

LA PROTECCIÓN DE LOS DATOS DE CARÁCTER PERSONAL EN EL HORIZONTE DE 2010

PABLO LUCAS MURILLO DE LA CUEVA
Magistrado del Tribunal Supremo
Catedrático de Derecho Constitucional

Resumen: Al cumplirse diez años de la entrada en vigor de la Ley Orgánica de Protección de los Datos de Carácter Personal son notables los progresos que se han producido en términos normativos e institucionales. Destaca, en efecto, el reconocimiento como derecho fundamental del que protege los datos personales y la creación de autoridades encargadas de velar por su respeto. No obstante, también permanecen las dificultades y han aparecido otras nuevas. Entre ellas debe tenerse en cuenta la tendencia a relativizar el alcance de este derecho, bien mediante modificaciones legislativas que rebajen los niveles de protección, bien mediante prácticas que vengán a traducirse en una menor exigencia en el cumplimiento de las normas. Sin embargo, los riesgos para las personas que llevaron al reconocimiento de este derecho fundamental no sólo permanecen sino que se han agravado como consecuencia del progreso tecnológico. Por eso, es preciso no olvidar su contenido esencial y, singularmente, las facultades de autodeterminación individual. Al mismo tiempo, sin renunciar al fomento del respeto a las normas que lo garantizan, ha de enfatizarse la responsabilidad de quienes tratan información personal, en especial de los poderes públicos, y la importancia del más pleno cumplimiento de la Ley.

Palabras clave: datos personales, autodeterminación, protección, consentimiento, finalidad, calidad.

Abstract: Ten years after the promulgation of the Spanish Data Protection Act, there is been a remarkable progress in terms of statutory and institutional aspects. First of all, personal data protection has been

recognized as a fundamental right and also it has been established the authorities to implement it. However, it remains some difficulties from the past and appeared other new ones. Among others, we have to be in mind the tendency to make relative the scope of the right by means of changes in the legislation to reduce the level of protection, or through practices that comes to reduce to a lower demand in the fulfillment of the law. Moreover, as a consequence of the technological progress the risks remain and become worse. So it is necessary to bear in mind its essential content and, particularly, the faculties of individual self-determination. At the same time, without to give up the encouragement of the respect of the law, it is necessary to emphasize the responsibility to the ones that treat personal data, in particular the public institutions and the importance of the fullest compliance with current legislation.

Keywords: Personal data, self-determination, protection, consent, purpose, quality.

Próximo a cumplirse el décimo aniversario de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, parece éste un buen momento para hacer algunas reflexiones sobre su aplicación y sobre los problemas con que han de enfrentarse quienes pretenden hacerla valer. Téngase en cuenta que a ese período ha de añadirse el que transcurrió bajo la vigencia de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD), y que el momento fundamental que representaron las sentencias del Tribunal Constitucional 292 y 290, de 30 de noviembre de 2000, también se ha ido alejando en el tiempo.

Su transcurso parece haber dejado atrás preocupaciones y debates de quienes se aproximaron al estudio del artículo 18.4 de la Constitución. De la incertidumbre provocada por su falta de desarrollo legislativo durante más de una década fuimos pasando a una situación caracterizada por la producción de diversas normas estatales, autonómicas y europeas que trajeron regulaciones generales desde las que desembocamos, ya con instituciones, estatal, autonómicas y europea, creadas específicamente para proteger nuestros datos personales, en la identificación del derecho fundamental que subyace a las previsiones de ese precepto constitucional. A partir de ese momento y de forma paralela al creciente proceso de regulación de aspectos de la sociedad de la información y de las tec-

nologías de la información y de las comunicaciones, se han ido introduciendo salvedades o especialidades encaminadas a preservar, bien la seguridad pública, bien la actividad económica que descansa en la utilización de datos de carácter personal¹.

