

EL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE LOS DATOS DE CARÁCTER PERSONAL EN LA CONSTITUCIÓN EUROPEA

María del Carmen Guerrero Picó*

SUMARIO

- 1.- Introducción.
- 2.- La protección de los datos de carácter personal en el ámbito comunitario.
- 3.- Los datos personales en los tratamientos realizados por las instituciones comunitarias.
- 4.- La tutela de la información personal en el tercer pilar.
- 5.- El art. 8 de la Carta de los derechos fundamentales.
- 6.- Los arts. I-51 y II-68 de la Constitución europea.
- 7.- Recapitulación.

1. INTRODUCCIÓN

Con el nacimiento y el (espectacular) desarrollo de las nuevas tecnologías de la información y la comunicación se aprecia, amén de indudables ventajas, una tendencia al registro masivo de datos concernientes a la vida privada de los individuos. Esta información, tratada posteriormente, ayuda a crear perfiles, a clasificar a la persona a que se refiere, a proporcionar nuevos datos acerca de ella, a tomar decisiones que le afectan justificadas únicamente en razón de tal tratamiento, etc. Pues bien, las posibilidades de que quien trata datos personales intente interferir en el normal desenvolvi-

* Doctora en Derecho. Miembro del Servicio de Estudios de la Corte Constitucional italiana.

miento de nuestras relaciones personales, profesionales, financieras o/y comerciales son más reales de lo que en principio podríamos imaginar.

Todas estas razones coadyuvan al nacimiento del derecho fundamental a la protección de los datos de carácter personal, derecho de la llamada tercera generación, uno de los exponentes del conflicto tecnología-Derecho y cuya razón de ser reside en dar al individuo la posibilidad efectiva de disponer y controlar los datos que le conciernen.

El Tratado por el que se instituye una Constitución para Europa incluye dos artículos dedicados al derecho fundamental a la protección de datos: el art. I-51, dentro del título que se dedica a la vida democrática de la Unión y referido específicamente a los tratamientos realizados en el ámbito institucional y, algunas páginas más adelante, en la Carta de los Derechos Fundamentales de la Unión, el art. II-68, donde se proclama de forma genérica que toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.

Para comprender los pros y los contras del modo en que la Constitución Europea acoge este derecho fundamental y por qué lo hace por partida doble, comenzaré exponiendo, de forma sintética debido a razones evidentes de espacio, cuál es el tratamiento jurídico que la protección de los datos personales ha recibido en la Unión Europea. Hasta el momento, las normas que tutelan el derecho del individuo a controlar y disponer de su información personal no son las mismas para todos los pilares de la Unión y ello ha condicionado la forma en que el derecho fundamental objeto del presente estudio se ha manifestado finalmente en la Carta Magna europea.

2. LA PROTECCIÓN DE LOS DATOS DE CARÁCTER PERSONAL EN EL ÁMBITO COMUNITARIO

2.1. De los primeros pasos del Parlamento Europeo y la Comisión a Schengen

Siguiendo la estela marcada por el Consejo de Europa, organismo que ex art. 8 CEDH protegerá tempranamente este derecho fundamental, en la esfera comunitaria se abrió pronto el debate sobre la adopción de medidas concretas para frenar los abusos que podían producirse tanto en el sector público como en el privado al tratar información personal. En 1973 un documento interno de la Comisión refleja la inquietud que, con respecto a los derechos de las personas, suscita el empleo de la informática y contempla la necesidad de alcanzar un consenso político que evite futuras divergencias

legislativas entre los Estados miembros¹. Igualmente, desde el Parlamento Europeo (quizás la institución más comprometida en la defensa de este derecho fundamental) se interpela al Consejo de las Comunidades Europeas sobre la protección de la vida privada de los ciudadanos comunitarios².

A partir de este momento y hasta el comienzo de la década de los ochenta se sucederán otras iniciativas de diversa envergadura. Así, por citar algún ejemplo: a) la Resolución del Parlamento Europeo de 21 de febrero de 1975³, sobre la protección de los derechos de la persona ante el desarrollo de los progresos técnicos en el ámbito de la informática que, basándose en el Informe Mansfield de la Comisión Jurídica, alienta a adoptar una directiva sobre libertad individual e informática, al objeto de asegurar a los ciudadanos comunitarios la mejor protección frente a abusos en el tratamiento de sus datos y de evitar la elaboración de legislaciones nacionales contradictorias. b) La creación, el 18 de mayo de 1977, de la Subcomisión "Informática y derechos de la persona" en el seno de la Comisión Jurídica del Parlamento. c) La Resolución de 8 de mayo de 1979 del Parlamento, sobre la protección de los derechos de la persona ante el desarrollo de los progresos técnicos en el ámbito de la informática⁴ donde, tomando como referencia esta vez el Informe Bayerl, se constata que la regulación de la protección de datos puede incidir directamente en la instauración y funcionamiento del mercado común, perturbando la competencia⁵. d) La Recomendación de la Comisión de 29 de julio de 1981, relativa al Convenio del Consejo de Europa sobre protección de las personas con respecto al tratamiento automatizado de datos de carácter personal⁶. Este Convenio del Consejo de Europa, el número 108 de 28 de enero de 1981, es el primer instrumento jurídico internacional contraído con vocación universal en el ámbito de la protección de datos y, junto a otros textos dictados en la época por la Organización para la Cooperación y el Desarrollo Económico (como

¹ SEC (73) 4300 final, "Una política comunitaria de informática", párrafo 39.

² Question orale núm. 193/73 avec debat de M. Cousté au nom du groupe des démocrates européens de progrès au Conseil des Communautés européennes (JO núm. C 40, de 08/04/1974, p. 21).

³ JO núm. C 60, de 13/03/1975, p. 48.

⁴ JO núm. C 140, de 5/06/1979, p. 34.

⁵ HEREDERO HIGUERAS ha destacado que, de haberse desarrollado con más detalle algunos aspectos de las recomendaciones dadas a la Comisión y al Consejo sobre los principios que debían inspirar las normas comunitarias, se habría podido disponer desde ese momento de una propuesta de directiva. Vid. La Directiva comunitaria de protección de los datos de carácter personal, Aranzadi, Pamplona, 1997, p. 19.

⁶ JO núm. L 246, de 29/08/1981. Ed. especial en español: capítulo 16, tomo 1, p. 77.

las Líneas directrices que han de regir en lo concerniente a la protección de la vida privada y los flujos transfronterizos de datos de carácter personal, de 23 de septiembre de 1980), tiene una indudable relevancia a nivel europeo⁷. Por ello la Comisión sugiere a los Estados miembros ratificarlo antes de terminar 1982. e) La Resolución del Parlamento de 9 de marzo de 1982, sobre la protección de los derechos de la persona ante el desarrollo de los progresos técnicos en el ámbito de la informática⁸, etc.

No obstante, siendo clara la necesidad de elaborar un texto propio —una directiva— sobre protección de datos de carácter personal, se abrirá un período de impasse que no cesará sino años más tarde.

Mientras tanto, el 14 de junio de 1985 Alemania, Bélgica, Francia, Holanda y Luxemburgo adoptan un acuerdo relativo a la supresión gradual de controles en las fronteras comunes, el Acuerdo de Schengen, y el 19 de junio de 1990, su Convenio de aplicación. El acervo Schengen concierne, además de al control del cruce de fronteras interiores y exteriores, a las peticiones de asilo y a la cooperación policial y judicial penal, a un sistema de información común. Ni la libre circulación de personas, ni la abolición de las fronteras ni, en definitiva, el desarrollo del mercado interior pueden alcanzarse a costa de generar un considerable déficit de seguridad; se requiere, por tanto, la adopción de ciertas medidas compensatorias y entre ellas está la creación del Sistema de Información Schengen (en adelante, SIS)⁹.

Regulado en el título IV del Convenio de aplicación, el SIS se compone de dos partes: una nacional, en cada uno de los Estados partícipes e idénticas entre sí, y una unidad de apoyo técnico, cuya gestión recae sobre Francia. Las autoridades designadas por las Partes podrán consultar este sistema de redes informáticas, que incluye datos concernientes a: personas buscadas para su detención a efectos de extradición, nacionales de países terceros que estén incluidos en la lista de no admisibles en un Estado

⁷ La madurez actual del sistema jurídico europeo de protección de datos también es deudora de las valiosas aportaciones hechas por el Consejo de Europa y la OCDE, contribuciones que, en no pocas ocasiones, fueron fruto de la mutua colaboración entre las tres organizaciones.

⁸ JO núm. C 87, de 05/04/1982.

⁹ Para profundizar en la incidencia de dicho sistema en la protección de datos personales véase L.S. ROSSI, "La protezione dei dati personali negli accordi di Schengen alla luce degli standards fissati dal Consiglio d'Europa e dalla Comunità europea", en B.NASCIMBENE, *Da Schengen a Maastricht: apertura delle frontiere, cooperazione giudiziaria e di polizia*, Giuffrè, Milán, 1995 y A. SÁNCHEZ BRAVO, "La protección de los datos personales en la Europa de Schengen", en ID, núm. 12-15, 13-14, 1996, pp. 1401-1459.

