º y 9º del Reglamento). Que ha de respetarse el principio de proporcionalidad y mínima ingerencia en su tratamiento, así como uso leal y lícito de los datos (art. 6 de la Directiva; y, de nuevo, art. 4 de la LOPD y arts. 8º y 9º del Reglamento). Y que deben tratarse con seguridad (arts. 16 y 17 de la Directiva; art. 9 de la LOPD; arts. 79 y ss. del Reglamento). Todo ello, además, como he señalado, garantizado a su vez por el

---

[21] Sobre el Reglamento vid., entre otras obras, Zabia (Director), *Protección de Datos. Comentarios al Reglamento*, Lex Nova, Valladolid, 2008. Piñar Mañas y Canales Gil, *Legislación de Protección de Datos*, Iustel, Madrid, 2008. Incluye, elaborado por el primero, un «Estudio introductoria. El derecho fundamental a la protección de datos personales. Contenido esencial y retos actuales. En torno al nuevo Reglamento de Protección de Datos» (págs. 17 a 94).

reconocimiento a los titulares de los datos de los derechos de acceso, rectificación, cancelación y oposición (arts. 12 y sigs. de la Directiva; arts. 15 y ss. de la LOPD; arts. 23 y ss. del Reglamento), imprescindibles para garantizar ese derecho de disposición de los datos que está en la base misma del sistema.

2.- En particular, el principio de control independiente.

Además, la Carta Europea de Derechos Humanos, siguiendo ya la tónica de textos anteriores, da un paso capital a favor de otro de los principios que ya son inherentes a la protección de datos: el principio que podría denominarse de control independiente. En efecto, al disponer que «*El respeto de estas normas [de protección de datos] quedará sujeto al control de una autoridad independiente*» está exigiendo la existencia de tal autoridad como requisito para considerar que el derecho a la protección de datos está suficientemente garantizado. De modo que se presume que, faltando esa autoridad, no es posible en ningún caso considerar aceptable el marco jurídico regulador del derecho. Precisamente uno de los puntos esenciales de las decisiones de adecuación que hasta ahora ha aprobado la Comisión Europea en relación con la protección ofrecida por terceros países

es la de la existencia de una autoridad independiente de control.

La previsión de la Carta Europea no es en absoluto nueva, aunque sí lo es el hecho de recogerla en documento de tanta trascendencia. La Resolución 45/95 de la Asamblea General de Naciones Unidas, de 14 de diciembre de 1990, por la que se establecen las Directrices de protección de datos, dispone en su punto 8 que «el derecho de cada país designará a la autoridad que, de acuerdo con su sistema jurídico interno, vaya a ser responsable de supervisar la observancia de los principios [de protección de datos]. Esta autoridad ofrecerá garantías de imparcialidad, independencia frente a las personas o agencias responsables de procesar y establecer los datos, y competencia técnica». Por su parte, el Protocolo Adicional al Convenio 108 del Consejo de Europa, relativo a las autoridades de Supervisión y a las Transferencias internacionales de datos, de 8 de noviembre de 2001, señala en su preámbulo que «las autoridades de supervisión, ejerciendo sus funciones con completa independencia, son elemento de la efectiva protección de los derechos de las personas en relación con el tratamiento de datos personales». En esta línea, el artículo 1.3 dispone que «las autoridades de supervisión ejercerán sus funciones con completa independencia», y el punto 4 del mismo artí-

culo añade que «las decisiones de las autoridades de supervisión que den lugar a reclamaciones, pueden ser recurridas judicialmente». Y, por supuesto, la Directiva 95/46/CE, cuyo artículo 28.1 dispone claramente que «los Estados miembros dispondrán que una o más autoridades públicas se encarguen de vigilar la aplicación en su territorio de las disposiciones adoptadas por ellos en aplicación de la presente Directiva. Estas autoridades ejercerán las funciones que le son atribuidas con total independencia».

En definitiva, pues, el principio de tutela del derecho a través de una autoridad independiente se ha constituido ya como verdadero principio del derecho a la protección de datos.

Y el Tribunal Constitucional ya se ha pronunciado, con tanta claridad como contundencia, sobre la posición que en el sistema de garantías del derecho fundamental a la protección de datos ocupa la Agencia Española de Protección de Datos. Ha sido en la ya citada Sentencia 290/2000, de 30 de noviembre, en la que resalta la importancia que en el sistema de la protección de datos tiene la autoridad independiente de control. Señala el Tribunal Constitucional español que «*En lo que respecta… a la Agencia de Protección de Datos…, ha de comenzarse señalando que en las regulaciones legales adoptadas antes de la entra-*

da en vigor de nuestra Constitución por varios Estados europeos con la finalidad de proteger los datos personales frente a los peligros de la informática (Ley sueca de 11 de mayo de 1973, Ley de la República Federal de Alemania, de 22 de enero de 1977, Ley francesa de 6 de enero de 1978, Ley noruega de 8 de junio de 1978), también está presente un elemento institucional. Pues dichas regulaciones, pese a las diversas denominaciones y dependencias orgánicas que establecen, tienen en común el haber creado instituciones especializadas de Derecho público, a las que se atribuyen diversas funciones de control sobre los ficheros de datos personales susceptibles de tratamiento automatizado, tanto de titularidad pública como privada». Y señala que en el modelo español la Agencia se configura como *«un Ente de Derecho Público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones»*. Asimismo el Tribunal justifica la atribución de funciones y potestades a la Agencia de Protección de Datos *«para asegurar, mediante su ejercicio, que serán respetados tanto los límites al uso de la informática como la salvaguardia del derecho fundamental a la protección de datos personales en relación con todos los ficheros, ya sea de titularidad pública o privada»*.

Y advierte que «*la creación de dicho ente de Derecho público y las funciones atribuidas al mismo permiten garantizar, …el ejercicio por los ciudadanos del haz de facultades que integra el contenido del derecho fundamental*». De modo que la Agencia de Protección de Datos «*garantiza el ejercicio por los ciudadanos del derecho fundamental a la protección de dichos datos*». Y dado «*que la garantía de estos derechos, así como la relativa a la igualdad de todos los españoles en su disfrute es el objetivo que guía la actuación de la Agencia de Protección de Datos, es claro que las funciones y potestades de este órgano han de ejercerse cualquiera que sea el lugar del territorio nacional donde se encuentren los ficheros automatizados conteniendo datos de carácter personal y sean quienes sean los responsables de tales ficheros*».

Es claro, pues, que la existencia de una autoridad independiente de control forma parte del sistema del derecho fundamental a la protección de datos personales. Entre nosotros el principio de control independiente se materializa a través de la Agencia Española de Protección de Datos (artículos 35 y ss. de la LOPD) y de las Agencias Autonómicas de Protección de Datos[22].

---

[22] Hasta ahora se han constituido las Agencias de Madrid (Ley 8/2001, de 13 de julio, de Protección de

3.- Protección de datos y otros derechos. En particular, protección de datos y libertad de expresión.

Que se reconozca un derecho autónomo a la protección de datos, sujeto a un sistema especialmente riguroso de tutela y supervisión para garantizar su efectividad, es especialmente importante no sólo para el derecho en sí, sino para el ejercicio y desarrollo de otros derechos.

La protección de datos, 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[23] 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

---

Datos de Carácter Personal en la Comunidad de Madrid), Cataluña (Ley 5/2001, de 19 de abril, de la Agencia Catalana de Protección de Datos) y País Vasco (Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de creación de la Agencia Vasca de Protección de Datos).

[23] El derecho a la protección de datos se reconoce a todas las personas físicas.

reales que se han producido en este sentido. Lo grave, además, es 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 (pensemos en una persona a la que se despide como consecuencia de la información obtenida sobre ella derivada de sus datos personales de creencias religiosas o afiliación sindical, o que no es contratada por una empresa como consecuencia del uso ilegítimo de sus datos genéticos, que permiten a la empresa acceder a su información personal. O la violación de la intimidad derivada del uso de cámaras de videovigilancia o de dispositivos de radiofrecuencia). Las nuevas tecnologías hacen posible situaciones de invasión de los derechos de libertad difícilmente imaginables hasta la fecha. Por ello debe resaltarse con intensidad la importancia que ha de otorgarse a la protección de datos de carácter personal como derecho que favorece el ejercicio efectivo de la libertad.

Por otra parte, sin embargo, la protección de datos puede considerarse como un obstáculo 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. Se ha llegado a considerar que la

protección de datos puede dificultar el ejercicio efectivo de estos derechos. Sin embargo no es en absoluto así. 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. A la relación entre libertad de expresión y protección de datos, se ha referido la conocida Sentencia del TJCE de 6 de noviembre de 2003, *Linqvist*, Asunto C-101/01. Pero con mayor detalle ha vuelto a ocuparse de ello el Tribunal de Justicia en su Sentencia de 16 de diciembre de 2008, *Satakunnan,* asunto C-73/07. Para apreciar la importancia del asunto resuelto, conviene exponer algunos de los hechos que dieron lugar al conflicto: Desde hace muchos años una determinada empresa recoge en Finlandia datos públicos de la administración fiscal finlandesa para publicar cada año extractos de dichos datos en las ediciones regionales del periódico *Veropörssi*. Los datos contenidos en dichas publicaciones comprenden el nombre y apellido de alrededor de 1.200.000 personas físicas cuyos ingresos superan determinados umbrales y con un margen de aproximación de 100 euros, los datos relativos a las rentas derivadas de sus rendimientos del trabajo y del capital, así como indicaciones relativas a la imposición de su patrimonio. La información se clasifica por municipio y por tipo de renta y se hace constar por orden alfabético. Del periódico

pueden eliminarse los datos personales a instancia del interesado y sin coste alguno. Aunque dicho periódico contiene también artículos, resúmenes y anuncios, su finalidad esencial es publicar información personal de carácter fiscal. La empresa en cuestión transmitió a Satamedia, de cuyo capital social son titulares las mismas personas, varios CD-ROM con los datos personales publicados en el periódico para su publicación por un sistema de mensajes de texto (SMS). A estos efectos, las dos sociedades firmaron un acuerdo con una operadora de telefonía móvil que, por cuenta de Satamedia, estableció un servicio de mensajes de texto que permite a los usuarios de teléfonos móviles recibir en su teléfono, por el pago de unos 2 euros, los datos publicados en el *Veropörssi*. A instancia del interesado, los datos personales se eliminan de dicho servicio[24]. Ante tales hechos, se plantearon diversas cuestiones prejudiciales de entre las que nos interesa la siguiente: ¿Debe interpretarse la Directiva 95/46/CE en el sentido de que puede considerarse que las diversas actividades mencionadas anteriormente constituyen un «tratamiento de datos personales realizado con fines exclusivamente periodísticos», en el sentido del artículo 9 de la Directiva, si se tiene en cuenta que los datos que se han recogido, y que se refieren a

[24] Epígrafes 25 a 29 de la Sentencia.

más de 1.000.000 de contribuyentes, proceden de documentos que son públicos en virtud de la normativa nacional sobre acceso a la información?.