Asimismo, la dimensión universal que han alcanzado las relaciones sociales gracias a las redes que superan las fronteras estatales ha llevado a buscar soluciones también universales para hacer efectiva la protección de datos de carácter personal. Precisamente, está anunciada cuando se escriben estas líneas una Conferencia Internacional de las Autoridades de Protección de Datos y Privacidad que se celebrará en Madrid, bajo los auspicios de la Agencia Española de Protección de Datos los días 4 a 6 de noviembre de 2009² con la vista puesta en lograr la aprobación de unas reglas comunes que aseguren un marco mínimo compartido internacionalmente³ y permitan, si no conjurar, al menos reducir significativamente los obstáculos que a la efectividad de la protección de datos opone el carácter universal de las redes de comunicaciones y de la llamada sociedad de la información.

Mientras todo esto ha ido sucediendo los problemas a los que desde el primer momento se han tenido que enfrentar, primero, quienes reivindicaban la articulación de una protección jurídica contra el acopio y la utilización incontrolados de datos personales por terceros y, después, aquellos a quienes se ha encomendado la responsabilidad de aplicar las normas en las que se ha ido plasmando esa garantía han permanecido.

Esos problemas son, entre otros, el desconocimiento que la mayor parte de las personas tienen sobre los peligros derivados del acceso por terceros a los datos que les identifican o permiten identificarlos cuando no afectan directamente a su vida íntima. Ignorancia que les lleva a no adoptar las cautelas que sí observarían si fueran conscientes de los resultados a que puede conducir la utilización de esa información y a no reaccionar frente a su utilización irregular. La relativa complejidad del lenguaje utilizado por el legislador, tributario en buena parte de ter-

¹ Sobre ese periplo, véase Pablo Lucas Murillo de la Cueva y José Luis Piñar Mañas, *El derecho a la autodeterminación informativa*. Fundación Coloquio Jurídico Europeo, Madrid, 2009.

² Se trata de la 31ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad. La información sobre la misma se halla en www.privacyconference2009.org

³ Propuesta Conjunta para la Redacción de Estándares Internacionales para la Protección de la Privacidad en relación con el tratamiento de Datos de Carácter Personal.

minologías y expresiones procedentes de directivas europeas, no es una ayuda para superar esta dificultad. Como tampoco lo es la tendencia de parte de los especialistas y de las instituciones de garantía a servirse de conceptos difíciles de comprender para la mayor parte de las personas.

El desconocimiento no es algo exclusivo de los ciudadanos. Se extiende a instituciones públicas y privadas que disponen de amplios volúmenes de información personal y, a veces, va acompañado por un escaso celo, cuando no despreocupación, en la aplicación de las normas legales y reglamentarias que la protegen. Esa circunstancia, sin duda preocupante, es más llamativa cuando de los poderes públicos se trata, por su vinculación positiva a la Ley y al Derecho y resulta aún más alarmante dada la próxima entrada en funcionamiento de la llamada Administración Electrónica⁴. A ello se añade, en estrecha relación, la colosal magnitud de la tarea puesta en manos de las autoridades creadas para proteger los datos personales. Magnitud directamente proporcional a la falta de conciencia social sobre los presupuestos del derecho a la protección de datos de carácter personal. La dimensión planetaria de estos problemas aporta dificultades adicionales de enorme entidad a las que se han recordado.

En estas condiciones, aunque se han producido avances significativos en el plano de la educación y de la información, son todavía muy escasos los logros y a pesar de que las estadísticas de las autoridades estatal y autonómicas de protección de datos reflejan incrementos extraordinarios en sus actividades --ya sean de información, orientación, promoción, inspección o sanción⁵-- lo cierto es que su tarea, sustancialmente confirmada por los tribunales de justicia, llega a una pequeña parte del inmenso espacio en el que tienen que actuar y, como es natural, tiende a guiarse por criterios pragmáticos. Es decir, aquellos que les permiten alcanzar con los medios de que disponen --desde luego no proporcionados a los problemas a que tienen que enfrentarse-- mejores resultados. Pero esa opción por el pragmatismo ya supone reconocer que en muchos aspectos no están en condiciones de atajar conductas o actuaciones contrarias al derecho a la protección de datos personales.

⁴ Según la disposición final tercera, tres de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, a partir del 31 de diciembre de 2009, los ciudadanos podrán ejercer el derecho a relacionarse por medios electrónicos con la Administración.