Schengen, personas desaparecidas, testigos y personas citadas para comparecer ante las autoridades judiciales, personas o vehículos registrados a efectos de vigilancia y objetos buscados con vistas a su incautación o como pruebas en un procedimiento penal. En lo que respecta a las personas, las categorías de datos cuyo registro se permite son: el nombre y los apellidos (en su caso, también los alias, pero registrados por separado), los rasgos físicos particulares, objetivos e inalterables, la primera letra del segundo nombre, la fecha y el lugar de nacimiento, el sexo, la nacionalidad, la indicación de si están armadas o son violentas, el motivo de la inscripción y la conducta que debe observarse. No se autorizan más anotaciones, en particular las referidas a los datos sensibles a los que alude el art. 6 del Convenio número 108 del Consejo de Europa, esto es, aquéllos que revelen origen racial o estén referidos a opiniones políticas, convicciones religiosas o similares, salud, vida sexual y condenas penales.

Sin ser ésta la única referencia que sobre la materia se puede encontrar en el Convenio, los arts. 102-118 articulan el elenco de garantías que protegen a las personas concernidas frente a la recogida, tratamiento y transmisión de sus datos de carácter personal en el marco del SIS. Más allá de imponer ciertas medidas de seguridad al responsable que trata la información, se consagran los principios de exactitud, actualidad, licitud, limitación temporal y adecuación a los fines perseguidos y se reconocen los derechos de acceso, rectificación y cancelación del afectado, si bien contemplándose un amplio número de excepciones no siempre justificadas y que, redactadas de manera indeterminada, no permiten asegurar la proporcionalidad de tales salvedades.

Por otra parte, el Convenio de aplicación crea la Autoridad de Control Común Schengen, compuesta por dos representantes de cada autoridad nacional de control. Es la encargada de verificar que las tareas encomendadas a la unidad de apoyo técnico del SIS se llevan a cabo de conformidad con lo dispuesto en el Convenio de aplicación Schengen, el Convenio número 108 del Consejo de Europa, la Recomendación del Comité de Ministro del Consejo de Europa nº R (87) 15, de 17 de septiembre, dirigida a regular la utilización de datos de carácter personal en el sector de la policía y el Derecho nacional de cada Parte.

Con todo, las garantías creadas en este específico ámbito para salvaguardar los derechos de las personas concernidas son insuficientes. Las competencias de la Autoridad de Control son bastante limitadas (elaborará propuestas de solución de los problemas que detecte) y tampoco se asegura un control externo del SIS, ya fuera realizado por el Parlamento Europeo o por el Tribunal de Justicia de la Comunidad Europea (en adelante, TJCE),

como encontraremos que sucede con casi todo lo relacionado con el tercer pilar de la Unión Europea.

2.2. La Directiva 95/46/CE

La dinámica del mercado interior, dentro del cual se garantiza la libre circulación de mercancías, personas, servicios y capitales, implica también la libre circulación de datos de carácter personal de un Estado a otro. La utilización de tratamientos de datos desde el sector económico privado es cada vez más demandada y lo mismo cabe decir del ámbito de la cooperación administrativa, científica y técnica. Pese a todo, las diferencias jurídicas en la regulación que cada Estado ha comenzado a hacer de esta materia obstaculiza fatídicamente ese flujo transfronterizo, por lo que la necesidad de armonizar (que no homogeneizar) las legislaciones nacionales en materia de protección de datos de carácter personal se transforma en un imperativo para las instituciones comunitarias. Las negociaciones se retoman a finales de los ochenta, alcanzándose posteriormente un acuerdo¹⁰.

La Directiva del Parlamento Europeo y del Consejo 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de sus datos de carácter personal y a la libre circulación de estos datos (en adelante, Directiva 95/46/CE)¹¹ es, pues, una herramienta para impedir las

¹⁰ El 18 de julio de 1990 la Comisión presenta al Consejo la primera propuesta de directiva, el COM (90) 314-SYN 287 y 288, de 24/09/1990. Dicho proyecto, fuertemente influenciado por las leyes federal alemana (sobre todo) y francesa, despierta de inmediato recelos. No satisface, v. gr., la dualidad de régimen jurídico impuesta al tratamiento público o privado de los datos, ni el modo en que se regula el consentimiento al tratamiento de la persona concernida. También hay dudas acerca de la competencia de la Comunidad para normar un ámbito en el que están implicados derechos fundamentales.

En julio de 1992, visto el dictamen del Parlamento Europeo, la Comisión presenta una nueva propuesta, el COM (92) 422 final (DO núm. C 311, de 27/11/1992), donde se aprecia la supresión de la distinción entre tratamiento público y privado; que el consentimiento tiene una menor incidencia a la hora de determinar la licitud del tratamiento; se introduce el concepto "tratamiento" en vez de hacer girar las normas en torno al de "fichero" (más restringido); se da la posibilidad de eximir de la notificación a determinados tratamientos o de simplificar sus trámites, etc. Atendidas las indicaciones hechas por los Estados y el Parlamento Europeo, el texto se conseguirá aprobar.

¹¹ DO núm. L 281, de 23/11/1995, p. 31. Véanse también el Primer informe sobre la aplicación de la Directiva sobre protección de datos (95/46/CE), COM (2003) 265 final, de 15 de mayo, y la Resolución del Parlamento Europeo, de 9 de marzo de 2004, <Titre>sobre el primer informe sobre la aplicación de la Directiva sobre protección de datos (95/46/CE).

Sobre esta directiva vid., por todos, D. ALONSO BLAS, "El futuro de la protección de datos a nivel europeo", en M.A. DAVARA RODRÍGUEZ (Coord.), Encuentros sobre Informática

trabas a la libre circulación de información personal en el contexto del mercado interior; el modo de evitar que la defensa de los derechos fundamentales se torne en freno para los objetivos de la integración económica, eludiendo por demás el inconveniente de que dicha tutela sea argüida por las Administraciones nacionales para falsear la competencia e incumplir los cometidos que les atribuye el Derecho comunitario. No es, como el Convenio número 108 del Consejo de Europa, un instrumento orientado directamente a la protección de los derechos de las personas, si bien es evidente que indirectamente conseguirá el objetivo menos crematístico de asegurar un elevado nivel de protección de la vida privada en la esfera comunitaria. Reflejo de todo ello es el art. 1 de la Directiva: “1. Los Estados miembros garantizarán, con arreglo a las disposiciones de la presente Directiva, 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 los datos personales. 2. Los Estados miembros no podrán restringir ni prohibir la libre circulación de datos personales entre los Estados miembros por motivos relacionados con la protección garantizada en virtud del apartado 1”.

El ámbito de aplicación de la norma comunitaria es más restringido que el del Convenio número 108 del Consejo de Europa. La Directiva se aplica al tratamiento total o parcialmente automatizado de datos personales e, igualmente, al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero (art. 3.1). El soporte en que se consignan los datos personales no es, pues, lo más relevante. A sensu contrario, quedan excluidos: los tratamientos realizados en ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario (v. gr. las de los títulos V y VI del TUE); los tratamientos de datos cuyo objeto sea la seguridad pública (v. gr., video-vigilancia policial), la defensa y la seguridad del Estado (incluido el bienestar económico de éste cuando dicho tratamiento esté relacionado con la seguridad del mismo), las actividades del Estado en materia penal y los tratamientos hechos por las perso-

y Derecho (1995-1996), Aranzadi, Pamplona, 1996, pp. 163-176; M. HEREDERO HIGUERAS, La Directiva comunitaria de protección..., op. cit.; J.M. PRIETO GUTIÉRREZ, “La Directiva 95/46/CE como criterio unificador”, Poder Judicial, núm. 48, 1997, pp. 165-233; A.A. SÁNCHEZ BRAVO, La protección del derecho a la libertad informática en la Unión Europea, Universidad de Sevilla, Sevilla, 1998, pp. 125-162; A. VIGURI PEREA, “Intimidación versus informática (La protección de datos de carácter personal: perspectiva desde el derecho comparado)”, La Ley, Tomo de Jurisprudencia 2/1999, pp. 1886-1900; y A.I. HERRÁN ORTIZ, El derecho a la intimidad en la nueva Ley Orgánica de Protección de Datos Personales, Dykinson, Madrid, 2002, pp. 115-194.

nas físicas en el ejercicio de actividades exclusivamente personales o domésticas (art. 3.2).

Precisamente el capítulo de excepciones ha sido fuente de algunos conflictos interpretativos, relacionados por demás con la elección de la base jurídica de la Directiva, que fueron estudiados en 2003 por el Tribunal de Justicia de la Comunidad Europea (en adelante, TJCE)¹². La STJCE de 20 de mayo de 2003 resuelve los asuntos C-465/00 (Rechnungshof contra Österreichischer Rundfunk) y los asuntos acumulados C-138/01 y C-139/01 (Neukomm y Lauer mann contra Österreichischer Rundfunk). Los jueces austriacos plantearon al TJCE si entraban en el campo de aplicación de la Directiva 95/46/CE algunas disposiciones de la Ley federal constitucional sobre la limitación de la retribución de funcionarios públicos. Ésta obliga a recoger datos sobre los ingresos de ciertos empleados de sociedades y entidades públicas, con el fin de incluirlos (indicando el nombre de las personas afectadas), en el informe anual del Tribunal de Cuentas, destinado a ser hecho público. En la STJCE de 6 de noviembre de 2003, que da respuesta al asunto C-101/01 (Göta hovrätt contra Bodil Lindqvist), la duda surgía a propósito de la aplicación de la Directiva a una página web personal, creada por una catequista sueca, en la que ésta había incluido datos personales de sus compañeros.