El Tribunal parte de la base de que, según reiterada jurisprudencia, la interpretación de las disposiciones de una directiva debe realizarse a la luz del objetivo perseguido por ésta y del sistema que establece (cita, en este sentido, la sentencia de 11 de septiembre de 2008, *Caffaro*, C-265/07, Rec. p. I-0000, apartado 14). El objeto de la Directiva 95/46/CE es «que los Estados miembros, al tiempo que permiten la libre circulación de datos personales, garanticen no obstante la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de dichos datos». Sin embargo, dicho objetivo no puede alcanzarse sin tener en cuenta que los referidos derechos fundamentales han de conciliarse, en una cierta medida, con el derecho fundamental a la libertad de expresión, contemplada en el artículo 9 de la Directiva, que tiene por objeto conciliar dos derechos fundamentales: por una parte, la protección de la intimidad y, por otra, la libertad de expresión. Para conciliar esos dos «derechos fundamentales» en el sentido de la Directiva, los Estados miembros han de prever determinadas excepciones o

restricciones a la protección de datos y, por lo tanto, al Derecho fundamental a la intimidad. Tales excepciones deben establecerse exclusivamente con fines periodísticos o de expresión artística o literaria, que están comprendidos dentro del derecho fundamental de la libertad de expresión artística o literaria, sólo en la medida en que resulten necesarias para conciliar el derecho a la intimidad con las normas que rigen la libertad de expresión. Para tener en cuenta la importancia que tiene la libertad de expresión en toda sociedad democrática –continúa el Tribunal–, procede, por una parte, interpretar ampliamente los conceptos relacionados con ella, entre ellos el de periodismo. Por otra parte, y para obtener una ponderación equilibrada de los dos derechos fundamentales, la protección del derecho fundamental a la intimidad exige que las excepciones y restricciones a la protección de los datos previstas en la Directiva se establezcan dentro de los límites de lo que resulte estrictamente necesario. Lo que, como señala el Tribunal, exige tener en cuenta los elementos siguientes. En primer lugar, las exenciones y excepciones previstas en el artículo 9 de la Directiva se aplican no sólo a las empresas de medios de comunicación, sino también a toda persona que ejerza una actividad periodística. En segundo lugar, el hecho de que se publiquen datos personales con ánimo de lucro no excluye *a priori* que pueda conside-

rarse una actividad «exclusivamente con fines periodísticos». En tercer lugar ha de tenerse en cuenta la evolución y la multiplicación de los medios de comunicación y de difusión de información. El soporte en el que se transmiten los datos, clásico como el papel o las ondas de radio, o electrónico como Internet, no es determinante para apreciar si se trata de una actividad «con fines exclusivamente periodísticos». De todo cuanto antecede resulta que actividades como las controvertidas, relativas a datos procedentes de documentos públicos según la legislación nacional, pueden calificarse de «actividades periodísticas» si su finalidad es divulgar al público información, opiniones o ideas, por cualquier medio de transmisión. No están reservadas a las empresas de medios de comunicación y pueden ejercerse con ánimo de lucro. Por consiguiente, el artículo 9 de la Directiva debe interpretarse en el sentido de que las actividades analizadas, relativas a datos procedentes de documentos públicos según la legislación nacional, han de considerarse actividades de tratamiento de datos personales efectuadas «exclusivamente con fines periodísticos» en el sentido de dicha disposición, si tales actividades se ejercen exclusivamente con la finalidad de divulgar al público información, opiniones

o ideas, siendo esta apreciación competencia del órgano jurisdiccional remitente[25].

Es evidente, pues, que, como el resto de los derechos (salvo, en mi opinión, el derecho a la vida y la propia dignidad de la persona), la protección de datos es un derecho no absoluto, o sujeto a límites. La Sentencia del Tribunal Constitucional 70/2009, de 23 de marzo, se refiere a ello, aunque en relación no con el derecho a la protección de datos sino con el derecho a la intimidad que reconoce el artículo 18.1 de la Constitución. Con unas consideraciones que, sin embargo, son perfectamente trasladables al primero. El Tribunal parte de la estrecha vinculación del derecho a la intimidad con la dignidad de la persona (art. 10.1 de la Constitución) y señala (FJ 2º) que «el derecho a la intimidad contenido en el art. 18.1 CE no sólo preserva al individuo de la obtención ilegítima de datos de su esfera íntima por parte de terceros, sino también de la revelación, divulgación o publicidad no consentida de esos datos, y del uso o explotación de los mismos sin autorización de su titular. Lo que el art. 18.1 CE garantiza es, por tanto, el secreto sobre la propia esfera de vida personal y, por tanto, veda a los terceros, particulares o poderes públicos, decidir sobre los contornos de la vida privada (STC 83/

[25] §§ 51 a 62 de la Sentencia.

2002, de 22 de abril, FJ 5)». Tal derecho sin embargo no es absoluto: Como señala el Tribunal en el FJ 4º, «los derechos fundamentales no son ni ilimitados ni absolutos (por todas STC 198/2004, de 15 de noviembre, FJ 8), por lo que pueden ser sometidos a restricciones. Llevando esta afirmación al derecho a la intimidad, y como ya afirmamos en la STC 196/2004, de 15 de noviembre, aunque la Constitución, en su artículo 18.1, no prevé expresamente la posibilidad de un sacrificio legítimo de tal derecho (a diferencia, por ejemplo, de lo que ocurre con los derechos a la inviolabilidad del domicilio o al secreto de las comunicaciones proclamados en los arts. 18.2 y 3 CE), ello no significa que sea un derecho absoluto (FJ 2). Y es que el derecho fundamental a la intimidad personal puede ceder ante otros derechos y bienes constitucionalmente relevantes, siempre que la limitación que haya de experimentar esté fundada en una previsión legal que tenga justificación constitucional, se revele necesaria para lograr el fin legítimo previsto y sea proporcionada para alcanzarlo, y sea además respetuosa con el contenido esencial del derecho (por todas, SSTC 57/1994, de 28 de febrero, FJ 6; 143/1994, de 9 de mayo, FJ 6, y 25/2005, de 14 de febrero, FJ 6).

El Tribunal Europeo de Derechos Humanos –recuerda el Tribunal Constitucional– ha

tenido en cuenta estas exigencias, reconociendo que si bien la garantía de la intimidad individual y familiar del art. 8 CEDH puede tener límites como la seguridad del Estado (STEDH de 26 de marzo de 1987, caso Leander), o la persecución de infracciones penales (mutatis mutandis casos Funke, de 25 de febrero de 1993, y Z. contra Finlandia, de 25 de febrero de 1997), tales limitaciones han de estar previstas legalmente y ser 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 (SSTEDH caso X. e Y., de 26 de marzo de 1985; caso Leander, de 26 de marzo de 1987; caso Gaskin, de 7 de julio de 1989; mutatis mutandis, caso Funke, de 25 de febrero de 1993; caso Z., de 25 de febrero de 1997). También el Tribunal de Justicia de las Unión Europea, en la Sentencia de 5 de octubre de 1994 (asunto X. contra Comisión, C-404/92 P), referida a la protección de la intimidad y al tratamiento de datos relativos a la salud, afirma que «los derechos fundamentales pueden ser sometidos a restricciones, siempre y cuando éstas respondan efectivamente a objetivos de interés general y no constituyan, en lo

que respecta al fin perseguido, una intervención desmesurada e intolerable que afecte a la propia esencia de los derechos garantizados».

Como digo, la Sentencia se refiere al derecho a la intimidad, pero sus conclusiones son perfectamente trasladables a la protección de datos. Incluso el Tribunal hace referencia expresa al Convenio 108 del Consejo de Europa y a la Directiva 95/46/CE (FJ 2, último párrafo) al objeto de resaltar la necesidad de otorgar una especial protección a los datos de salud y señalar que «el derecho a la intimidad queda así relevantemente afectado cuando, sin consentimiento del paciente, se accede a datos relativos a su salud o a informes relativos a la misma».

III. *El derecho a la protección de datos en España. Una evolución legislativa*[26].

1.- De la LORTAD a la LOPD.

Muy bien puede decirse que el marco jurídico de la protección de datos en España nace específicamente con la Ley Orgánica 5/

---

[26] Las consideraciones del presente apartado las tomo en lo esencial de mi trabajo «Estudio Introductoria. El derecho fundamental a la protección de datos personales…», en Piñar y Canales, *Legislación de Protección de Datos*, op. cit., págs. 31 y ss.

1992, de 29 de octubre, de Regulación del tratamiento automatizado de datos de carácter personal (LORTAD) que supuso un hito en el reconocimiento del derecho a la protección de datos y sentó las bases del que es sin duda uno de los modelos europeos más garantistas y respetuosos con los derechos de las personas. La ley venía a desarrollar el artículo 18.4 de la Constitución, que como hemos visto es el punto de conexión constitucional del derecho a la protección de datos y que si bien se refiere esencialmente al reconocimiento de tal derecho en el ámbito de los tratamientos automatizados, en el ámbito de la informática, también es, junto con el artículo 10 de la Constitución, el origen de la más amplia concepción del derecho, extensible asimismo a los tratamientos no automatizados.