⁵ Las respectivas memorias pueden consultarse en www.agpd.es las de la Agencia Española de Protección de Datos; [www.madrid.org.apdem](http://www.madrid.org/apdem) las de la Agencia de Protección de Datos de la Comunidad de Madrid; en www.apdcat.net las de la Agencia Catalana de Protección de Datos; y en www.avpd.euskadi.net las de la Agencia Vasca de Protección de Datos.

Por otro lado, junto a las exigencias de la seguridad pública ante la utilización de las tecnologías de la información y de las comunicaciones para la comisión de delitos, ya sea por delincuentes comunes o por organizaciones terroristas, exigencias que llevan a imponer límites que afectan, entre otros derechos fundamentales, al que protege los datos personales, nos encontramos con que, cada vez más, el valor económico de la información personal impulsa a empresas de las más diversas características a hacerse con ella y utilizarla, bien para desarrollar sus actividades bien para suministrarla, a otras elaborada de diferentes formas.

Este aspecto de la realidad económica incide también en otros planos, según se ha podido comprobar con ocasión del debate establecido entre la Unión Europea y los Estados Unidos a propósito de la información personal que se ha de facilitar a las autoridades norteamericanas sobre quienes viajen en avión a ese país y, en general, respecto de las condiciones en que cabe autorizar movimientos internacionales de datos desde Europa a Estados Unidos. Hasta ahora, todo parece apuntar a que van prevaleciendo los puntos de vista norteamericanos que confían más en formas de autorregulación que en normativas jurídicas hechas valer por los poderes públicos⁶.

La combinación de todos estos factores conduce a un escenario que, no es, ciertamente, el ideal y que puede llevar, incluso, a que nos preguntemos si, a estas alturas, este derecho que hemos incluido en el catálogo de los derechos fundamentales, se corresponde con esa naturaleza o, si, pasada la novedad que supuso su regulación y reconocimiento, no está experimentando un proceso de relativización, que le está vaciando de buena parte de su contenido. Da la impresión, en efecto, de que nos encontramos en un momento especialmente importante.

Desde que se aprobó la Ley Orgánica 5/1992, la LORTAD hasta hoy no ha variado el núcleo esencial sobre el que se ha ido construyendo el

⁶ Véase la Decisión de la Comisión Europea de 26 de julio de 2000 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América. Diario Oficial de las Comunidades Europeas de 25 de agosto de 2000. Sobre las formas de autorregulación, véase Diana Sancho Villa, "Normas corporativas vinculantes (binding corporate rules): aspectos sustantivos y de cooperación internacional de autoridades", en Revista Española de Protección de Datos, nº 4/2008, págs. 35 y sigs.

sistema jurídico de protección de datos personales. Se han producido algunas modificaciones, sobre todo las que aportó la vigente Ley Orgánica 15/1999 so pretexto de acomodar nuestra legislación a la Directiva europea 95/46 CE, pero fuera de algunos extremos discutibles a los que se hace mención más adelante, la disciplina legal ha permanecido sin cambios. Sobre todo, en lo relativo a las premisas o condiciones que hacen lícito el tratamiento de datos personales --es decir, el consentimiento del afectado o la autorización por la ley-- y a los principios de protección de datos. Así, hemos visto cómo se han proyectado esas reglas básicas y principios hacia diversos ámbitos sectoriales en los que se han establecido las excepciones y particularidades consideradas necesarias. Incluso, se advierte como los nuevos estatutos de autonomía lo incluyen entre los derechos de los que se ocupan, si bien a propósito de su ámbito competencial.

En este escenario de despliegue normativo pero de sustancial estabilidad de sus contenidos, la jurisprudencia se ha caracterizado, en general, por hacer valer los elementos más garantistas del régimen jurídico de la protección de datos. No de otro modo debe entenderse el pronunciamiento del Tribunal Constitucional de las sentencias 292 y 290, ambas de 30 de noviembre de 2000⁷, que da carta de naturaleza entre los derechos fundamentales al de protección de datos personales anclándolo en el artículo 18.4 de la Constitución. Ni tampoco las sentencias de las Salas de lo Contencioso Administrativo de la Audiencia Nacional y de los Tribunales Superiores de Justicia o las dictadas por la Sala Tercera del Tribunal Supremo a propósito de la actuación de las Agencias de Protección de Datos⁸.