En las conclusiones presentadas a los dos casos, el Abogado General afirma que ambas situaciones quedan fuera del ámbito de aplicación de la Directiva 95/46/CE¹³. En el primero, porque esa actividad atañe a la política presupuestaria nacional, no regulada a nivel comunitario sino competencia de los Estados miembros, y en el segundo, porque se trata de una actividad no económica y la Comunidad Europea no tiene competencia para dictar normas en materia de derechos fundamentales. El art. 100 A TCE (actual art. 95 TCE) no puede invocarse como el fundamento de medidas que no encuentran su justificación en el objetivo de promover “el establecimiento y el funcionamiento del mercado interior”.

Los argumentos aportados por el TJCE en la sentencia de mayo salvaron los inconvenientes señalados. Según el TJCE, el recurso a la base

¹² Vid. P.A. DE MIGUEL ASENSIO, “Avances en la interpretación comunitaria sobre protección de datos personales”, *La Ley*, núm. 5964, 27/02/2004, pp. 1-4.

¹³ Conclusiones del Abogado General Sr. A. TIZZIANO presentadas el 14/11/2002 (asunto C-465/00 y asuntos acumulados C-138/01 y C-139/01) y el 19/09/2002 (asunto C-101/01).

En la doctrina española apoya las tesis del Abogado General, cuestionando la base jurídica de la Directiva, RUIZ MIGUEL (“El derecho a la protección de los datos personales en la Carta de Derechos Fundamentales de la Unión Europea: análisis crítico”, *RDCE*, núm. 14, Enero-Abril 2003, pp. 7-43).

jurídica del art. 100 A TCE no presupone la existencia de un vínculo efectivo con la libre circulación entre los Estados miembros en cada una de las situaciones contempladas por el acto que se funda en ella. Lo trascendente es que dicho acto tenga efectivamente por objeto la mejora de las condiciones de establecimiento y funcionamiento del mercado interior (parágrafo 41)¹⁴. De este modo, “la aplicabilidad de la Directiva 95/46 no puede depender de la cuestión de si las situaciones concretas de que se trata en los asuntos principales tienen un vínculo suficiente con el ejercicio de las libertades fundamentales garantizadas por el Tratado y, en particular en los referidos asuntos, con la libre circulación de los trabajadores. En efecto, una interpretación contraria podría hacer que los límites del ámbito de aplicación de la referida Directiva se vuelvan particularmente inciertos y aleatorios, lo que sería contrario al objetivo esencial de ésta, que es la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros con el fin de eliminar los obstáculos al funcionamiento del mercado interior derivados precisamente de las disparidades entre las legislaciones nacionales” (parágrafo 42).

Se reafirma el Tribunal en esta posición en su sentencia de noviembre (parágrafos 40 y 41), donde, a su vez, limita el alcance de las excepciones del art. 3.2, resultando que las actividades citadas en el primer guión (actividades previstas por las disposiciones de los títulos V y VI TUE y tratamientos que tengan por objeto la seguridad pública, la defensa, la seguridad del Estado y las actividades del Estado en materia penal) son “en todos los casos, actividades propias del Estado o de las autoridades estatales y ajenas a la esfera de actividades de los particulares” y sólo se aplica a aquellas actividades que se mencionan expresamente o que pueden incluirse en la misma categoría (parágrafos 43 y 44). Y las del segundo guión son actividades exclusivamente personales o domésticas (parágrafo 46). En consecuencia, el TJCE concluye que la obligación de suministrar al Tribunal de Cuentas austriaco el nombre e ingresos de las personas ligadas al sector público que perciben un determinado sueldo y la inclusión de datos personales en una página web personal entran en el ámbito de aplicación de la Directiva 95/46/CE. Cuestión distinta será, y así deberán apreciarlo los órganos jurisdiccionales nacionales, si en el caso austriaco se cumplen los requisitos que permiten limitar legítimamente el derecho fundamental a la protección de datos personales (los del art. 8.2 CEDH) o, en el caso sueco,

¹⁴ Vid. también los Asuntos Alemania contra Parlamento y Consejo, de 05/10/2000, *British American Tobacco (Investments) e Imperial Tobacco*, de 10/12/2002.

cómo ha de resolverse el conflicto entre el derecho a la protección de datos y el derecho de creación artística o la libertad de expresión.

2.2.a) Principios y derechos de la persona concernida

Los principios que como mínimo deben acoger las normas nacionales en materia de protección de datos personales están bastante detallados en la Directiva 95/46/CE y son los siguientes:

1) Principios relativos a la calidad de los datos (art. 6). La Directiva parte de que todo tratamiento ha de adecuarse al principio de lealtad y licitud. Después especifica que la recogida de datos personales debe responder a fines determinados, explícitos y legítimos y que éstos no podrán ser tratados posteriormente de manera incompatible con tales fines. La STJCE de 20 de mayo de 2003 ha declarado el efecto directo del art. 6.1,c), que es el que atiende a estos extremos. Un particular puede invocarlos ante los órganos jurisdiccionales nacionales para evitar la aplicación de normas de Derecho interno contrarias a dichas disposiciones.

Por otra parte, los datos no se conservarán durante más tiempo que el preciso para realizar los fines que motivaron la recogida o tratamiento (limitación que no afecta a los datos almacenados con fines históricos, estadísticos o científicos). Transcurrido ese lapso, no se conservarán en forma que permita identificar al individuo.

Ligado a lo anterior está el principio de proporcionalidad de la información. Exige que la información personal sea adecuada, pertinente y no excesiva con relación a los fines del tratamiento. En este sentido, los datos deberán ser exactos y estar actualizados para que en cada momento respondan con fidelidad a la realidad del sujeto. De no cumplirse esta previsión, se prevé un procedimiento de rectificación o cancelación de los mismos.

2) Principios relativos a la legitimación del tratamiento de los datos de carácter personal (art. 7). Son varias las condiciones que, concurriendo, nos permiten hablar de un tratamiento legítimo: a) que el interesado preste su consentimiento inequívoco (expreso o tácito); b) que el tratamiento sea necesario para la ejecución de un contrato en el que el interesado sea parte o bien para la aplicación de medidas precontractuales adoptadas a petición de éste; c) que sea preciso para cumplir una obligación jurídica a la que esté sujeto el responsable del tratamiento; d) que se requiera para proteger el interés vital del interesado; e) que deba hacerse para cumplir una misión de interés público o inherente al ejercicio del poder público conferida al responsable del tratamiento o a un tercero a quien se comuniquen los datos; f) que sea preciso para la satisfacción del interés legítimo perseguido por el res-

ponsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos (v. gr. los ficheros de solvencia y morosidad), siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado.

El TJCE declaró en mayo de 2003 el efecto directo de los derechos consagrados en los apartados c) y e) del art. 7.

3) Especial protección para el tratamiento de ciertas categorías de datos (art. 8). Los datos que revelan el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos o aspectos referidos a la salud o la sexualidad, calificados de “sensibles”, son merecedores de una mayor protección en atención a que pudieran ser el fundamento de decisiones discriminatorias o especialmente perjudiciales para sus titulares. Su tratamiento está prohibido, aunque la regla admite numerosas salvedades.

Excepcionalmente, podrán tratarse si: a) el interesado prestó su consentimiento explícito (a no ser que lo prohíba la legislación nacional); b) el tratamiento tenga que realizarse para respetar las obligaciones y derechos específicos del responsable del tratamiento en materia de Derecho laboral (si se prevé en la legislación y con las garantías adecuadas); c) el tratamiento es requerido para salvaguardar el interés vital del interesado u otra persona (v. gr. si él está física o jurídicamente incapacitado); d) el tratamiento se efectúa en el curso de sus actividades legítimas y con las debidas garantías por una fundación, asociación o cualquier organismo sin fin de lucro cuya finalidad sea política, filosófica, religiosa o sindical, siempre que concierna exclusivamente a sus miembros o personas que mantengan contactos regulares con ellas (no obstante, no se cederán a terceros sin consentimiento de los titulares); e) se tratan datos que el interesado haya hecho manifiestamente públicos o es algo necesario para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial. La prohibición general tampoco operará en contextos relacionados con la salud: cuando el tratamiento se deba a la prevención o el diagnóstico médico, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios. Y será así cuando se realice por un profesional sanitario sujeto al secreto profesional o una persona ligada a una obligación equivalente. A la vez, la Directiva deja la puerta abierta a los Estados para establecer un régimen más amplio de excepciones. Están autorizados a hacerlo, implantando las garantías adecuadas, a través de su legislación o mediando una decisión de su autoridad de control. Su proceder habrá de estar motivado por significativas razones de interés público y deberán notificarlo a la Comisión.

La norma comunitaria alude específicamente a otros dos tipos de datos:

a) los relativos a infracciones, condenas penales o medidas de seguridad. Su tratamiento estará sometido al control de la autoridad pública, mas podrá realizarse por otros sujetos si hay previstas garantías específicas en el Derecho nacional y el Estado no lo impide. El registro completo de las condenas penales sólo puede efectuarse bajo el control de los poderes públicos y queda a la voluntad de los Estados miembros someter a ese control a los datos relativos a sanciones administrativas o procesos civiles.

b) Los números de identificación. No se prohíbe la existencia de un número nacional o similar de identificación de los ciudadanos; serán los Estados quienes fijen las condiciones en que éste podrá ser objeto de tratamiento.