La LORTAD –cuya aprobación se precipitó ante la incorporación de España al espacio Shenguen y debido a las garantías que debían establecerse en el tratamiento de datos que el mismo traería consigo–, se adoptó cuando ya estaban en marcha los trabajos que darían lugar a la Directiva 95/46/CE, pero en cualquier caso es previa a la norma comunitaria. No obstante, pudo ya recoger gran parte de lo que más tarde sería el texto de la Directiva, pero con algunas diferencias dignas de tener en cuenta. Así, sólo era aplicable a los tratamientos automatizados de datos (en línea, por

lo demás, con el artículo 18.4 de la Constitución, que como sabemos habla del uso de «la informática») y no recogía el derecho de oposición, además de dejar fuera de su ámbito ficheros y tratamientos que luego serían incorporados a la LOPD (por ejemplo, el Registro de la Propiedad).

La LORTAD –cuya Exposición de Motivos merece ser leída por los planteamientos novedosos que la misma contiene y aunque sólo sea para compensar la desconcertante ausencia de Exposición en la LOPD–, fue objeto de desarrollo reglamentario. Se dictaron los Reales Decretos 428/1993, de 26 de marzo, por el que se aprobó el Estatuto de la Agencia de Protección de Datos, 1332/1994, de 20 de junio de desarrollo parcial de la LORTAD y 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad[27]. Asimismo, la Agencia dictó las Instrucciones 1[28] y 2/1995[29], 1[30] y 2/1996[31] y 1/1998[32].

---

[27] Mediante Real Decreto 195/2000, de 11 de febrero se estableció el plazo para implantar las medidas de seguridad de los ficheros automatizados previstas por el Reglamento de medidas de seguridad.

[28] Instrucción 1/1995, de 1 de marzo, relativa a prestación de servicios de información sobre solvencia patrimonial y crédito.

[29] Instrucción 2/1995, de 4 mayo, de medidas que garantizan la intimidad de los datos personales recabados

2.- La LOPD y alguna legislación sectorial con incidencia en el derecho a la protección de datos.

Tras la adopción de la Directiva 95/46/CE, del Parlamento y el Consejo, de 24 de octubre, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, era necesario aprobar un nuevo texto legal al objeto de transponer su contenido al ordenamiento interno. Su artículo 32.1 daba a los Estados miembros un plazo de tres años desde la adopción de la misma para que adoptasen las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo establecido en ella, plazo que se extendía hasta doce años en relación con «el tratamiento de datos que ya se encuentren incluidos en ficheros manuales en la fecha de entrada en vigor de las disposicio-

---

como consecuencia de la contratación de un seguro de vida de forma conjunta con la concesión de un préstamo hipotecario o personal

[30] Instrucción 1/1996, de 1 marzo, de ficheros automatizados establecidos con la finalidad de controlar el acceso a edificios

[31] Instrucción 2/1996, de 1 marzo, de ficheros automatizados establecidos con la finalidad de controlar el acceso a los casinos y salas de bingo

[32] Instrucción 1/1998, de 19 de enero, relativa al ejercicio de los derechos de acceso, rectificación y cancelación.

nes nacionales adoptadas en aplicación de la presente Directiva». Este es precisamente el motivo por el que en la Disposición Adicional primera de la LOPD se establece un plazo de 12 años, a contar desde el 24 de octubre de 1995, para la adecuación a la Ley de los ficheros y tratamientos no automatizados[33].

Los primeros borradores y el Proyecto de nueva Ley habían surgido como reforma parcial de la LORTAD al objeto de adaptar su texto a la Directiva, y así se explicaba en la breve Exposición de Motivos que incluía el proyecto inicial[34]. Sin embargo, durante el trámite de

---

[33] Plazo que ya finalizó el pasado octubre de 2007.

[34] «La presente Ley tiene por objeto la adaptación del Derecho español a la Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Y para ello se procede a introducir en la normativa española reguladora de la materia, contenida en la Ley Orgánica 5/1992, de 29 de octubre, las modificaciones que vienen reclamadas por el contenido de la referida Directiva, a fin de que el conjunto normativo resultante se adapte y acomode a las exigencias de homogeneidad dispositiva establecidas por la Unión Europea.

En el momento de promulgarse la Ley Orgánica 5/1992, de 29 de octubre, que ahora es objeto de modificación, estaba en trámites de discusión y elaboración la Directiva que se transpone, por lo que los contenidos normativos de lo que en aquel tiempo era una mera propuesta se tuvieron en cuenta por el legislador español

discusión parlamentaria y en el marco de un proceso legislativo cuando menos atípico, se transformó en una nueva y diferente Ley (hecho éste, entre otros, que explica –pero no justifica– la ausencia de Exposición de Motivos de la LOPD) que incorporaba algunas, no muchas pero importantes, novedades. Novedades de sobra conocidas y en las que ahora no podemos entrar.

---

para dar respuesta a la problemática derivada de la protección de la intimidad en el tratamiento de datos personales. Ello significa que la mencionada Ley Orgánica 5/1992, se ajusta en la gran mayoría de sus previsiones a las disposiciones contenidas en la Directiva 95/46/CE, siendo necesario únicamente introducir en aquélla las precisas reformas que den como resultado la total adecuación entre dicha Ley y la Directiva comunitaria.

Ahora bien, las modificaciones legislativas que para la necesaria adecuación a la Directiva se introducen en la Ley vigente, no por aparentemente exiguas carecen de una singular relevancia, pues en definitiva afectan a aspectos tan importantes como los siguientes: Se amplía el ámbito de aplicación de la Ley, si bien se mantienen determinados supuestos en que no es de aplicación el régimen de protección de datos establecido en la misma; se incrementa la protección de los afectados, tanto en lo que respecta a su necesaria información en la obtención de los datos como en la constante presencia de su consentimiento en el tratamiento y cesión de sus datos personales; se incorpora el derecho del afectado de oponerse al tratamiento de sus datos en determinados supuestos; se prevén nuevos supuestos de excepción en las transferencias internacionales de datos, y se aplican a los ficheros convencionales o no automatizados las disposiciones de la Ley reguladora del tratamiento de datos»: *Boletín Oficial de las Cortes Generales. Congreso de los Diputados*. Serie A, nº 135-1, de 31 de agosto de 1998.

Poco después de aprobarse la LOPD el Tribunal Constitucional dictó sus importantes Sentencias 290 y 292/2000, a las que ya me he referido. Sentencias que vienen a consolidar el derecho a la protección de datos como derecho autónomo e independiente del derecho a la intimidad.

La disposición final primera de la LOPD contiene una cláusula de habilitación para su desarrollo reglamentario a cuyo fin dispone que «el Gobierno aprobará, o modificará, las disposiciones reglamentarias necesarias para la aplicación y desarrollo de la presente Ley». Pero, por un lado, no establece plazo alguno al efecto[35], y por otro, la disposición transitoria segunda de la misma Ley establece que «hasta tanto se lleven a efectos las previsiones de la disposición final primera de esta Ley, continuarán en vigor, con su propio rango, las normas reglamentarias existentes y, en especial, los Reales Decretos 428/1993, de 26 de marzo; 1332/1994, de 20 de junio, y 994/1999, de 11 de junio, en cuanto no se opongan a la presente Ley».

---

[35] Aunque, como sabemos, el establecimiento de un plazo no condiciona en principio la legalidad de la norma reglamentaria de desarrollo aprobada tras su vencimiento, lo cierto es que representa de alguna manera una suerte de compromiso para el Gobierno. Compromiso que, como digo, no se fijó en la LOPD.

El juego de ambas disposiciones y la desidia de los sucesivos Gobiernos ha hecho que hayamos tenido que esperar más de nueve años para ver por fin publicado el Reglamento de desarrollo de la LOPD, que por cierto deroga de forma expresa tanto el Real Decreto 1332/1994, como el 994/1999 (no así el Estatuto de la Agencia, que sigue en vigor). Durante este tiempo hemos debido convivir con un marco normativo disperso y fragmentado, cuya vigencia, además, no siempre era clara. Tal era el caso, por ejemplo, del Reglamento de Medidas de Seguridad, aplicable para algunos[36] (en lo que fuese de aplicación) a los tratamientos no automatizados, mientras que otros[37] mantenían con firmeza que sólo se aplicaba a los ficheros y tratamientos automatizados, lo que llevaba necesariamente a la conclusión, más que discutible, de que los primeros, los llamados manuales, estaban exentos de implementar medida de seguridad alguna.

Por otra parte, tras la LOPD (y también, en algún caso, desde antes de su aprobación) se han ido aprobando diversas leyes sectoriales que tienen una muy importante incidencia en

---

[36] Esta era la opinión de la Agencia Española de Protección de Datos.

[37] Por ejemplo, la Agencia de Protección de Datos de la Comunidad de Madrid.

el ámbito de la protección de datos (y en el ejercicio de las competencias por parte de la AEPD). De entre ellas merecen especial referencia la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones[38], la Ley 34/2002, de 11 julio, de Servicios de la Sociedad de la Información y la Ley 59/2003, de 19 de diciembre, de Firma Electrónica. Leyes que atribuyen nuevas competencias a la Agencia y que también estaban necesitadas de desarrollo reglamentario, siquiera sea para regular el procedimiento aplicable en el ejercicio de la potestad sancionadora que a la misma se atribuye.

Asimismo deben ser tenidas en cuenta otras muchas leyes, que afectan, directa o indirectamente a la protección de datos. Tal es el caso, por citar sólo algunas, de la Ley 19/1993, de 28 de diciembre, sobre determinadas medidas de prevención del blanqueo de capitales; la 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; la Ley 41/2002, de 14 de noviembre, reguladora de la autonomía del paciente y de derechos y obli-

[38] Que viene a trasponer la importante Directiva 2002/58/CE, del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas.

gaciones en materia de información y documentación clínica; la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos; la Ley 30/2007, de contratos del sector público; la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, la Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información, o la Ley Orgánica 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN. Leyes a las que, como digo, pueden añadirse muchas más, así como múltiples normas reglamentarias.

3.- La legislación autonómica sobre protección de datos. El marco normativo de la distribución competencial.

En cuanto a las Comunidades Autónomas[39], las previsiones de la LOPD han sido puestas en práctica hasta el momento por tres Comunidades Autónomas: Madrid, Cataluña y País Vasco[40]: Ley 8/2001, de 13 de julio, de protección de datos de carácter personal en la

[39] A ello me he referido ya en «Protección de datos personales y entidades locales», en R. Parada y J.A. Fuentetaja (dirs.), *Reforma y retos de la Administración Local*, Pons, Madrid, págs. 227 y ss.