La tendencia a valorar crecientemente este derecho fundamental ha discurrido en paralelo al proceso experimentado en la Unión Europea y, también, en la doctrina del Tribunal Europeo de Derechos Humanos. Si este último lo ha encuadrado con perfiles propios en el seno del artículo 8 del Convenio de Roma, en el ordenamiento comunitario ha alcanzado

⁷ Que, por otra parte, representan la culminación de una serie de sentencias precedentes --con alguna excepción-- que ya dejaban entrever el reconocimiento del derecho fundamental a la protección de datos que las citadas en el texto llevaron a cabo. Se menciona primero la n^o 292 porque es en ella donde el Tribunal Constitucional construye el concepto y define el contenido de ese derecho.

⁸ En la obra coordinada por Carlos Lesmes Serrano, *La Ley de Protección de Datos. Análisis y comentario de su jurisprudencia*. Lex Nova, Valladolid, 2008, se aprecia esa orientación, sobre todo en lo que se refiere a la interpretación de las reglas sobre el consentimiento, al juego del principio de finalidad o a la especial tutela de los datos sensibles.

un estatuto singular desde el momento en que lo ha recogido la Carta de los Derechos Fundamentales de la Unión Europea⁹.

Ahora bien, el despliegue de las regulaciones legislativas y el reconocimiento al máximo nivel normativo de esta figura parece haber supuesto una suerte de punto de inflexión. Es como si, logrado ese objetivo de la positivación del derecho fundamental, las energías desplegadas para alcanzarlo se hubieran agotado y, en su lugar, apareciera una dinámica animada por intereses de variada naturaleza y dirigida a perfilar en términos restrictivos aquellos aspectos de la disciplina legal que dejan márgenes a la interpretación. Entre otras, las apelaciones a la seguridad pública¹⁰ y a la dimensión económica de los datos personales¹¹, se afirman frente a los espacios de autodeterminación que el ordenamiento jurídico ha puesto en manos de los afectados. Lo cual, por lo demás, viene a coincidir con las dificultades que en la práctica supone velar por el respeto de las previsiones legales y reglamentarias.

Son perfectamente comprensibles las complicaciones de todo tipo que supone llevar a la realidad las previsiones de cualquier ley. Mucho más lo son las que trae consigo esa operación cuando la proyección de las normas es tan general como en este caso y, sobre todo, cuando es necesario establecerlas no sólo en el interior de los Estados, sino, especialmente, a nivel internacional para evitar que en la complejidad de la sociedad red se sorteen las garantías jurídicas por el simple proceder de operar desde dentro de las fronteras de un ordenamiento que no protege este derecho.

Desde esa perspectiva es igualmente lógico que quienes tienen la principal responsabilidad de velar por la protección de los datos personales --las autoridades que con diversas denominaciones se han ido creando por las leyes que la regulan-- insistan en la importancia de la información y de la educación, que valoren los códigos de buenas prácticas y la autorregulación, en definitiva, confíen especialmente en cuanto fomente actitudes conscientes de la relevancia de la información personal y en la necesidad de respetar en su utilización los derechos de los afectados.

⁹ A la que el artículo 1 del Tratado de Lisboa --modificando para ello el artículo 6 del Tratado de la Unión Europea-- atribuye el mismo valor jurídico que los tratados.

¹⁰ Por ejemplo, las introducidas por la Ley Orgánica 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y de redes públicas de comunicaciones.

¹¹ El mejor ejemplo lo ofrece la misma Directiva 95/46 CE y su preocupación por asegurar la circulación de información personal, ciertamente, en el respeto a los principios y derechos que enuncia. El artículo 14 del Reglamento de desarrollo de la Ley Orgánica 15/1999 también refleja esa sensibilidad por facilitar a las empresas la realización de tratamientos de datos al admitir el consentimiento tácito.