4) Tratamientos realizados con fines periodísticos, de expresión artística o literaria (art. 9). La norma comunitaria no ignora el conflicto que pudiera darse entre la protección de datos y otros derechos fundamentales, por lo que indica a los Estados que podrán establecer excepciones al régimen general si los datos son tratados con fines periodísticos, de expresión artística o literaria. Las excepciones "sólo" versarán sobre las disposiciones de los capítulos II (condiciones generales de licitud de los tratamientos), IV (transferencias internacionales) y VI (autoridad de control), prácticamente todo el sistema protector de la Directiva.

5) Confidencialidad y seguridad del tratamiento (arts. 16 y 17). Constituye una importante medida de control de los tratamientos restringir el acceso a los datos personales a sus encargados o a terceros que actúen bajo instrucciones del responsable del tratamiento o por imperativo legal.

El responsable del tratamiento está obligado a aplicar las medidas técnicas y de organización adecuadas para proteger los datos personales contra su destrucción (accidental o ilícita), su pérdida, alteración, difusión o acceso no autorizados (en particular cuando haya una transmisión de datos dentro de una red) y contra cualquier otro tratamiento ilícito. Las medidas de protección y las obligaciones de seguridad que conciernen al responsable del tratamiento se hacen extensivas al encargado del mismo, que habrá de estar vinculado a aquél por medio de un contrato.

Todos estos principios deben ser cumplidos por el responsable del tratamiento con independencia de que éste sea consentido por la persona concernida. El centro de gravedad del sistema protector instaurado por la Directiva 95/46/CE se desplaza a las condiciones de licitud del tratamiento, a diferencia de la propuesta de directiva de 1990, que daba mayor relevancia al papel jugado por el consentimiento.

En otro orden de consideraciones, la Directiva 95/46/CE determina que deben reconocerse los siguientes derechos a las personas concernidas:

1) El derecho a ser informado, tanto si los datos se obtienen del titular como si no (arts. 10 y 11). Este derecho es primordial para el correcto funcionamiento del sistema de protección de datos pues difícilmente se podrán ejercer derechos como el de acceso u oposición al tratamiento si el individuo no ha obtenido una previa información de ciertos extremos.

Salvo que hubiera sido informada con anterioridad, el responsable del tratamiento o su representante deberán advertir a la persona de quien recaben sus datos de: a) su identidad (la de ambos); b) los fines del tratamiento; c) suplementariamente, cuando sea preciso para garantizar un tratamiento leal de los datos, comunicarán, por ejemplo: quiénes son los destinatarios o las categorías de destinatarios de los datos, el carácter obligatorio o no de su respuesta más las consecuencias de una negativa a ella y la existencia de los derechos de acceso y rectificación.

En la hipótesis de que los datos no se recabaran del interesado, la obligación de informar procede, en idénticos términos, desde el momento del registro de los datos o, cuando se piensen comunicar a un tercero, en el momento de la primera comunicación. No es preciso informar (adoptando las garantías pertinentes) si se trata de un tratamiento con fines estadísticos o de investigación histórica o científica, cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados o el registro o la comunicación a un tercero estén expresamente prescritos por ley.

2) Los derechos de acceso, rectificación y cancelación (art. 12). Los Estados miembros tienen que garantizar al interesado el derecho a obtener del responsable del tratamiento libremente, sin restricciones, con una periodicidad razonable y sin retrasos ni gastos excesivos, la confirmación de la existencia o no de tratamientos de datos que le conciernan, los fines de tales tratamientos, las categorías de datos que constan y los destinatarios o las categorías de destinatarios a quienes se comunicarán dichos datos. El responsable tendrá que hacerle saber, de manera inteligible, qué datos son objeto de tratamiento y su origen, así como la lógica utilizada en los tratamientos automatizados que los contengan (al menos en los casos en que se vayan a adoptar decisiones automatizadas).

El interesado disfrutará de un derecho de rectificación, supresión o bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la Directiva (v. gr. por ser incompletos o inexactos). La rectificación, supresión o bloqueo se notificará después a los terceros a quienes se hayan comunicado los datos, a no ser que resulte imposible o suponga un esfuerzo desproporcionado.

3) El derecho de oposición (art. 14). La Directiva prescinde de reconocer un derecho general de oposición aunque, vistos los términos en los que se

pronuncia, tampoco cabe concluir que lo circunscribe únicamente a los dos supuestos que enuncia.

En primer lugar, el interesado puede oponerse a que sus datos sean objeto de tratamiento, “al menos” en los supuestos del art. 7,e) y f) (cumplimiento de una misión de interés público o inherente al ejercicio de un poder público o tratamiento necesario para satisfacer un interés legítimo del responsable), en cualquier momento y por razones legítimas propias de su situación particular, salvo que el Estado decida no permitirlo. En segundo lugar, se faculta al individuo a oponerse, previa petición y sin gastos, al tratamiento de sus datos destinado a la prospección. Antes de que dichos datos se comuniquen por vez primera a terceros o se usen en nombre de éstos (también a efectos de prospección) deberá informársele y ofrecerle expresamente la posibilidad de oponerse, igualmente sin gastos, a dicha comunicación o utilización.

4) El derecho a no verse sometido a una decisión basada en tratamientos automatizados de datos (art. 15). Las personas tienen el derecho a no verse sometidas a una decisión que tenga efectos jurídicos sobre ellas o les afecte de manera significativa y se base sólo en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad (rendimiento laboral, crédito, fiabilidad, conducta, etc.). Se excepcionan los supuestos en que: a) dicha decisión se adoptara en el marco de la celebración o ejecución de un contrato hecho a petición del interesado o cuando éste tenga la posibilidad de defender su punto de vista para salvaguardar su interés legítimo; b) esa valoración esté autorizada por una ley que establezca medidas que garanticen el interés legítimo del interesado.

5) El derecho a una indemnización (art. 23). La persona que sufra un perjuicio como consecuencia de un tratamiento ilícito o de una acción incompatible con las disposiciones nacionales adoptadas en aplicación de la Directiva, tiene derecho a obtener del responsable del tratamiento la reparación del perjuicio sufrido. La responsabilidad objetiva de dicho responsable podrá excluirse si demuestra que no cabe imputarle el hecho que ha provocado el daño (v. gr. por responsabilidad del interesado o fuerza mayor, considerando 55).

6) El derecho a un sistema de recursos y sanciones (arts. 22 y 24). Aparte de la existencia de un recurso administrativo ante la autoridad nacional de protección de datos (art. 28), se podrá acudir a la vía judicial en caso de violación de los derechos de los interesados. Por supuesto, los Estados establecerán las medidas adecuadas para garantizar la plena aplicación de la Directiva, fijando las sanciones que deben aplicarse de incumplirse las

pautas que proporciona. Sin esta referencia el sistema de garantías, simplemente, no estaría completo.

Más allá de excepciones puntuales a las que la propia Directiva 95/46/CE se refiere, en paralelo al reconocimiento de estos derechos el art. 13 faculta a los Estados a establecer límites al principio de calidad de los datos, información, acceso, rectificación y cancelación y a la obligación de dar publicidad a los tratamientos. Podrán hacerlo cuando constituya una medida necesaria para la salvaguarda de: a) la seguridad del Estado; b) la defensa; c) la seguridad pública; d) la prevención, investigación, detección y represión de infracciones penales o de la deontología en las profesiones reglamentadas; e) un interés económico y financiero importante de un Estado miembro o de la Unión Europea, incluidos los asuntos monetarios, presupuestarios y fiscales; f) una función de control, de inspección o reglamentaria relacionada, aunque sólo sea ocasionalmente, con el ejercicio de la autoridad pública en los casos de seguridad pública, infracciones penales e interés económico; g) la protección del interesado o de los derechos y libertades de otras personas. Naturalmente todo ello obedece a que no hay ningún derecho fundamental absoluto y a que su ejercicio ha de compatibilizarse con el de otros derechos o intereses que deben protegerse debidamente.

De la misma manera, sin perjuicio del establecimiento de las garantías legales apropiadas, los Estados podrán, si manifiestamente no existe ningún riesgo de atentado contra la vida privada del interesado, limitar mediante disposición legislativa los derechos de acceso, rectificación y cancelación cuando los datos vayan a ser exclusivamente tratados con fines de investigación científica o estadística.

2.2.b) Las transferencias internacionales de datos

Teniendo en cuenta que la Directiva 95/46/CE se dicta, primordialmente, por la relevancia económica que tiene el intercambio de datos personales entre los Estados miembros, resulta evidente que el legislador comunitario no iba a soslayar la trascendencia de dichos intercambios con terceros Estados¹⁵. El peligro de fomentar siquiera indirectamente la existencia de

¹⁵ Véanse, por todos, O. ESTADELLA YUSTE, *La protección de la intimidad frente a la transmisión internacional de datos de carácter personal*, Tecnos, Madrid, 1995; H. ANCOS FRANCO, "La regulación de las transferencias internacionales de datos como barrera al comercio internacional: de la Directiva 95/46 a los acuerdos UE-terceros Estados", *RDCE*, núm. 6, Julio-Diciembre 1999, pp. 497-516; R. DÍAZ ARIAS, "España: Transferencia de Datos de

paraísos de datos lleva a que las transferencias internacionales de datos personales sólo puedan efectuarse cuando se garantice un nivel de protección adecuado (arts. 25-26). Los criterios a tomar en consideración, en cada supuesto concreto, para valorar la adecuación son: la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y de destino final, la legislación (general o sectorial) vigente, las normas profesionales y las medidas de seguridad en vigor.