Comunidad de Madrid, Ley 5/2002, de 19 de abril, de la Agencia Catalana de Protección de Datos, y Ley 2/2004, de 25 de febrero, de ficheros de datos de carácter personal de titularidad pública y de creación de la Agencia Vasca de Protección de Datos. Y lo cierto es que ninguna de las tres leyes coincide plenamente con ninguna de las otras dos al definir su ámbito de aplicación.

La ley madrileña es la más respetuosa con la LOPD. Su artículo 2 se ciñe en lo esencial a lo dispuesto por el artículo 41 de la LOPD. Establece que la Agencia de Protección de Datos de la Comunidad de Madrid ejerce sus funciones sobre los ficheros de datos de carácter personal creados o gestionados por las Instituciones de la Comunidad de Madrid, y por los Organos, Organismos, Entidades de Derecho público y demás entes públicos integrantes de su Administración pública, exceptuándose las sociedades mercantiles, así como sobre los ficheros de los Entes que integran la Administración Local del ámbito territorial de la Comunidad de Madrid, de conformidad con lo previsto en el artículo 41 de la Ley Orgánica 15/1999.

---

[40] Por el orden en que han aprobado sus correspondientes leyes reguladoras de las Agencias Autonómicas respectivas.

La Ley catalana es mucho más ambiciosa. El artículo 3º atribuye a la Agencia Catalana de Protección de Datos competencias sobre los tratamientos de datos personales llevados a cabo por la Generalidad de Cataluña, por los entes que integran la Administración Local y por las Universidades en el ámbito territorial de Cataluña, por los organismos y las entidades autónomas que dependen de la Administración de la Generalidad o los entes locales y por los consorcios de los cuales forman parte, de conformidad con lo que establecen la LOPD y las disposiciones que la desarrollen. Pero también ejerce sus competencias con relación a los ficheros creados por las administraciones, los organismos y las entidades a que nos hemos referido cuando sean gestionados por entidades públicas o privadas en la prestación de servicios públicos, sean o no concesionarias de estos, o por asociaciones o fundaciones, o por las sociedades civiles o mercantiles en las cuales la Generalidad o los entes locales tengan la participación mayoritaria del capital, cuando llevan a cabo actividades por cuenta de una administración pública.

Como es fácil comprobar el citado artículo 3º se extralimita claramente en relación con lo previsto por el artículo 41 de la LOPD, con una redacción, además, enormemente ambigua. Debe tenerse en cuenta, en cualquier caso, que el nuevo Estatuto de Autonomía de

Cataluña de 2006[41] incluye importantes previsiones en materia de protección de datos. Por un lado, el artículo 31 dispone que «Todas las personas tienen derecho a la protección de los datos personales contenidos en los ficheros que son competencia de la Generalitat y el derecho a acceder a los mismos, a su examen y a obtener su corrección. Una autoridad independiente, designada por el Parlamento, debe velar por el respeto de estos derechos en los términos que establecen las leyes»[42]. Por otro, el capital artículo 156 atribuye a la Generalidad *«la competencia ejecutiva en materia de protección de datos de carácter personal que, respetando las garantías de los derechos fundamentales en esta materia, incluye en todo caso*:

---

[41] En relación con la regulación de los derechos en el nuevo Estatuto, vid. V. Farreres, P. Biglino y M. Carrillo, *Derechos, deberes y principios en el nuevo Estatuto de Autonomía de Cataluña»*, Centro de Estudios Políticos y Constitucionales, Madrid, 2006.

[42] El texto, por cierto, es claramente limitador del derecho, pues, por ejemplo, no hace referencia al derecho de cancelación o de oposición. Es importante, sin embargo, destacar que se ha incluido una referencia expresa a la existencia de una autoridad independiente, lo que refuerza el principio de control independiente al que más atrás me refería.

a) La inscripción y el control de los ficheros o los tratamientos de datos de carácter personal creados o gestionados por las instituciones públicas de Cataluña, la Administración de la Generalitat, las administraciones locales de Cataluña, las entidades autónomas y las demás entidades de derecho público o privado que dependen de las administraciones autonómica o locales o que prestan servicios o realizan actividades por cuenta propia a través de cualquier forma de gestión directa o indirecta, y las universidades que integran el sistema universitario catalán.

b) La inscripción y el control de los ficheros o los tratamientos de datos de carácter personal privados creados o gestionados por personas físicas o jurídicas para el ejercicio de las funciones públicas con relación a materias que son competencia de la Generalitat o de los entes locales de Cataluña si el tratamiento se efectúa en Cataluña.

c) La inscripción y el control de los ficheros y los tratamientos de datos que creen o gestionen las corporaciones de derecho público que ejerzan sus funciones exclusivamente en el ámbito territorial de Cataluña.

d) La constitución de una autoridad independiente, designada por el Parlamento, que vele por la garantía del derecho a la protec-

ción de datos personales en el ámbito de las competencias de la Generalitat».

De la lectura del precepto, y sin poder entrar ahora en mayores detalles, podemos deducir algunas conclusiones iniciales: Ante todo, que el Estatuto amplía considerablemente las competencias de la Generalidad en la materia. Especial mención merece el apartado *b)* que parecería haber roto el esquema general de distribución de competencias entre el Estado y las Comunidades Autónomas en virtud del cual al primero le corresponde la competencia exclusiva en relación con los ficheros privados. Al atribuir ahora el Estatuto a la Generalidad la competencia ejecutiva en los términos que acabamos de ver, parece, como digo, que el esquema se ha roto. Pero debe tenerse muy en cuenta que sigue manteniéndose una directa relación de tales ficheros privados con el ejercicio de funciones públicas que correspondan a la Generalidad o a los entes locales de Cataluña. Además, el tratamiento debe efectuarse en Cataluña. En este estricto ámbito debe entenderse la competencia ahora asumida. Por otra parte, la misma no es exclusiva, sino ejecutiva, lo que se traduce, según el artículo 112 del Estatuto en que «la potestad reglamentaria, que comprende la aprobación de disposiciones para la ejecución de la normativa del Estado, así como la función ejecutiva, que en todo caso

incluye la potestad de organización de su propia administración y, en general, todas aquellas funciones y actividades que el ordenamiento atribuye a la Administración pública». Es decir, será necesario aprobar una norma específica que determine el alcance de la competencia. No basta, pues, con el Estatuto, sino que es necesaria, como digo, una normativa de concreción competencial. En tanto no se dicte, seguirá siendo de aplicación la Ley 5/2002, de 19 de abril.

En fin, la Ley vasca 2/2004, de 25 de febrero dispone en su artículo 2.1 que la misma será aplicable «a los ficheros de datos de carácter personal creados o gestionados, para el ejercicio de potestades de derecho público» por diversas entidades de derecho público que el legislador ha preferido enumerar. En principio no parecería que se plantease problema alguno, pero el artículo 23 introduce un elemento de confusión al establecer que las infracciones serán sancionadas con multas económicas en función de la naturaleza de aquéllas (leves, graves o muy graves). Tal previsión no puede entenderse en el sentido de que las Entidades públicas pueden ser sancionadas con multas económicas. El artículo 24 deja claro que en caso de infracción cometida en relación con los ficheros a que se refiere el artículo 2.1 será de aplicación el régimen previsto por aquél, que no ha tomado

en consideración la posibilidad de imponer sanciones económicas. Debe entenderse que las multas económicas han sido estipuladas para el caso de que la Agencia Vasca pueda iniciar expediente sancionador contra un encargado del tratamiento que, siendo privado, actúe por cuenta del responsable público.

La legislación autonómica comentada ha sido objeto del correspondiente desarrollo reglamentario[43]. Pero aún así también estaba necesitada de la aprobación del Reglamento, de desarrollo de la LOPD, pues algunas de sus previsiones tienen carácter básico y se aplican

---

[43] En Madrid, Decreto 40/2004, de 18 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos de la Comunidad de Madrid; Decreto 67/2003, de 22 de mayo, por el que se aprueba el Reglamento de desarrollo de la Agencia de Protección de Datos de la Comunidad de Madrid de tutela de derechos y de control de ficheros de datos de carácter personal; y Decreto 99/2002, de 13 de junio, de regulación del procedimiento de elaboración de disposiciones de carácter general de creación, modificación y supresión de ficheros que contienen datos de carácter personal, así como su inscripción en el Registro de Ficheros de Datos Personales. En Cataluña, Decreto 48/2003, de 20 de febrero, por el que se aprueba el Estatuto de la Agencia Catalana de Protección de Datos. En el País Vasco, Decreto 308/2005, de 18 de octubre, por el que se desarrolla la Ley 2/2004, de 25 de febrero, de ficheros de datos de carácter personal de titularidad pública y de creación de la Agencia Vasca de Protección de Datos y Decreto 309/2005, de 18 de octubre, por el que se aprueba el Estatuto de la Agencia Vasca de Protección de Datos.

en consecuencia a las Comunidades Autónomas. En efecto, la disposición final primera del Real Decreto 1720/2007 enumera los preceptos del reglamento que se dictan al amparo de lo dispuesto en el artículo 149.1.1.ª de la Constitución, que atribuye al Estado la competencia exclusiva para la regulación de las condiciones básicas que garanticen la igualdad de todos los españoles en el ejercicio de los derechos y en el cumplimiento de los deberes constitucionales, y que en consecuencia son aplicables en todo el territorio nacional[44], vinculando, por tanto a las Comunidades Autónomas y, en particular a las Agencias autonómicas de protección de datos.

4.- El desarrollo reglamentario de la LOPD En particular el Reglamento aprobado mediante Real Decreto 1720/2007. Motivos que hacían necesaria su aprobación[45].

Tras la LOPD la Agencia Española de Protección de Datos aprobó tres Instrucciones: la 1/2000, de 1 de diciembre, relativa a las normas por las que se rigen los movimientos internacionales de datos[46]; la 1/2004, de 22 de diciembre, sobre publicación de las resolu-

---

[44] El Título I, con excepción del apartado c) del artículo 4, los Títulos II, III, VII y VIII, así como los artículos 52, 53.3, 53.4, 54, 55.1, 55.3, 56, 57, 58 y 63.3

[45] Vid *supra*, nota 26.

ciones de la Agencia, y la 1/2006, de 8 noviembre, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras. Debe señalarse que la segunda de las citadas tenía su origen, fundamentalmente, en la reforma que se operó en el artículo 37 de la LOPD al que se añadió un nuevo apartado, el 2, mediante Ley 62/2003, de 30 de diciembre. Tanto la reforma legal como la Instrucción tenían como objetivo esencial incrementar la transparencia en la actuación de la Agencia, respondiendo así a las indicaciones que más o menos informalmente se venían efectuando desde la Comisión Europea y permitiendo el más amplio conocimiento de la doctrina de la Agencia por parte de todos.