En esa línea se sitúan aquellas aproximaciones que enfatizan la necesidad de que los poderes públicos y los sujetos privados implicados --desde los fabricantes de *hardware* y *software* hasta los consumidores-- cooperen en la consecución del respeto efectivo a la autodeterminación informativa. Por esas líneas discurre la teorización sobre la *gobernanza de la privacy*¹².

No obstante, una cosa es el pragmatismo y la preocupación por la eficiencia y otra distinta la reducción de los niveles estrictamente jurídicos de tutela. Es decir, no es lo mismo perseguir el respeto a las normas que establecen los derechos de los afectados ante quienes pretenden servirse de sus datos personales por vías que promueven o estimulan en términos positivos su más amplio cumplimiento, que rebajar el contenido de esos derechos en sí mismos considerados. Sobre lo primero poco hay que señalar ya que no supone ninguna novedad: la promoción del respeto voluntario a las normas jurídicas mediante la enseñanza de los bienes que protegen no es algo privativo de este derecho fundamental. Por otra parte, está claro que cuando las autoridades creadas para garantizarlo subrayan la utilidad de ese enfoque, de ningún modo pretenden hacer dejación de sus restantes responsabilidades y, en particular, de la persecución de las infracciones y de la sanción a los responsables de las mismas.

El verdadero problema es cualitativo y puede venir --aunque no necesariamente-- de la mano del pragmatismo. Es el que surge cuando, en el marco del contraste entre los intereses en juego, se intente saldar el ajuste entre los que asisten a las personas a quienes pertenece la información y los de quienes la quieren tratar en beneficio de estos últimos, llevando a las normas ese desequilibrio o imponiéndolo en su interpretación. En efecto, entre el reconocimiento de las dificultades que conlleva la aplicación de las leyes, cuando no de la simple imposibilidad de hacerlo, y la rebaja de sus contenidos garantistas media un gran paso. No obstante, son conocidas las apetencias de diversos sectores económicos por la información personal y la incidencia que han tenido sus puntos de vista en la elaboración de la vigente Ley Orgánica 15/1999, como pone de manifiesto la lectura de las actas que recogen los debates parlamentarios. Por eso, el riesgo de que a la flexibilización de las normas le acompañen intentos de imponer interpretaciones, so pretexto de realismo, restrictivas no es irreal.

¹² Así, Colin Bennett *The Governance of Privacy*, escrito con Charles Raab. MIT Press, 2006.

En este sentido, no debe olvidarse la secuencia que se ha producido en la peripecia histórica de los derechos de la llamada primera generación¹³. La que lleva desde su reivindicación por quienes, al necesitarlos para satisfacer sus necesidades básicas, los reclaman hasta su conversión, una vez que han entrado en el ordenamiento jurídico, en categorías formales desprovistas de la sustancia que justificó su reconocimiento. Aunque el contexto en el que surgió la crítica al carácter meramente formal de las libertades burguesas y el que tiene ante sí el derecho a la protección de datos personales no es el mismo, no deja de ser cierto que siempre que se positiviza un derecho o una institución se produce su incorporación a un conjunto en el que les rodean otros derechos e instituciones que los delimitan y con los que pueden entrar en conflicto. Dejan, pues, de ser absolutos y se transforman, como todos los derechos e instituciones, en categorías circunscritas dentro de unos confines cuya determinación puede, en ocasiones, ser difícil, pero que no dejan de existir por esa razón.

No es, pues, desconocida la hipótesis de la devaluación de los derechos en general ni, vistas las particulares circunstancias que acompañan al derecho a la protección de datos en particular, está excluido que la padezca.