La Directiva 95/46/CE erige en garante de las transferencias internacionales de datos a la Comisión. Cuando ella misma (directamente o informada por un Estado miembro) compruebe que un tercer Estado no garantiza un nivel de protección adecuado, adoptará las medidas precisas para evitar cualquier transferencia de datos a él y se halla obligada a realizar las negociaciones pertinentes para corregir tal situación. A sensu contrario, podrá hacer constar que un país tercero asegura un nivel de protección adecuado, vista su legislación interna o sus compromisos internacionales. A día de hoy ha declarado la adecuación de Suiza, Hungría, Argentina, la Bailía de Guernsey y la Isla de Man y, en determinados supuestos, de Estados Unidos (empresas adheridas al Puerto Seguro y PNR) y Canadá (entidades privadas de ámbito federal que recojan, utilicen o divulguen datos personales en sus actividades comerciales)¹⁶.

Sin embargo, realizar una transferencia a un tercer Estado aun cuando no garantice un nivel adecuado de protección puede ser legítimo. Salvo disposición en contra del Estado miembro, se permitirá siempre y cuando: a) medie el consentimiento inequívoco del interesado a la transferencia; b) la transferencia se requiera para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales tomadas a petición del interesado; c) sea preciso para la celebración o ejecución de un contrato celebrado o por celebrar, en interés del titular de los datos, entre el responsable del tratamiento y un tercero; d)

carácter personal. ¿Llegarán nuestros datos a buen puerto?”, REDI, núm. 23, Junio-2000; E. ACED FÉLEZ, “Transferencias internacionales de datos personales entre Europa y USA”, ponencia al II Congreso Mundial de Derecho informático: España; cuna de un mundo global (Madrid, 2002) y D. SANCHO VILLA, Transferencia internacional de datos personales, APD, Madrid, 2003.

¹⁶ Decisiones de la Comisión de 26 de julio de 2000, sobre Suiza, Hungría (hoy Estado miembro) y Puerto Seguro (DO núm. L 215, de 25/08/2000, p. 1, 4 y 7, respectivamente); de 20 de diciembre de 2001, sobre Canadá (DO núm. L 2, de 04/01/2002, p. 13); de 30 de junio de 2003, sobre Argentina (DO núm. L 168, de 05/07/2003, p. 19); de 21 de noviembre de 2003, sobre Guernsey (DO núm. L 308, de 25/11/2003, p. 27) y de 28 de abril de 2004, sobre la Isla de Man (DO núm. L 208, de 10/06/2004, p. 47).

sea necesario o venga legalmente exigido para la salvaguarda de un interés público importante o para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial; e) se pretenda para la protección de un interés vital del interesado; f) la transferencia tenga lugar desde un registro público que, en virtud de disposiciones legales o reglamentarias, esté concebido para facilitar información al público y abierto a la consulta general o por cualquier persona que pueda demostrar un interés legítimo (cumpliendo las condiciones que establezca la ley para la consulta).

Y, por si el régimen de excepciones no fuera suficientemente generoso, se recoge otro supuesto de licitud de las transferencias: los Estados miembros podrán autorizarla, informando a la Comisión, si el responsable del tratamiento ofrece garantías suficientes respecto de la protección de la vida privada y sus derechos instrumentales. En este sentido, es frecuente que tales garantías se deriven de cláusulas contractuales apropiadas¹⁷.

Pero si hay un supuesto que está resultando especialmente polémico es el acceso al PNR (Passenger Name Records) por parte de las autoridades estadounidenses. De hecho, ha motivado un grave conflicto entre las instituciones de la Unión.

Tras el 11-S se dicta en Estados Unidos una batería de leyes y normas diversas tendentes a reforzar la seguridad nacional. Entre ellas, la Aviation and Transport Security Act, de 19 de noviembre de 2001 y la Enhanced Border Security and Visa Entry Reform Act, de 14 de mayo de 2002, obligan a todas las compañías dedicadas al transporte aéreo internacional de pasajeros, con vuelos con destino, origen o escala en Estados Unidos, a proporcionar acceso electrónico al PNR¹⁸ al Servicio de Aduanas y Protección de Fronteras del Departamento de Seguridad Interior estadounidense. De esta

¹⁷ La Comisión ha creado modelos de cláusulas tipo para facilitar las transferencias, aunque pueden utilizarse otras. Véanse las Decisiones de la Comisión de 15 de junio de 2001 (DO núm. L 181, de 04/07/2001, p. 19) y de 27 de diciembre de 2001 (DO núm. L 6, de 10/01/2002, p. 52).

¹⁸ Dependiendo de los usos comerciales, en el PNR pueden constar hasta sesenta tipos de datos que permiten identificar al pasajero, las personas que lo acompañan, las que han efectuado la reserva en su nombre, la agencia o el empleado que tramitó la reserva y/o emitió el billete, y los miembros de la tripulación: itinerario y billetes, medios de pago, número de tarjeta de crédito, condiciones especiales ofrecidas a grupos específicos (pasajeros frecuentes, miembros de grupos especiales), direcciones de correo electrónico y direcciones físicas, números de teléfono particulares y/o profesionales declarados, personas de contacto, servicios específicos vinculados al estado de salud y preferencias sobre alimentación, observaciones concretas efectuadas por el personal de la compañía aérea, detalles relacionados con las reservas para el alquiler de un automóvil, etc.

suerte, entrando informáticamente en el registro electrónico de las compañías y utilizando el sistema APIS (Advance Passenger Information System), las autoridades norteamericanas pretenden determinar de antemano el peligro potencial que podría entrañar cada uno de los pasajeros, asegurar la identificación y detención de cualquier terrorista o individuo responsable de delitos graves o impedir su entrada en Estados Unidos.

Esta orden ocasiona espinosos problemas desde el punto de vista de la protección de datos personales. Estados Unidos no reconoce con carácter general el derecho fundamental a la protección de datos personales, pese a que la privacidad se menciona en la Cuarta Enmienda a la Constitución norteamericana. Lo hace básicamente cuando existe un riesgo de abuso gubernamental en el trato de la información personal y, de este modo, la ley federal interviene sólo frente a él (Privacy Act de diciembre de 1974) o cuando se trata de negocios que almacenan información personal sensible (v. gr. datos médicos, financieros o sobre el alquiler de determinadas películas de vídeo). En el resto de casos, si se disciplina, se hace por medio de disposiciones de carácter autorregulatorio. Además, en el concreto ámbito al que se alude no existe tutela alguna respecto de los datos de pasajeros que no son ciudadanos de los Estados Unidos (o residentes legales) ni tampoco recurso judicial contra eventuales abusos en la aplicación de dichas medidas.

Acceder al PNR significaba realizar una transferencia internacional ilegal según los cánones de la Directiva 95/46/CE, por ello entre junio de 2002 y mayo de 2004 se desarrolló un complejo proceso de negociación para paliar tal contradicción. Dicho proceso ha concluido con la autorización de las transferencias a través de la Decisión de 14 de mayo de 2004, relativa al carácter adecuado de la protección de los datos personales incluidos en los registros de nombres de los pasajeros que se transfieren al Servicio de aduanas y protección de fronteras de Estados Unidos (Bureau of Customs and Border Protection) y la Decisión 2004/496/CE del Consejo, de 17 de mayo, relativa a la celebración de un 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, Oficina de aduanas y protección de fronteras, de los Estados Unidos¹⁹.

No obstante, vistos los términos del acuerdo, el acceso al PNR seguía sin respetar el contenido y la finalidad de la Directiva 95/46/CE, por lo que

¹⁹ DO n° L 235 de 06/07/2004, p. 11 y DO núm. L 183, de 20/05/2004, p. 83, respectivamente.

ambos textos fueron recurridos por el Parlamento Europeo ante TJCE el 25 de junio de 2004. Dada la condición de socio estratégico de Estados Unidos y de ciertas “licencias” permitidas en aras a la persecución del terrorismo, se ha tolerado que una medida de simple ejecución de la Directiva 95/46/CE tenga por efecto perverso reducir la tutela brindada a los datos personales de los ciudadanos en la Unión

2.2.c) Los códigos de conducta

La Directiva también se refiere a las normas de autorregulación de los diferentes sectores que utilizan tratamientos de datos personales (art. 27). El uso de esas prácticas se contempla con agrado desde el ámbito comunitario y por los Estados miembros, puesto que constituye una forma de alcanzar un plus en su tutela desde la buena voluntad de los sectores empresariales implicados en los tratamientos.

Para los de ámbito nacional, la norma comunitaria establece la posibilidad de que estos códigos se sujeten al examen de las autoridades nacionales de control, en aras a verificar su conformidad con las prescripciones comunitarias. Tratándose de códigos de conducta comunitarios, éstos serán sometidos a examen por el Grupo del art. 29 y, si reciben de éste un informe favorable, la Comisión podrá darles una publicidad adecuada²⁰.