Varios Reales Decretos y varias Instrucciones, en uno y otro caso anteriores y posteriores a la LOPD, configuraban por tanto el marco jurídico reglamentario de la LOPD. Pero ninguna de tales normas cumplía, ni formal ni materialmente, la habilitación-mandato incluida en la disposición final primera de la Ley Orgánica 15/1999.La situación normativa a nivel reglamentario en el Estado requería, pues, una urgente adaptación a la LOPD.

---

[46] Sobre dicha Instrucción téngase en cuenta la STS de 25 de septiembre de 2006, por la que se anula el apartado 2 de la norma tercera de la misma.

Dada esa necesidad, la Agencia Española de Protección de Datos inició ya en los primeros meses de 2003 los estudios y trabajos preparatorios necesarios para la elaboración del Reglamento. Fue en la Agencia donde, de acuerdo con el Ministerio de Justicia, se dieron los primeros pasos en la redacción de los primeros textos. Una comisión integrada por representantes de una y otro redactó el primer borrador, que se remitió al Ministerio el 30 de diciembre de 2005, y que constituye sin duda el punto a partir del que más tarde se ha trabajado. Lo importante era contar con un borrador inicial abierto a la discusión y el debate y que sirviese como punto de partida para lo que más tarde sería el texto final. Se puso entonces en marcha una serie de actividades para dar a conocer los primeros borradores. Y se redactaron tres versiones más: las de 28 de noviembre de 2006, 30 de marzo de 2007, y 12 de julio de 2007. El Proyecto fue objeto de Dictamen del Consejo de Estado (Dictamen de 15 de noviembre de 2007, Referencia 1909/2007), en el que se deja constancia del gran número de entidades, públicas y privadas, e instituciones que han participado en su elaboración, a través fundamentalmente de la presentación de alegaciones u observaciones[47].

---

[47] Llama la atención el hecho de que el Dictamen del Consejo de Estado no haga referencia al borrador de 30

Dotar al sistema de mayor seguridad jurídica (así como dar cumplimiento a la antes citada Disposición Final de la LOPD) era sin duda el más importante de los motivos que entonces se tuvieron en cuanta para acometer tan necesaria empresa. Pero también había otros muchos de alcance no menor. Sin pretensión de ser exhaustivo, cabe señalar: *a)* la conveniencia de adaptar el incompleto y fragmentario marco reglamentario existente (de desarrollo de la vieja Ley de 1992, que no de la LOPD, como antes decía) a las previsiones de la Ley de 1999. Por ejemplo, como sabemos, la aplicación de la segunda a los tratamientos no automatizados, que no eran regulados por la LORTAD; *b)* La recepción de la doctrina que sobre protección de datos habían ido elaborando tanto los Tribunales (Tribunal Constitucional, Tribunal Supremo, Audiencia Nacional y Tribunales Superiores de Justicia) como la propia Agencia Española de Protección de Datos. Doctrina de enorme interés que ha consolidado ya criterios interpretativos de la LOPD y que ahora se recogen de forma expresa en el nuevo Reglamento. Tal es el caso de la posibilidad de subcontratar los servicios por parte de los

---

de diciembre de 2005 (sí lo hace a los otros tres), lo que podría derivarse del hecho de que el mismo no fuese incluido en el expediente remitido al citado órgano consultivo.

encargados del tratamiento, el reconocimiento y ejercicio del derecho de oposición o los criterios para acreditar la obtención del consentimiento de los interesados, entre otros temas; *c)* La necesidad de aclarar diversas cuestiones relativas a la adecuación de la legislación española al derecho comunitario, y en particular a la Directiva 95/46/CE sobre protección de datos. Incluso se han incorporado algunos conceptos o aclaraciones acuñados por el propio Tribunal de Justicia de la Unión Europea. La breve Exposición de Motivos del Reglamento afirma que «se aprueba este Reglamento partiendo de la necesidad de dotar de coherencia a la regulación reglamentaria en todo lo relacionado con la transposición de la Directiva y de desarrollar los aspectos novedosos de la Ley Orgánica 15/1999, junto con aquellos en los que la experiencia ha aconsejado un cierto de grado de precisión que dote de seguridad jurídica al sistema».

IV. *Retos actuales y futuros de la protección de datos*

Pero aún siendo de capital importancia el análisis y esclarecimiento del marco normativo de la protección de datos, parece que es imprescindible llevar a cabo un estudio aproximativo de los grandes retos que hoy tiene planteados el derecho fundamental a la protección de datos, que pueden llegar a afectar

de modo considerable su propia esencia, cuando no limitar su contenido esencial.

En mi opinión son al menos cinco los retos que debe afrontar la protección de datos. Primero, el de las nuevas tecnologías; segundo, el de la seguridad ciudadana; tercero, la relación con la transparencia y el acceso a la información; cuarto, las necesidades y exigencias del mercado; y por último, la necesidad de revisar gran parte de los planteamientos de la protección de datos en un mundo globalizado en el que la circulación y flujo de datos son absolutamente ajenos a las fronteras físicas convencionales. A continuación analizo algunos de ellos.

1.- Protección de datos y nuevas tecnologías.

Como ya he señalado en otras ocasiones[48], nunca antes como hoy había sido posible, utilizando las tecnologías que están ya al alcance de casi cualquiera, invadir la privacidad de las personas hasta los límites a los que se está llegando. Pensemos que hoy es

---

[48] Recientemente en «Consideraciones introduc-torias sobre el derecho fundamental a la protección de datos de carácter personal», *Boletín del Ilustre Colegio de Abogados de Madrid*, monográfico sobre *La Protección de Datos (I)*, núm. 36, 3ª época, abril 2007, págs. 13 y ss. Asimismo en *¿Existe la Privacidad?*, op. cit., págs. 13 y ss.

posible conocer los contenidos de los correos electrónicos, de las llamadas efectuadas o recibidas mediante teléfonos móviles; que pueden tratarse para múltiples finalidades los datos genéticos; que el uso de datos biométricos está casi a la orden del día; que las nuevas tecnologías pueden afectar grave e intensamente a los derechos fundamentales e incluso pueden condicionar el contenido de las normas jurídicas[49]; que mediante dispositivos de radiofrecuencia[50] es posible no sólo controlar las ventas en un centro comercial sino también localizar personas; que la capacidad de los ordenadores personales y sus funcionalidades se incrementan constantemente al tiempo que se reduce el coste de tales innovaciones –como expresa la llamada «Ley

---

[49] Sobre ello vid. N. IRTI y E. Severino *Dialogo su Diritto e Tecnica*, Editori Laterza, Roma-Bari, 2001; S. Rodota *Tecnologie e diritti*, Il Mulino, Bari, 1995; *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Editori Laterza, Roma-Bari, 1997. Hay traducción al español: *Tecnopolítica. La democracia y las nuevas tecnologías de la información,* Losada, Buenos Aires, 2000; J.L. Piñar Mañas, «Revolución tecnológica, Derecho Administrativo y Administración Pública. Notas provisionales para una Reflexión», en Varios Autores, *La Autorización administrativa. La Administración Electrónica. La Enseñanza del Derecho Administrativo*, Publicaciones de la Asociación Española de Profesores de Derecho Administrativo, Thomson Aranzadi, Cizur Menor, 2007.

[50] Los llamados RFID, «identificadores por radiofrecuencia»

de MOORE»[51]– implicando riesgos potenciales para la privacidad y para la protección de datos personales[52]; que la sociedad corre el riesgo de verse sometida a una videovigilancia constante[53]. Los sistemas de reconocimiento

---

[51] El coste económico de los avances tecnológicos y de nuevos dispositivos es cada vez menor, lo que facilita aún más su uso e implantación. Gordon MOORE 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 «The complexity for minimum component costs has increased at a rate of roughly a factor of two per year… Certainly over the short term this rate can be expected to continue, if not to increase. Over the longer term, the rate of increase is a bit more uncertain, although there is no reason to believe it will not remain nearly constant for at least 10 years»: «Cramming more components onto integrated circuits», *Electronics*, Volumen 38, Número 8, 19 de Abril de 1965.

[52] Vid. Castells, Manuel, *La era de la información. Vol. 1, La sociedad red*, Alianza Editorial, Madrid, 3ª ed., 2005, pág. 70.

[53] El incremento de las cámaras de vigilancia en las calles es ya tan alarmante como algo desgraciadamente normal. Plantea problemas de gran importancia sobre la privacidad y la protección de datos. Vid. el *Dictamen de la Comisión de Venecia sobre la videovigilancia en lugares públicos por parte de las autoridades públicas y la protección de los derechos humanos*, en *Revista Española de Protección de Datos*, nº 3 (julio-diciembre 2007), págs. 427 y ss. La Agencia Española de Protección de Datos ha dictado la Instrucción 1/2006, de 8 de noviembre, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o de videocámaras, a la que me he referido ya más atrás en el

facial, *face recognition technologies*[54], mediante cámaras de videovigilancia permiten el reconocimiento facial de las personas. Hoy a través de los teléfonos móviles es posible localizar prácticamente a cualquier usuario, y lo malo es que puede hacerse sin conocimiento del interesado y por tanto sin su consentimiento. El desarrollo de lo que se ha venido en llamar *ubiquitous computing*[55] puede llegar

---

texto. La Conferencia Internacional de Autoridades de Protección de Datos celebrada en Londres durante los días 1 a 3 de noviembre de 2006 tuvo por tema precisamente la necesidad de adecuar la videovigilancia a las exigencias del derecho fundamental a la protección de datos.

[54] Ver por ejemplo K.W. Bowyer, «Face recognition technology: security versus privacy», *Technology and Society Magazine, IEEE*, Primavera de 2004, Volumen 23, páginas 9 y ss. Jay Stanley y Barry Steinhardt. «Face-Recognition Technology Threatens Individual Privacy.» *Opposing Viewpoints: Civil Liberties*. Ed. Tamara L. Roleff. San Diego: Greenhaven Press, 2004. Ver http://www.enotes.com/civil-liberties-article/41394. Ver un ejemplo de tal sistema en Holtzman, *Privacy lost. How Technology is endangering your Privacy,* Jossey-Bass, San Francisco, 2006, pág. 6.