Y, sin embargo, las amenazas a la dignidad, a la identidad, a la libertad y a la intimidad de las personas que justifican este derecho y explican su recepción en las Constituciones, en las leyes y en la jurisprudencia no han desaparecido. Al contrario, todo apunta que se han incrementado exponencialmente de la mano de las posibilidades crecientes que ofrece la tecnología, entre las que destaca la facilidad creciente de establecer sistemas de videovigilancia que se hacen, ya no con datos personales más o menos desagregados, sino con imágenes de los afectados en los ámbitos más variados: domicilio, trabajo, vía pública, establecimientos comerciales, lugares de ocio, etc¹⁴. O los mecanismos que, incorporados a documentos de identidad, hacen posible el seguimiento y localización de individuos¹⁵ y, naturalmente, la definitiva superación de la protec-

¹³ Antonio Enrique Pérez Luño, *Los derechos fundamentales*. Tecnos, Madrid, 2007.

¹⁴ Colin Bennett insiste en el peligro de la videovigilancia en su obra, *The Privacy Advocates: resisting the spread of surveillance* MIT Press, 2008.

¹⁵ Es el caso de los sistemas miniaturizados de identificación por radiofrecuencias (conocidos por sus siglas en inglés RFID: *radio frequency identification*) que pueden incorporarse a documentos de identidad, pasaportes, permisos de conducir, tarjetas de crédito o etiquetas de productos comerciales.

ción que en otro tiempo y respecto de otros peligros podían ofrecer las fronteras estatales. Por tanto, el panorama no ha cambiado. Si acaso, ha empeorado desde el punto de vista de los riesgos que acechan a la capacidad de autodeterminación informativa de las personas ya que el entorno global es más hostil.

En este contexto, la conclusión a la que se debe llegar, una vez que se ha reconocido el derecho fundamental a la protección de datos, no puede ser otra que la del fortalecimiento de la tutela que aporta a los individuos y la insistencia en su contenido sustantivo. Para ello, son, sin duda, muy importantes cuantos esfuerzos se hagan desde las instituciones llamadas directamente a preservarlo para imponer su respeto, bien por las vías del fomento y el acuerdo, bien por las de la coacción. E, igualmente, son especialmente valiosas las iniciativas dirigidas a extender a escala universal unos niveles mínimos de protección de los datos que reduzcan los inconvenientes derivados del actual estado de la cuestión, caracterizado porque en la Unión Europea y, en particular, en algunos de sus Estados miembros están vigentes regímenes más exigentes que los establecidos fuera de ella, allá donde existen.

No obstante, tales actuaciones no son suficientes. Además, es preciso volver sobre los aspectos esenciales de este derecho y, en particular, sobre las fuentes que legitiman los tratamientos y los principios que le inspiran. Es decir, sobre los elementos que son más genuinamente característicos de este derecho fundamental. A este respecto, conviene mencionar un reciente estudio que reconstruye el proceso que ha llevado al reconocimiento del derecho a la protección de datos y lo relaciona con la evolución experimentada por la concepción de los otros del artículo 18 de la Constitución¹⁶. Más allá de sus reflexiones sobre su fundamentación y, en general, sobre la de los derechos fundamentales, interesa resaltar que, al distinguir los aspectos principales de ese desarrollo, subraya como, desde una inicial configuración esencialmente negativa de tales derechos, se ha pasado a otra principalmente positiva que se distingue, en lo que ahora importa, porque sitúa en el poder de control de la información personal el elemento característico del que descansa en el artículo 18.4 de la Constitución.

¹⁶ Se trata del discurso de ingreso en la Real Academia de Ciencias Morales y Políticas pronunciado el 18 de noviembre de 2008 por Andrés Ollero Tassara. *De la protección de la intimidad al poder de control sobre los datos personales. Exigencias jurídico-naturales e historicidad en la jurisprudencia constitucional*. Real Academia de Ciencias Morales y Políticas, Madrid, 2008.

Ese poder, la capacidad de autodeterminación informativa que comporta, tiene que estar en el centro de las preocupaciones que suscita este derecho fundamental y eso no siempre se percibe con la debida claridad. Del mismo modo que no siempre se aprecia que, a la postre, las consideraciones sobre tratamientos, cesiones, ficheros, accesos, movimientos internacionales, códigos-tipo, ... todas ellas tienen sentido en la medida en que hacen referencia a datos de personas identificadas o identificables. Ni que del respeto a las normas jurídicas que han regulado todos esos extremos depende que los titulares de esa información no sólo vean preservada efectivamente su capacidad de decisión, sino, también, que puedan, gracias a ella, evitarse perjuicios e incomodidades que no tienen por qué soportar.