2.2.d) Las autoridades de control y el Grupo del art. 29

Dado que la protección de datos personales constituye un aspecto básico de la tutela de los derechos de los ciudadanos, se exige a los Estados la habilitación de una o más autoridades públicas que se encarguen de velar por la aplicación en su territorio de la normativa adoptada en aplicación de la Directiva (art. 28.1). No se concreta el modelo institucional (órgano simplemente especializado o “separado”, ente no inserto en la estructura de la Administración, constitucional o administrativo, etc.). Dichas autoridades deberán ejercer sus funciones con total independencia. La noción de independencia aparece vinculada a la no sujeción a instrucciones y tampoco se ofrece criterio alguno sobre si debiera ligarse igual a la forma de elección o cese de sus responsables, decisión que no es baladí.

²⁰ Pese a que códigos deontológicos hay bastantes, son pocos los que se animan a inscribirlos o notificarlos a las autoridades comunitarias o nacionales. A nivel comunitario sólo hay un código de conducta que haya recibido el placet de la Comisión: el de la FEDMA (Federación Europea de Marketing Directo).

Tendrán poderes de investigación e intervención, así como capacidad procesal en caso de que se infrinja la normativa de transposición o capacidad de poner dichas infracciones en conocimiento de la autoridad judicial. Sus decisiones lesivas de derechos serán susceptibles de recurso judicial. Asimismo, deberán presentar informe periódico de sus actuaciones (que será publicado) y cooperar con las demás autoridades de control (v. gr. intercambiándose información útil).

Por otra parte, la Directiva crea el “Grupo de la protección de las personas en lo que respecta al tratamiento de datos de carácter personal” (en adelante, Grupo del art. 29). Estará formado por un representante de la autoridad o autoridades de control designadas por cada Estado miembro, un representante de la autoridad o autoridades creadas por las instituciones y organismos comunitarios y un representante de la Comisión, institución que ejerce las funciones de secretaría. Tomará sus decisiones por mayoría simple de los representantes de las autoridades de control y tiene naturaleza eminentemente consultiva. El Grupo actuará de forma independiente, circunstancia que se cree garantizar mediante la elección de sus representantes (no designados por los Gobiernos) y por el sistema de adopción de sus actos.

Sus funciones son: a) estudiar toda cuestión relativa a la aplicación de las disposiciones nacionales de transposición con vistas a contribuir a la aplicación homogénea de la Directiva; b) emitir un dictamen destinado a la Comisión sobre el nivel de protección existente dentro de la Comunidad y en los países terceros; c) asesorar a la Comisión sobre cualquier proyecto de modificación de la Directiva, otras medidas adicionales o específicas y los proyectos de medidas comunitarias que afecten a los derechos y libertades de las personas físicas en lo que respecta al tratamiento de sus datos; d) emitir un dictamen sobre los códigos de conducta comunitarios (art. 30). Este órgano consultivo puede actuar por iniciativa propia, formulando recomendaciones, o a instancia de la Comisión. Así pues, no se trata de un órgano de cooperación entre Estados, sino que se le atribuyen funciones de control y vigilancia de la aplicación y cumplimiento de las disposiciones de la Directiva²¹.

2.2.e) Manifestaciones sectoriales: la Directiva 2002/58/CE

Junto a la propuesta de Directiva general sobre protección de datos contenida en el COM SYN 287, se propugnaba la adopción de otra serie de

²¹ Todos sus documentos se pueden consultar en http://europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/index_fr.htm.

actos referidos a sectores más específicos, como el de las telecomunicaciones (SYN 288), pero el retraso en la adopción de la primera determinó una pérdida de conciencia progresiva sobre los problemas de la protección de datos en contextos sectoriales. Pasados unos años, se aprueba la Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, norma sectorial relativa al tratamiento de los datos de carácter personal y a la protección de la intimidad en el ámbito de las telecomunicaciones, que precisa y completa a la Directiva 95/46/CE. Ésta ha sido reemplazada por la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio, relativa al tratamiento de los datos de carácter personal y a la protección de la intimidad en el sector de las comunicaciones electrónicas²². En este momento está en proyecto completarla con otra polémica directiva que, tras los últimos atentados sufridos en el Continente y en aras a aumentar la defensa nacional y la seguridad pública, propone una retención indiscriminada de los datos de tráfico que generan los usuarios en sus comunicaciones electrónicas²³.

3. LOS DATOS PERSONALES EN LOS TRATAMIENTOS REALIZADOS POR LAS INSTITUCIONES COMUNITARIAS

No todas las medidas sobre protección de datos personales que se van adoptando en el seno de la Unión Europea tienen por destinatarios a los Estados miembros. Tras aprobarse la Directiva 95/46/CE, tanto la Comisión como el Consejo se comprometieron públicamente a aplicarla mas, con la modificación operada por el Tratado de Ámsterdam en 1997, es el art. 286 TCE el que pasa a establecer que: "1. A partir del 1 de enero de 1999, los actos comunitarios relativos a la protección de las personas respecto del tratamiento de datos de carácter personal y a la libre circulación de dichos datos serán de aplicación a las instituciones y organismos establecidos por el presente Tratado o sobre la base del mismo. 2. Con anterioridad a la fecha indicada en el apartado 1, el Consejo establecerá, con arreglo al procedimiento previsto en el artículo 251, un organismo de vigilancia independiente, responsable de controlar la aplicación de dichos actos comunita-

²² DO núm. L 201, de 31/07/2002, p. 37.

²³ COM(2005) 438 final de 21/09/2005: "Proposition de Directive du Parlement Européen et du Conseil sur la conservation de données traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public, et modifiant la directive 2002/58/CE". Sobre este tema vid. M.C. GUERRERO PICÓ, "Protección de datos personales e Internet: la conservación indiscriminada de los datos de tráfico", Revista de la Facultad de Derecho de la Universidad de Granada, núm. 8, 2005, pp. 109-139.

rios a las instituciones y organismos de la Comunidad y adoptará, en su caso, cualesquiera otras disposiciones pertinentes”. Se lleva, por tanto, al Derecho originario la necesidad de que el tratamiento de información personal en la esfera comunitaria responda homogéneamente al alto estándar tuitivo consagrado en la Directiva 95/46/CE.

El art. 286 TCE pretende ser una muestra de los esfuerzos que realiza la Unión Europea por paliar su criticada falta de transparencia, la misma motivación que va a justificar posteriormente la inclusión en la Constitución Europea de un artículo sobre protección de datos dentro del título dedicado a la vida democrática de la Unión.

El desarrollo del mandato que contiene el art. 286 TCE lo encontramos en el Reglamento (CE) nº 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos de carácter personal por las instituciones y los organismos comunitarios y a la libre circulación de estos datos (en adelante, Reglamento (CE) nº 45/2001)²⁴. Quedan fuera de su ámbito de aplicación los tratamientos realizados fuera del ámbito estrictamente comunitario (art. 3.1), esto es, en el marco del segundo y tercer pilar, a los que con posterioridad me referiré.

El Reglamento (CE) nº 45/2001 consagra el principio de calidad de los datos (art. 4), de licitud del tratamiento (art. 5) —previando el cambio de fines (art. 6)—, de información (arts. 11-12) y de confidencialidad y seguridad (arts. 21-23), estableciendo determinadas particularidades en lo que respecta al tratamiento de las categorías especiales de datos (art. 10). Reconoce los derechos de acceso (art. 13), rectificación (art. 14), bloqueo (art. 15), supresión (art. 16), notificación a terceros (art. 17), oposición (art. 18) y no sometimiento a decisiones individuales automatizadas (art. 19), recogiendo un régimen de excepciones en el art. 20. Establece asimismo cuáles son las obligaciones del responsable del tratamiento (arts. 24-31) e implanta un sistema de recursos (arts. 32-33) y sanciones (art. 49). También encuentran acomodo en él algunas normas destinadas a regular la transmisión de datos de carácter personal, distinguiendo en función de que ésta se

²⁴ DO núm. L 8, de 12/01/2001, p. 1. El Reglamento contempla disposiciones muy parecidas a las de la Directiva 95/46/CE, si bien el capítulo IV se refiere a la protección de los datos en el contexto de las redes internas de telecomunicación, esto es, al objeto de la antigua Directiva 97/66/CE. Vid. también la Decisión 2004/644/CE del Consejo, de 13 de septiembre, por la que se adoptan las normas de desarrollo del Reglamento (CE) núm. 45/2001 (DO núm. L 296, de 21/09/2004, p. 16).

lleve a efecto entre las instituciones u organismos comunitarios (art. 7) o con otros diferentes (arts. 8 y 9).

Cumpliendo con el mandato del art. 286 TCE, el Reglamento crea una autoridad de control independiente, el Supervisor Europeo de Protección de Datos. A él, que no puede recibir instrucción alguna, corresponde fiscalizar la aplicación efectiva de las disposiciones reglamentarias por las instituciones y organismos comunitarios.

Las tareas que se le encomiendan son: investigar eventuales violaciones de las normas sobre protección de datos (a iniciativa propia o en respuesta a reclamaciones) y comunicar a los interesados su resultado en plazo razonable; supervisar y asegurar la aplicación del Reglamento y cualquier otro acto comunitario que proteja en el plano institucional a las personas físicas (salvo los tratamientos que realice el TJCE cuando actúe en el ejercicio de sus funciones jurisdiccionales); asesorar, previa petición o a iniciativa propia, a todas las instituciones y organismos comunitarios, especialmente antes de que elaboren normas internas sobre este tema; colaborar con las autoridades de control nacionales, con los organismos de control creados en el marco del tercer pilar y participar en las actividades del Grupo del art. 29; hacer públicas y explicitar los motivos en los que se fundan las excepciones o autorizaciones que el Reglamento permite adoptar (en materia de datos sensibles, información cuando los datos no proceden del titular, decisiones automatizadas o datos de tráfico de las comunicaciones); mantener un registro de los tratamientos y efectuar una comprobación previa de los que se le notifiquen.