[55] El término se utilizó por primera vez en torno a 1988 por Mark Weiser. Ver su trabajo *The Computer for the 21st Century*, http://www.ubiq.com/hypertext/weiser/SciAmDraft3.html. Ver Reijo Aarnio, «Data Protection and New Technologies: «Ubiquitous Computing»», en Varios Autores, *Proccedings of the First European Congress on Data Protection. Madrid, 29-31 March 2006*, Fundación BBVA, Madrid, 2008, págs. 107 y ss. Asimismo Marc Langheinrich, «Privacy by Design-Principles of Privacy-Aware Ubiquitous Systems», 2001,

a permitir un seguimiento omnipresente de las personas mediante la interconexión de muy diferentes aparatos y sistemas, lo que a su vez permitirá obtener una información completa de aquéllas sin que tengan conciencia de ello. La nanotecnología permite ya elaborar dispositivos capaces de captar y elaborar información hasta extremos insospechados y de un modo totalmente desapercibido; tal es el caso de los llamados *roboflies*, o de los *nanobots*[56].

Los ejemplos podrían multiplicarse casi hasta el infinito, y muy bien podría decirse que cualquier situación o circunstancia imaginable es ya posible. Pese a resultar un lugar común citarlo en estos casos, es necesario rememorar de nuevo la famosa denuncia orwelliana del Gran Hermano que todo lo sabe y todo lo escruta, sin posibilidad de eludir su insaciable afán de vigilante omnipresente. Vuelve incluso a recuperarse la idea del *Panóptico*n de Jeremy Bentham, esa cárcel cuyo diseño permite al carcelero vigilar a todos los reclusos sin que estos sepan siquiera que están siendo observados, lo que haría de ellos dóciles sujetos, al saberse constantemente vigilados. Idea que más adelante teori-

---

en http://www.vs.inf.ethz.ch/res/papers/privacy-principles.pdf

[56] Clippinger, *A Crowd of one. The Future of Individual Identity*, Public Affaires, New York, 2007, págs. 28 y 32.

zó Michael Foucault[57] como forma de vigilancia constante y control social[58]. Se habla de la «vigilancia total»[59]. Algo que las nuevas tecnologías pueden hacer realidad[60]. Como Jeffrey Rosen ha señalado, estamos sometidos a una «mirada no deseada», que puede destruir nuestra privacidad[61].

No son simples *«horror stories»* sobre el carácter intrusivo de las nuevas tecnologías, sobre el uso y abuso de datos personales[62]. Son situaciones reales que deben hacernos reflexionar sobre cómo es nuestra vida en el

---

[57] *Vigilar y castigar*, Ed. Siglo XXI, México, 1976. A ello se ha referido también Daniel J. Solove, *The Digital Person. Technology and Privacy in the Information* Age, New York University Press, 2004, págs. 30-31.

[58] Vid. Bennett y Raab, *The Governance of Privacy. Policy Instruments in Global Perspective*, op. cit., págs. 16 y ss.

[59] Reg Whitaker, *The End of Privacy: how Total Surveillance is Becoming a Reality*, New Press, New York, 1999. Cit. por Bennett y Raab, op. ult. cit, pág. 338. Existe traducción al español de la obra de Whitaker: *El fin de la privacidad. Como la vigilancia total se está convirtiendo en realidad*, Paidos, 1999.

[60] Vid. David. H. Holtzman, *Privacy lost. How Technology is endangering your Privacy*, Jossey-Bass, San Francisco, 2006, págs. 265 y ss.

[61] J. Rosen, *The Unwanted Gaze. The Destruction of Privacy in America*, Vintage Books, New York, 2000.

[62] Vid. R. Smith, *War Stories: Accounts of Persons Victimized by Invasions of Privacy*, Privacy Journal, 1993. Cit. por Bennett y Rabb, *Governance of Privacy*…., op. cit., pág. 7.

entorno de las nuevas tecnologías: cómo es nuestra vida, nuestra libertad y nuestra felicidad tras la explosión digital, según han estudiado Abelson, Ledden y Lewis[63]. Se ha hablado de la muerte de la privacidad en el Siglo XXI[64]. Jon L. Mills se refiere a la privacidad como «el derecho perdido»[65] y Mauro Paissan llega más lejos: «la privacidad está muerta»[66]. El primero advierte de los innumerables riesgos que para la privacidad derivan de las «*More-Intrusive Tecnologies*»[67], con múltiples ejemplos, que sin embargo podrían multiplicarse.

Y lo preocupante no es ya que tales innovaciones tecnológicas invadan nuestra privacidad, sino que lo hacen pasando desapercibidas. No somos conscientes de lo que ello supone. Hablar ahora de las redes sociales sería fácil y apropiado. Se trata de un

---

[63] *Blown to Bits. Your Life, Liberty and Happines after the Digital Explosion,* Addison-Wesley, 2008. Se trata de un muy interesante libro con reveladoras reflexiones acerca del futuro que pueden depararnos las nuevas tecnologías.

[64] Simson Garfinkel, *Database Nation: the Death of Privacy in 21st Century*, O'Reilly Media, Sebastopol, California, 2001.

[65] J L. Mills, *Privacy. The Lost Right*, Oxford University Press, New York, 2008.

[66] *La Privacy è morta, viva la Privacy*, Ed. Ponte alle Grazie, Roma, 2009.

[67] Op. cit., pág. 29.

fenómeno que implica una pérdida inimaginable de privacidad. Que se alimenta además de un peligro extraordinariamente grave en relación con la situación que vengo exponiendo: el de considerar que todas esas medidas amenazantes para la privacidad del ser humano son no solo adecuadas, sino necesarias en la nueva sociedad del conocimiento, y que por tanto debemos aceptarlas no sólo resignada sino convencidamente. Medidas que poco a poco van incorporándose a nuestra vida cotidiana y que aceptamos como algo inevitable e incluso positivo. Se incorporan a nuestro moderno y normal modo de vida como un integrante más que ya ni se cuestiona.

2.- Protección de datos y seguridad[68].

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 ciudadana. Los terribles atentados del 11-S, así como los de Londres y Madrid, han modificado los standares de seguridad y las exigencias que de ello derivan, con riesgo en no pocas ocasiones para el ejercicio de

[68] Reitero ahora algunas reflexiones que ya he adelantado en *Seguridad, Transparencia y Protección de Datos. El futuro de un necesario e incierto equilibrio*, Fundación Alternativas, Madrid, 2009.

otros derechos, como es, señaladamente, la protección de datos de carácter personal.

La aprobación tras el 11-S de la *Patriot Act* en Estados Unidos ha venido seguida de la adopción de medidas restrictivas que inciden considerablemente en la protección de datos. Los llamados casos PNR[69] o Swift[70] 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 tensión entre seguridad y libertad. Pero también esa tensión se ha producido en el seno de Europa. La Directiva sobre retención de datos de telecomunicaciones[71] es prueba de ello. Por otra parte, cada vez se generaliza más la instalación de cámaras y videocámaras de modo que puede afirmarse que se corre el

---

[69] Cesión de datos de pasajeros a las autoridades aduaneras de Estados Unidos.

[70] 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.

[71] 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.

riesgo de estar sometidos a una vigilancia omnipresente.

En este escenario se plantea con especial intensidad la tensión entre protección de datos/intimidad y seguridad. Tensión que, una vez más, debe buscar el justo equilibrio valorando en todo caso el estricto respeto a los derechos fundamentales.

El derecho a la seguridad está reconocido en el art. 17.1 de la Constitución y ha sido reconocido por el Tribunal Europeo de Derechos Humanos[72]. 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 Europea de los Derechos Fundamentales reconoce que «toda persona tiene derecho a la libertad y a la seguridad». Los Estados tienen obligación de adoptar medidas dirigidas a proteger a los ciudadanos frente a la inseguridad[73]. Pero tales medidas han de ser respetuosas con los derechos fundamentales,

---

[72] Sobre ello vid. Comisionado para los Derechos Humanos del Consejo de Europa, *Protecting the Right to Privacy in the Fight Against Terrorism*, CommDH/Issue Paper 3, Strasburgo, 4-12-08, p. 12.

[73] Op. loc. Ult. cit. Vid *Guidelines on human rights and the fight against terrorism*, Adoptadas por el Comité de Ministros del Consejo de Europa, el 11-7-02, pág. 7.

y en particular con el de protección de datos. La STC 292/2000 ha resaltado que tales limitaciones han de estar previstas legalmente y deben ser 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 (como ha vuelto a señalar en su Sentencia 70/2009, como vimos más atrás). Según el Tribunal:

«9. *En cuanto a los límites de este derecho fundamental... 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…*

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 mar-

zo de 1987, §§ 47 y sigs.), 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)».

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 la seguridad del Estado) y las actividades del Estado en materia penal»[74]. La Directiva, pues, no se aplica ni en el ámbito del Segundo Pilar (Política Exterior y de Seguridad Común), ni en el del Tercer Pilar (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 o no 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 Tribu-

---

[74] El Considerando (43) de la Directiva dispone que «los Estados miembros podrán imponer restricciones a los derechos de acceso e información y a determinadas obligaciones del responsable del tratamiento, en la medida en que sean estrictamente necesarias para, por ejemplo, salvaguardar la seguridad del Estado, la defensa, la seguridad pública».

nal 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[75], 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

[75] *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).

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[76] 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[77]. En todos los casos se pone de relieve la importancia que en el intercambio de datos tiene el principio de disponibilidad, establecido en el Programa de La Haya. De modo que los datos no sólo podrán ser transmitidos entre los Estados miembros, sino que deben hacerse disponibles, sin obstáculos, para las autoridades competentes de los distintos Estados[78].

---

[76] DOUE C-53, de 3 de marzo de 2005.

[77] Instrumento de ratificación publicado en el *BOE* de 25 de diciembre de 2006. Entró en vigor en España el 1 de noviembre de 2006.