Pues bien, al volver la vista sobre el sujeto del derecho y sobre el núcleo de las facultades que comporta se advierten algunos elementos que no son coherentes con cuanto se acaba de decir.

En efecto, lo primero que ha de traerse a colación a propósito del derecho a la protección de datos personales es el consentimiento. Se halla en el centro del mismo. El consentimiento y las causas en virtud de las cuales se puede prescindir de él a la hora de realizar determinados tratamientos, así como los límites de la autorización que comporta ese consentimiento. Límites materiales, temporales y teleológicos que han de ser mantenidos en sus justos y proporcionados términos sin que puedan entenderse con tal amplitud que vengan a vaciar de contenido las facultades del afectado.

No obstante y pese a decir la Ley 15/1999 en su artículo 6.1, que el consentimiento ha de ser inequívoco, el artículo 14 del Reglamento permite el que simplemente se presume. Lo uno no parece coherente con lo otro. Del mismo modo, si el consentimiento para el tratamiento de datos personales determinados y concretos se limita a la finalidad para la que se hayan solicitado y el respeto al principio de finalidad es uno de los elementos objetivos del sistema de protección establecido por el legislador y continuado por la jurisprudencia constitucional, no parece coherente que se deje la puerta abierta a su utilización para fines distintos con tal de que no sean incompatibles. Interpretación ésta que se apoya en el artículo 4.2 de la Ley Orgánica 15/1999 y busca su fundamento en la Directiva 95/46 CE pero que no encaja en el sistema de dicho texto legal, no sólo porque el legislador exige el consentimiento inequívoco para los tratamientos de datos que no procedan de fuentes accesibles al público, sino porque pugna con el principio de interpretación más favorable a

los derechos fundamentales y con el que el mismo artículo 4, pero en su apartado 4, obliga a cancelar los datos que hayan dejado de ser necesarios o pertinentes para la finalidad para la que fueron recogidos.

Abierto el camino de la relativización del derecho mediante la redefinición a la baja de sus elementos esenciales y con independencia de que los efectos de los mencionados cambios puedan ser contrarrestados efectivamente en el curso de la aplicación de las normas y de su control jurisdiccional, no deben descartarse intentos ulteriores. La creciente complejidad que la extensión de las regulaciones protectoras y su diversificación traen consigo y la indicada tendencia a manejar un lenguaje en exceso técnico y especializado pueden facilitar en la medida en que dificulten la percepción del verdadero alcance de eventuales modificaciones normativas o de propuestas de actuación en la materia.

El momento es, pues, particularmente importante y requiere, junto a la realización del balance de lo conseguido, el diseño de un planteamiento de futuro comprometido con la más plena realización del derecho. Planteamiento que prescinda de todo lo que pueda significar pérdida de calidad o disminución de la protección de los datos personales que los poderes públicos deben asegurar y, en cambio, enfatice la responsabilidad que les corresponde a la hora de promover ellos mismos, empezando por su propia actuación, el respeto a las normas que la establecen. Y la responsabilidad de quienes se sirven de datos personales en el desarrollo de actividades lícitas o de cualquier manera intervienen en las operaciones relacionadas con su tratamiento para que dicha utilización se mantenga --además de en el respeto a las restantes previsiones normativas-- en los límites de la autorización que la ha hecho posible y no corra el riesgo de desembocar en perjuicios para los afectados a quienes corresponden los datos.

Es cuestión, sencillamente, de seguir tomando en serio este derecho fundamental para garantizar que, junto a los restantes constitucionalmente reconocidos, suministre a las personas los medios jurídicos que precisan para asegurar la satisfacción de sus necesidades básicas. En este caso, las de no verse sometidas a un escrutinio integral de todos los aspectos de sus vidas y a no sufrir perjuicios a causa del uso incontrolado por terceros de los datos que les conciernen.