Además, entre sus competencias está: asesorar a las personas en el ejercicio de sus derechos; acudir al responsable del tratamiento en caso de presunta infracción y formular propuestas encaminadas a corregirla; ordenar la atención de los derechos que se denieguen indebidamente; advertir o amonestar, cuando proceda, al responsable del tratamiento; imponer una prohibición temporal o definitiva del tratamiento; someter un asunto a la institución u organismo comunitario de que se trate; someter un asunto al TJCE en las condiciones previstas en el Tratado e intervenir en los asuntos presentados ante él (algo que presumiblemente hará en el "affaire PNR"). Anualmente presentará un informe anual sobre su actividad al Parlamento Europeo, Consejo y Comisión y lo hará público.

Merece la pena destacar que, sin perjuicio de eventuales recursos ante el TJCE, todo interesado está facultado a presentar (sin necesidad de pasar por la vía jerárquica) una reclamación ante el Supervisor si considera violados los derechos que le reconoce el art. 286 TCE. Por otra parte, las decisiones del Supervisor son susceptibles de recurso ante el TJCE.

La valoración que se hace de esta norma es positiva; viene a potenciar la vida democrática en las instituciones comunitarias y así ha sido subrayado por la doctrina. No obstante, debemos decir que en la práctica se han dado algunos problemas por el incorrecto entendimiento de algunos preceptos del Reglamento (CE) nº 45/2001 y de la Directiva 95/46/CE. El Defensor del Pueblo Europeo ha advertido que, en numerosas ocasiones, las normas sobre protección de datos personales se han utilizado para socavar el principio de transparencia en las actividades públicas de la Unión, alegándose un —inexistente— derecho a la participación anónima en actividades públicas, que formaría parte del derecho fundamental a la protección de los datos de carácter personal.

4. LA TUTELA DE LA INFORMACIÓN PERSONAL EN EL TERCER PILAR

Tal y como he avanzado, se excluyen del ámbito de aplicación de las Directivas 95/46/CE y 97/66/CE, del art. 286 TCE y del Reglamento (CE) nº 45/2001 los tratamientos de las instituciones y organismos efectuados en el marco de la PESC o de la cooperación policial y judicial penal, esto es, de los títulos V y VI del TUE. Hay una falla, por tanto, en el propósito de igualar los criterios que orientan los tratamientos de datos personales realizados por todas las instituciones y organismos de la Unión Europea. Dos son las cuestiones que se suscitan a propósito de la tutela del derecho a la protección de datos en esta esfera: el régimen jurídico de los tratamientos realizados por las instituciones y el de los grandes sistemas de información del tercer pilar.

Tras la inclusión del art. 286 TCE se plantea la creación de un reglamento donde se unifiquen las pautas a seguir en materia de protección de datos en el ámbito institucional, sin hacer distinciones. La Comisión se muestra favorable a ello aunque con matices, pues juzga conveniente que el ámbito de aplicación de la norma no englobe los tratamientos efectuados por los organismos creados en el marco del título VI del TUE, por ejemplo Europol²⁵. El Consejo se opone tajantemente a la propuesta de unificación y el Parlamento Europeo, aunque era partidario de ella, terminará aviniéndose a la posición de aquél para aprobar en primera lectura un texto normativo conside-

²⁵ COM (1999) 337 final, de 14 de julio: “Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos de la Comunidad y sobre la libre circulación de estos datos”.

rado necesario. Idéntico propósito lleva a la Comisión a cejar en su propósito, si bien posteriormente declarará que: “toma nota de que las instituciones proceden al tratamiento de datos personales en virtud de los títulos V y VI del Tratado de la Unión Europea. Considera que es necesario someter dichos tratamientos a reglas jurídicas claras e inequívocas en cuanto a la protección de los datos personales. La Comisión afirma que dicha normativa puede adoptarse sobre la base del artículo 286 del Tratado constitutivo de la Comunidad Europea. Considera que dicha base cubre el tratamiento de datos efectuado por las instituciones y organismos comunitarios en todos aquellos casos en que actúan, incluido en el ámbito de las actividades propias de los títulos V y VI del Tratado de la Unión Europea. Por ello, no comparte la interpretación del Consejo de que el artículo 286 del Tratado constitutivo de la Comunidad Europea cubriría únicamente las actividades reguladas por ese mismo Tratado. La Comisión se reserva la posibilidad de presentar otras tantas iniciativas legislativas al efecto. Se reserva asimismo la posibilidad de someter los tratamientos de datos personales efectuados por la Comisión en virtud de actividades derivadas de los títulos V y VI del Tratado de la Unión Europea a los principios contenidos en el presente Reglamento hasta que se establezcan reglas aplicables a dichos tratamientos de datos”²⁶.

El propósito de esta declaración de intenciones es loable. Sin embargo, desde el punto de vista técnico, cabe dudar de su corrección jurídica. Para que pudiera aplicarse a esos ámbitos una disposición del TCE (v. gr. el art. 286), tendrían que darse dos condiciones cumulativamente: que su redacción no lo impidiese y que se mencionara en los arts. 28-41 TUE. Esto último no sucede y debemos tener presente que la lista fue actualizada por el Tratado de Ámsterdam —el mismo que introdujo el art. 286—, lo cual parece suficientemente expresivo. Este artículo no podría ser la base jurídica que permitiera imponer los criterios de la Directiva 95/46/CE a los tratamientos realizados por las instituciones en el marco de los títulos V y VI del TUE.

Con todo, a pesar de no regirse por el art. 286 TCE y quedar fuera del ámbito de aplicación del Reglamento nº (CE) 45/2001, por medio del considerando 15 de dicha norma se intenta transmitir la idea de que en el resto de casos también se presta una protección suficiente al derecho del indivi-

²⁶ Declaración 120/00, Ad apartado 1 del artículo 3, en el Anexo II del Documento del Consejo 14547/00, de 13 de diciembre, Lista mensual de los actos del Consejo-Noviembre de 2000.

duo a disponer y controlar su información personal, porque la protección de los derechos fundamentales se garantiza respetando el art. 6 TUE y porque “el acceso a los documentos, incluidas las condiciones de acceso a los documentos que contengan datos personales, depende de las normas adoptadas sobre la base del artículo 255 del Tratado CE, cuyo ámbito de aplicación abarca los Títulos V y VI del Tratado de la Unión Europea”.

Esta declaración no puede dejar de suscitar perplejidad, por varios motivos. Es verdad que el art. 6 TUE declara el respeto a los derechos fundamentales por parte de las instituciones de la Unión, mas no es menos cierto que, por el momento, los particulares no disponen de un recurso directo para someter al TJCE los actos adoptados por las instituciones en el marco del segundo y tercer pilar que vulnerasen derechos fundamentales. El art. 46,d) TUE declara la competencia del Tribunal para juzgar el respeto del art. 6 TUE de los actos sometidos a su jurisdicción. Esto significa que, en lo que concierne al título V del TUE, podrá conocer lo que atañe al art. 28 y, en lo atinente al título VI, el art. 35 concede sólo a los Estados miembros y la Comisión legitimación activa para que el Tribunal enjuicie ciertos actos. No resulta, pues, tal clara la afirmación de que se está garantizado suficientemente en estos espacios el respeto al derecho a la protección de datos. Y aún se entiende menos la referencia al art. 255 TCE. Aparentemente se estaría trazando una suerte de equivalencia entre el derecho de acceso, garantía instrumental del derecho a la protección de datos, y el derecho de acceso a la documentación de las instituciones. No obstante, el derecho de acceso a los documentos no resulta adecuado para que la persona concernida sepa qué información personal se tiene de ella. A lo sumo podrá comprobar si se la cita y bajo qué circunstancias en uno o varios documentos determinados, pero esto es algo que pueden hacer todos los ciudadanos y sin que los documentos incluyan información sobre ellos. Y al contrario. El derecho de acceso no responde al deseo de asegurar la transparencia administrativa sino que permite al interesado conocer qué información suya consta en un determinado fichero, con qué fines se trata, a quién se cede, etc.

La segunda cuestión a la que aludía al comenzar este epígrafe es la protección de los datos personales obrantes en los sistemas de información del tercer pilar. Al SIS sigue la instauración de otros grandes sistemas basados en las tecnologías de la información: el Sistema de Información Aduanera²⁷, cuyo objetivo es contribuir a prevenir, investigar y perseguir las in-

²⁷ Convenio establecido sobre la base del artículo K.3 del Tratado de la Unión Europea, relativo a la utilización de la tecnología de la información a efectos aduaneros (DO n° C 316, de 27/11/1995, p. 34).

fracciones graves de las leyes nacionales aumentando, mediante la rápida difusión de información, la eficacia de los procedimientos de cooperación y control de las Administraciones aduaneras de los Estados miembros; el Sistema de Información Europol²⁸, creado para facilitar la prevención y lucha contra el terrorismo, el tráfico ilícito de estupefacientes y otras formas graves de delincuencia internacional, y el Sistema de Información Eurojust²⁹, que intensificará la cooperación judicial entre los Estados miembros, en particular en la lucha contra las formas graves de delincuencia, de la que son responsables frecuentemente organizaciones transnacionales.