[78] Sobre dicho Tratado y la protección de datos, vid. Cristina Dietrich Plaza, «El Tratado de Prüm en el marco de la regulación de la protección de datos personales en la Unión Europea», en *Revista de Derecho Constitucional Europeo,* nº 7, Enero-Junio de 2007, págs. 31 a 64.

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*, fija las condiciones que deben ser en todo caso respetadas a la hora de intercambiar información en base al 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.

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 principios de información, de finalidad y de 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, ese 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 el tratamiento de datos esté previsto sea una finalidad precisa y legítima, y que los datos recabados sean utilizados exclusivamente para esa finalidad 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[79]) al analizar las iniciativas estadounidenses referentes a la recopilación de datos de pasajeros, conocida como PNR[80]. Iniciativas que ahora se pretenden aplicar en el seno de los países de la Unión Europea y que también ha 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*

---

[79] *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.

[80] 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, que ya he citado más atrás en el texto, pero no ha entrado en el fondo del asunto, pues sólo se ha centrado en cuestiones formales.

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 critica la propuesta por considerar que no justifica una necesidad apremiante de recogida de dato; es excesiva la cantidad de datos personales que deben transferir las compañías aéreas; la filtración de datos sensibles debería ser hecha por la persona responsable del tratamiento de los datos; el período de conservación de los datos es desproporcionado; 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; el gran margen de discreción concedido a los Estados miembros podría dar lugar a interpretaciones diversas de la Decisión marco, y el régimen de protección de datos de las transferencias que se realizarán a terceros países es poco claro. Concluyendo que 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.

Las anteriores son consideraciones que creo sirven para clarificar los términos de la relación entre protección de datos y seguridad. No se trata de renunciar ni a la una ni a la otra, sino de buscar el justo equilibrio entre ambos derechos, lo cual no siempre es fácil.

3.- Protección de datos y transparencia[81].

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, «Sunlight is said to be the best of disinfectants»[82], «la luz del sol es el mejor

---

[81] Algunas de las reflexiones y consideraciones siguientes las he adelantado ya Piñar y Mañas «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*, op. cit. págs. 66 y ss., y en *Seguridad, Transpaencia y Protección de Datos...*, op. cit.

[82] *Other Peoples's Money*, 1932. Puede consultarse en http://library.louisville.edu/law/brandeis/opm-ch5.html. La frase completa es: «Publicity is justly commended as a remedy for social and industrial diseases. Sunlight is said to be the best of disinfectants; electric

desinfectante». Cada vez con más insistencia se habla del derecho a conocer, del *right to know*[83].

Daniel J. Solove se ha preguntado: «How can the tension between transparency and privacy be reconciled? Must acces to public records be sacrificed at the altar of privacy? Or must privacy evaporate in order for government to be desinfected by sunlight?»[84].

Resulta en efecto imprescindible aclarar la relación existente entre transparencia y protección de datos[85], 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, pero sin olvidar

---

light the most efficient policeman. And publicity has already played an important part in the struggle against the Money Trust».

[83] Véase por ejemplo Thomas S. Blanton, «The World's Right to Know», en *Foreign Policy*, julio-agosto 2002, págs. 50 y ss.; Herbert N. Foerstel, *Freedom of Information and the Right to Know*, Greenwood Press, Westport, CT, 1999.

[84] *The Digital Person. Technology and Privacy in the Information Age*, New York University Press, 2004, pág. 150.

[85] A ello se ha referido el Tribunal de Justicia en su Sentencia de 20 de mayo de 2003, *Rundfunk y otros*, Asuntos C-465/00, C-138/01 y C-139/01, sobre la que más adelante volveré.

que una de las excepciones que pueden invocarse al ejercer el derecho de acceso es la derivada del derecho a la protección de datos o de la existencia de información o documentos que afecten a la intimidad de las personas[86], así como de información que afecte a la seguridad ciudadana. Westin ha señalado con acierto que «The modern totalitarian state relies on secrecy for the regime, but high surveillance and disclosure for all other groups... the democratic society relies on publicity as a control over government, and on privacy as a shield for group and individual life.»[87]

España es uno de los pocos países de la Unión Europea que carece todavía de una ley de transparencia o de acceso a la información[88]. El mandato contenido en el artículo

---

[86] Así, por ejemplo, en el Reglamento (CE) Nº 1049/2001, de 30 de mayo de 2001, relativo al acceso del publico a los documentos del Parlamento Europeo, del Consejo y de la Comisión.

[87] *Privacy and Freedom*, Atheneum, New York, 1967, pp. 23-25.

[88] Pese a la previsión del artículo 105 de la Constitución. Como es sabido, el acceso a archivos y documentos se regula fundamentalmente en el artículo 37 de la Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. Recientemente se han aprobado 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 (incorpora las Directivas

105 *b)* de la Constitución está todavía sin desarrollar. Pese a que el derecho a la transparencia se considera hoy un derecho fundamental. 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».

Pues bien, dicho lo anterior, es evidente que ni la transparencia ni la protección de datos son derechos absolutos. Es imprescindible conseguir un equilibrio entre ambos derechos[89].

2003/4/CE y 2003/35/CE) y 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.

[89] El IV Encuentro de Agencias Autonómicas de Protección de Datos, celebrado en Vitoria los días 23 y 24 de octubre de 2007, tuvo como tema central *Protección de Datos y acceso a la información. Un encuentro necesario entre derechos concurrentes*. La mayoría de las ponencias presentadas están disponibles en la Web de la Agencia Vasca de Protección de Datos: http://www.avpd.euskadi.net/s04-4319/es/

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 1999 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 del público a acceder a la información del sector público, y en este sentido el Grupo concluye que es necesario tener en cuenta los siguientes aspectos: a) 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.); b) principios de finalidad y legitimidad; c) información de la persona en cuestión; d) derecho de oposición de la persona en cuestión; utilización de las nuevas tecnologías para contribuir

al respeto del derecho a la intimidad[90]. Por su parte, el Supervisor Europeo de Protección de Datos, en su importante Documento *Public access to documents and data protection*[91] 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 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[92].

La Sentencia *Rundfunk*[93] señala que en el tratamiento de datos personales son de aplica-

---

[90] Dictamen 3/99, cit., pág. 12.

[91] Un resumen del Documento puede consultarse en Guichot «Acceso a la información en poder de la Administración y protección de datos personales», *Revista de Administración Pública*, núm. 173, mayo-agosto 2007, págs. 423 y ss.

[92] Sobre la Sentencia *Rundfunk* vid. Piñar Mañas, «El derecho a la protección de datos de carácter personal en la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas», op. cit., págs. 61 y ss.

[93] Que gira en torno a la posibilidad o no de hacer públicos, con los nombres de los afectados, ciertos

ción los principios relativos a la calidad de los datos (artículo 6 de la Directiva 95/46/CE) y a la legitimación del tratamiento (artículo 7), así como, en particular, el principio de finalidad y proporcionalidad[94]. 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 «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»»[95]. Dicho esto, afirma que la comunicación a terceros (aunque sea a una autoridad pública) de los datos relativos a las remuneraciones del personal

---

informes del equivalente al Tribunal de Cuentas, referidos, entre otros extremos, a las retribuciones de altos cargos de diversas entidades públicas.

[94] Apartados 65 y 66.

[95] Apartado 71.

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[96].

Sentado que la comunicación de datos a un tercero supone una injerencia en la vida privada, el Tribunal analiza si en el caso concreto tal injerencia 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[97], 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

---

[96] Apartado 74 de la Sentencia. El Tribunal trae a colación la Sentencia del TEDH Amann c. Suiza, de 16 de febrero de 2000, § 70.

[97] Apartado 81.

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[98]. 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

[98] Apartados 85 y 86.

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»[99]. A la misma conclusión llega el Tribunal al analizar la cuestión a la luz de la Directiva 95/46/CEE[100].

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 intere-

---

[99] Apartado 90.

[100] «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.

sados 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 en base al Reglamento (CE) nº 1049/2001, del Parlamento y del Consejo de 30 de mayo de 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»[101]. 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:

[101] Apartado 123 de la Sentencia.

el asunto controvertido entra en el ámbito de aplicación del Reglamento 1049/2001 que 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 perjuicio o no de que afectasen a la intimidad de los interesados. Por ello 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»[102], 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.

---

[102] Apartado 132.

El análisis caso a caso se impone. Sin embargo es necesario resaltar una cuestión de relevante importancia: para conseguir ese equilibrio es imprescindible contar con un marco normativo que regule la protección de datos y que defina el alcance de la transparencia y el acceso a la información. Y hay que decir, como ya apunté más atrás, que la situación en este punto deja mucho que desear en España. La ausencia de una ley de transparencia, además de facilitar la corrupción, impide contar con un marco que defina la relación entre ambos derechos: protección de datos y acceso a la información. De esta manera, en muchas ocasiones la falta de transparencia se ampara en la falta de normativa adecuada y en consecuencia en la falta de un título legal suficiente que permita el tratamiento de datos (el acceso a la información implica un tratamiento de datos) sin consentimiento de los afectados. Hasta el punto de que se ha llegado a decir con razón que la legislación de protección de datos está instrumentalizándose para negar por parte de no pocas Administraciones Públicas el acceso a la información[103].

---

[103] El Defensor del Pueblo Europeo ya llamó la atención hace tiempo sobre la amenaza que para la transparencia podía suponer un mal entendimiento de los fines y límites de la protección de datos. Así en su carta de noviembre de 2001 sobre *Openness and data protection* (http://www.europarl.europa.eu/ombudsman/letters/en/20011114-1.htm). Recientemente (Conferencia en los

En conclusión, pues, la aprobación de una ley de transparencia y acceso a la información en España es una asignatura pendiente que ya no admite demoras.

4.- Garantía del derecho a la protección de datos y globalización.

Voy concluyendo. Ante la realidad de que los ataques a la privacidad trascienden con mucho las fronteras físicas, es imprescindible alcanzar un modelo global de protección de datos[104]. A ello se han referido, por ejemplo, Colin J. Bennett y Charles D. Raab en su obra *The Governance of privacy. Policy Instruments in Global Perspective*[105]. La XXVII Conferencia Internacional de Autoridades de Protección de Datos de 2005 iba en esa dirección,

---

Cursos de Verano de la Universidad de Málaga, 18 de julio de 2008), Carlos Lesmes, Presidente de la Sala de lo Contencioso-administrativo de la Audiencia Nacional (competente para conocer de los recursos que se interpongan contra las resoluciones de la Agencia Española de Protección de Datos) ha señalado que «si todo lo envolvemos en el secreto por la protección de datos estamos vulnerando otras libertades». Actualmente, ha señalado, «hay un cierto exceso en el tema de la protección de datos», por lo que «hay que encontrar un equilibrio» entre tal derecho y la transparencia.

[104] Jon L. MILLS también lo ha señalado: «Intrusions are becoming truly global, and remedies must be global as well»: *Privacy. The Los Right*, op. cit., pág. 301.

[105] The Massachusetts Institute of Technology Press, 2006.

y en ella se aprobó una Declaración Final sobre «*The protection of personal data and privacy in a globalised world: a universal right respecting diversities*»[106]. En la XXVIII Conferencia (Londres, 2006) se adoptó la

---

[106] La Conferencia se celebró en Montreux, Suiza, los días 13 a 15 de septiembre de 2005. En la Declaración Final se hace una referencia a los principios que deberían regir a nivel global el derecho a la protección de datos:

16. «Recognising that the principles of data protection derive from international legal binding and non binding instruments such as the OECD Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, the United Nations Guidelines concerning Computerized Personal Data Files, the European Union Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data and the Asia Pacific Economic Cooperation Privacy Framework,

17. Recalling that these principles are in particular the following:

- Principle of lawful and fair data collection and processing,
- Principle of accuracy,
- Principle of purpose-specification and -limitation,
- Principle of proportionality,
- Principle of transparency,
- Principle of individual participation and in particular the guarantee of the right of access of the person concerned,
- Principle of non-discrimination,
- Principle of data security,
- Principle of responsibility,
- Principle of independent supervision and legal sanction,

llamada *London Initiative*; la XXX (Estrasburgo, 2008) tuvo como tema *Protecting Privacy in a Borderless World* y la próxima, la XXXI, que se celebrará en Madrid en este año 2009, analizará, entre otros, el tema «*Hacia una regulación global de la privacidad: propuestas y estrategias*». La Declaración Final del VI Encuentro de la Red Iberoamericana de Protección de Datos (Cartagena, Colombia, 2008) tiene por título «*Un compromiso para alcanzar estándares internacionales de protección de datos y privacidad*».

Ya sólo las anteriores referencias son de por sí elocuentes acerca de la trascendencia de la perspectiva global. Así lo exige, como decía más atrás, el hecho de que las nuevas tecnologías, intrusivas para la privacidad, no conocen de fronteras. Pero así lo exige también la necesidad de contar con unos standares o principios generales de protección de datos que permitan el flujo transnacional de información con plenas garantías para tal derecho fundamental.

Los esfuerzos por contar con instrumentos eficaces para luchar a nivel global contra las amenazas que se ciernen sobre la privacidad no son pocos. De hecho, la mayoría de los

---

- Principle of adequate level of protection in case of transborder flows of personal data».

pasos que en la evolución del derecho a la protección de datos se han dado han venido de la mano de instrumentos internacionales[107]. Desde Naciones Unidas a la Unión Europea, el Consejo de Europa, la OCDE, la Comunidad Iberoamericana o APEC. Los objetivos, en este sentido, serían dos. Por un lado llegar a la posible aprobación de unos principios o standares comunes, a nivel internacional, que permitiesen fijar criterios comunes de protección de la privacidad. Por otro, alcanzar a nivel bilateral o multilateral compromisos de colaboración para luchar eficazmente contra las amenazas de la privacidad[108].

En estos momentos hay dos modelos que aparentemente pugnan entre sí: el americano y el europeo, pero que son mucho más cercanos de lo que podría parecer. En realidad se nutren de principios muy semejantes, y comparten orígenes también cercanos, que giran en torno a la idea de autodeterminación o *self-determination* respecto de la información personal, como ya expuse más atrás. Sin duda, la

---

[107] Ver James B. Rule y Graham Greenleaf (Eds.) *Global Privacy Protection: The First Generation*, Edward Elgar Publishing, Northampton, 2009.

[108] Por ejemplo, el llamado *London Action Plan*, para luchar contra el Spam, o el *Memorandum of Undersatnding* suscrito entre la Federal Trade Commission y la Agencia Española de Protección de Datos en 2005, con el mismo objetivo.

Directiva 95/46/CE ejerce un papel de claro protagonismo en el escenario de la privacidad, y la necesidad de obtener la declaración de adecuación en materia de protección de datos está reforzando su posición. Pero el reto es de una envergadura innegable: ¿qué principios de protección de datos? ¿A través de qué instrumentos? ¿Cómo pueden hacerse efectivos? ¿Es necesaria una autoridad internacional de tutela y control de protección de datos? Desde luego las dudas son muchas, y las respuestas no fáciles. Así, por ejemplo, mientras en Estados Unidos se prefiere un modelo basado en la autorregulación, en los códigos de conducta, en las buenas prácticas, en Europa se ha optado claramente por la heterorregulación y por la consideración de la protección de datos como un verdadero derecho fundamental. Mientras que en Estados Unidos no se considera necesaria la existencia de una autoridad independiente de tutela de la protección de datos (sin perjuicio de la existencia de Agencias Independientes con competencias sectoriales que inciden de forma directa en la protección de datos, como la Federal Trade Commission al proteger los derechos e intereses de los consumidores), en Europa tal existencia se ha elevado a principio esencial del derecho, recogido incluso en el artículo 8º de la Carta Europea de Derechos Fundamentales, como ya sabemos.

Mientras tanto, las transferencias internacionales de datos no sólo no pueden pararse, sino que cada vez son más intensas. Para facilitarlas garantizando al mismo tiempo plenas garantías para la protección de datos, se ponen sobre la mesa nuevas herramientas, como las llamadas *Binding Corporate Rules*, Reglas Corporativas Vinculantes, que permitirían el intercambio internacional de datos en el seno de grupos multinacionales sin necesidad de acudir a la vía del consentimiento de los afectados o de las relaciones contractuales multilaterales. Tema éste que está en primera línea y que ha merecido múltiples opiniones del Grupo de Trabajo del Artículo 29[109]. Como el de las cláusulas contractuales tipo en las transferencias internacionales de responsable a responsable, de responsable a encargado o de responsable o encargado a subencargado[110].

En fin, parece llegada la hora de acometer esa reflexión ya inaplazable acerca de la privacidad en un mundo globalizado. Europa

---

[109] Los documentos pueden localizarse en http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/

[110] Ver, del Grupo de Trabajo, la «Opinion 3/2009 on the Draft Commission Decision on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC *(data controller to data processor)*», de 5 de marzo de 2009, WP 161.

está por un lado exportando, con notable éxito, su modelo de protección de datos. Pero siguen siendo mayoría los países no europeos que carecen de leyes de protección de datos y el principio de territorialidad de la aplicación de las leyes (que no del tratamiento de datos, que es, como he reiterado, ajeno al territorio) amenaza con debilitar notablemente el nivel de protección de la privacidad. Por eso se impone un diálogo entre la regulación normativa y la autorregulación, entre la protección de datos como derecho fundamental (algo a lo que Europa no puede en ningún caso renunciar) y como criterio para el tratamiento de datos y compromiso por parte de quienes los manejan. Diálogo que ha de extenderse al que, como hemos ya señalado, ha de darse entre protección de datos y transparencia, protección de datos y seguridad, protección de datos y nuevas tecnologías. Es mucho lo que nos jugamos.

PABLO LUCAS MURILLO DE LA CUEVA. Es Magistrado del Tribunal Supremo y catedrático de Derecho Constitucional. Ha publicado diversos trabajos sobre el derecho a la protección de datos personales desde su monografía *El derecho a la autodeterminación informativa* (1990).

JOSÉ LUIS PIÑAR MAÑAS. Es Catedrático de Derecho Administrativo de la Universidad CEU-San Pablo de Madrid. *Adjunct Professor of Law* de la Georgetown University (2005-2007). Premio San Raimundo de Peñafort, de la Real Academia de Jurisprudencia y Legislación. Entre otros libros es autor de *Las relaciones entre el Estado y las Regiones. La experiencia italiana* (1986), *Scientific Research in Spain. Essays on Constitutional, Administrative and Financial Problems*, (coeditor con Andrea Orsi Battaglini, 1992), *Derecho de Fundaciones y voluntad del Fundador* (junto con Alicia Real Pérez, 2000), *¿Existe la Privacidad?*, (2008), y, como Director, *El Tercer Sector en Iberoamérica. Fundaciones, Asociaciones y ONGs* (2001), *Protección del medio ambiente y desarrollo sostenible* (2002), *Protección de Datos en Iberoamérica* (2005).

LIBROS PUBLICADOS

1. Robert Alexy: *Derechos sociales y ponderación*

2. Luigi Ferrajoli, José Juan Moreso, y Manuel Atienza: *La teoría del derecho en el paradigma constitucional*

3. Alfonso Ruiz Miguel y Rafael Navarro-Valls: *Laicismo y Constitución*

4. Pietro Costa y Benito Aláez Corral: *Nacionalidad y ciudadanía*

5. Víctor Ferreres y Juan Antonio Xiol: *El carácter vinculante de la jurisprudencia*

6. Michele Taruffo, Perfecto Andrés Ibáñez y Alfonso Cadau Pérez: *Consideraciones sobre la prueba judicial*

7. Roberto Romboli y Marc Carrillo: *Los consejos de garantía estatutaria*

8. Pedro Salazar Ugarte, Josep Aguiló Regla y Miguel Ángel Presno Linera: *Garantismo espurio*

9. Eugenio Bulygin, Manuel Atienza y Juan Carlos Bayón: *Problemas lógicos en la teoría y práctica del Derecho*

10. Pablo Lucas Murillo de la Cueva, José Luis Piñar Mañas: *El derecho a la autodeterminación informativa*

Próximas publicaciones:

Stefan Huster, Antonio Pau y María J. Roca: *Estado y cultura*

Paolo Comanducci, Mª Ángeles Ahumada y Daniel González Lagier: *Positivismo jurídico y neoconstitucionalismo*

Francisco J. Laporta, Juan Ruiz Manero y Miguel Ángel Rodilla: *Certeza y predecibilidad de las relaciones jurídicas*