Quedan fuera del Reglamento (CE) nº 45/2001, aunque en el considerando 17 el mismo se apunta que: “La eficacia de la protección de las personas respecto al tratamiento de datos personales en la Unión requiere la coherencia de las normas y de los procedimientos aplicables en la materia a las actividades correspondientes a diferentes marcos jurídico. La elaboración de principios fundamentales relativos a la protección de datos personales en el ámbito de la cooperación judicial en materia penal y en el de la cooperación policial y aduanera, y la creación de una secretaría para las autoridades de control comunes, establecidas en virtud del Convenio Europol, el Convenio relativo a la utilización de la tecnología de la información a efectos aduaneros y el Convenio de Schengen, constituyen a este respecto una primera etapa”. Resulta extraño que para el legislador sea tan significativa la unificación de las tres secretarías³⁰. Es más una medida tendente a reducir gastos administrativos que a proporcionar, ni siquiera tímidamente, una tutela homogénea en esos ámbitos.

El Parlamento Europeo viene denunciando desde hace tiempo que los tratamientos efectuados en el marco particularmente delicado de los sistemas europeos de información están sometidos a una normativa fragmentaria y que no proporciona a la persona concernida un nivel suficiente de protección. El marco de referencia suele ser el Convenio número 108 del Consejo de Europa, mucho menos detallado que la Directiva 95/46/CE, y la Recomendación nº R 15 (87) sobre el sector policial. Además, sus normas son

²⁸ Convenio basado en el artículo K.3 del Tratado de la Unión Europea, por el que se crea una Oficina Europea de Policía (DO núm. C 316, de 27/11/1995, p. 1).

²⁹ Decisión del Consejo de 28 de febrero de 2002 por la que se crea Eurojust para reforzar la lucha contra las formas graves de delincuencia (DO núm. L 63, de 06/03/2002, p. 1).

³⁰ Decisión del Consejo de 17 de octubre de 2000 (DO núm. L 271, de 24/10/2000, p. 1). Ahora ha quedado fuera de la secretaría única la Autoridad Común de Control de Eurojust, de más reciente creación.

sometidas a numerosas excepciones que afectan a los derechos de las personas concernidas y, aunque parte de la misión del Supervisor Europeo de Protección de Datos es colaborar con los organismos de control creados en el marco del tercer pilar para mejorar la coherencia en la aplicación de las normas cuyo respeto tienen encomendadas, esto no es objetivamente suficiente para sostener que se vela adecuadamente por el respeto de este derecho. Urge la creación de un instrumento jurídico de carácter obligatorio que establezca unas reglas y garantías comunes sobre protección de datos.

Preocupa también que Europol o Eurojust estén autorizadas a celebrar acuerdos con terceros países u organizaciones de terceros Estados si garantizan un nivel adecuado de protección y que, en realidad, la autoridad de control no sea competente para vigilar la transmisión y el tratamiento de los datos; que el papel que se concede al Parlamento Europeo en este ámbito sea tan sumamente reducido, limitándose a recibir algún informe o a ser consultado en muy pocas ocasiones; que no se reconozca la competencia del TJCE para dictaminar la validez de los acuerdos sobre transferencias a otros Estados u organizaciones o la correcta interpretación de dichos acuerdos, etc.

Como se constata igualmente que los atentados de Nueva York, Madrid y Londres están precipitando la adopción de medidas de seguridad preventivas que no son todo respetuosas que debieran con los derechos fundamentales de los ciudadanos. Por ejemplo, en el tránsito del Sistema de Información Schengen hacia el nuevo Sistema de Información Schengen II, los planes del Consejo pasan por aumentar las categorías de personas, objetos y datos (incluso biométricos) a inscribir, la ampliación de los plazos para conservar las anotaciones y el acceso a él de organismos del tercer pilar y autoridades nacionales no autorizados inicialmente y con fines distintos a los consagrados al diseñar este sistema.

5. EL ART. 8 DE LA CARTA DE LOS DERECHOS FUNDAMENTALES

Hasta el momento hemos podido comprobar que la consecución de un objetivo económico sirve de revulsivo para instar a los Estados miembros a proteger eficazmente los datos personales. Esto no debiera sorprender en demasía pues inicialmente la tutela de los derechos fundamentales en el ámbito comunitario no se contempla y el caso del derecho a la protección de datos no iba a ser diferente.

Haciendo un breve repaso sobre la protección de los derechos fundamentales en la Unión hay que comenzar señalando que, dado que los objetivos de la integración económica son los prioritarios, los Tratados cons-

titutivos apenas si recogen alguna disposición de este tipo y cuando lo hacen se trata de libertades de corte económico. Por ende, el TJCE rechaza aquellas alegaciones basadas en derechos fundamentales protegidos por las Constituciones internas. Con todo, a finales de los años sesenta se produce un trascendental giro en la jurisprudencia de este órgano judicial y comienza a tutelar los derechos, entendiendo que están comprendidos dentro de los principios generales del Derecho comunitario y teniendo presente en su discurso argumentativo que: a) la protección de los derechos fundamentales se inspira en los principios constitucionales comunes a los Estados miembros³¹ y b) los instrumentos internacionales relativos a la protección de los derechos humanos en los que los Estados miembros han cooperado o a los que se han adherido, entre los que brilla con luz propia el CEDH, pueden facilitar asimismo indicaciones que es preciso tener en cuenta en el marco del Derecho comunitario.

No obstante, las limitaciones que presenta un sistema de protección de los derechos pretoriano son evidentes y ese es uno de los motivos que está en el origen de ciertas modificaciones en los Tratados constitutivos operadas a través del Acta Única Europea (1986), el Tratado de Maastricht (1992) y el Tratado de Ámsterdam (1997). De hecho, el art. 6.2 TUE establece que: "La Unión respetará los derechos fundamentales tal y como se garantizan en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales firmado en Roma el 4 de noviembre de 1950, y tal y como resultan de las tradiciones constitucionales comunes a los Estados miembros como principios generales del Derecho Comunitario". Como igualmente se reconoce que el TJCE, en el ámbito de sus competencias, puede enjuiciar los actos de las instituciones en caso de apreciarse una violación de derechos fundamentales (art. 46,d TUE), algo que no viene sino a confirmar la situación que se venía dando en la práctica³².

Algo más adelante, puesto que el TJCE determina que la Comunidad Europea carece de competencia para legislar en materia de derechos funda-

³¹ En una de sentencias del TJCE más relevantes de esta época, la que resuelve el Asunto Stauder, está implicada la protección de datos personales. El beneficiario de un subsidio para las víctimas de guerra consideraba que obligarle a indicar su nombre al registrarse para la compra de mantequilla a precio reducido suponía una violación de su dignidad personal y del principio de igualdad (STJCE de 12/11/1969). De todas formas, el reconocimiento y desarrollo del derecho que nos ocupa no vendrá dado por vía jurisprudencial sino por vía de Derecho derivado.

³² Realizando el significado político-constitucional que tiene el art. 6 TUE véase M. AZPITARTE SÁNCHEZ, "La cultura constitucional de la Unión Europea. Análisis del artículo 6 TUE", en F. BALAGUER CALLEJÓN, Derecho Constitucional y cultura. Estudios en homenaje a Peter Häberle, Tecnos, Madrid, 2004, pp. 369-386.

mentales y que la Unión no puede adherirse al CEDH por carecer de personalidad jurídica, la idea de dotar a la Unión Europea de un catálogo propio de derechos fundamentales toma cuerpo en las sesiones del Consejo Europeo de Colonia y Tampere en 1999³³. Aprovechando esta coyuntura, el Grupo de Trabajo del art. 29, a través de su Dictamen 4/99, de 7 de septiembre, recomienda la inclusión del derecho fundamental a la protección de datos en el catálogo europeo de derechos fundamentales³⁴. La sugerencia se estima oportuna y, de este modo, cuando el 7 de diciembre de 2000 se proclame en Niza la Carta de los Derechos Fundamentales de la Unión Europea (en adelante, CDF), su art. 8 consagrará, con el siguiente tenor, el derecho a la protección de datos: “1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación. 3. El respeto de estas normas quedará sujeto al control de una autoridad independiente”. El reconocimiento, por tanto, es un indicador del arraigo que este derecho —como el resto de los proclamados— está alcanzando en los Ordenamientos nacionales de los Estados miembros.

De la lectura de la Carta se puede concluir que éste es uno de los derechos fundamentales que se explicitan con mayor amplitud y que aparece deslindado con claridad meridiana de otros como el respeto a la vida privada y familiar. En cuanto al contenido del precepto, en primer lugar se

³³ Tal y como subraya BALAGUER CALLEJÓN, la configuración de una Comunidad de Derecho que responda a un orden constitucional propio —como pretende ser la Unión Europea— exige la adecuación de sus estructuras a los elementos que han configurado tradicionalmente el constitucionalismo, como la adopción de un catálogo de derechos fundamentales. Vid. “Derecho y derechos en la Unión Europea”, en J. CORCUERA ATIENZA (Coord.), *La protección de los derechos fundamentales en la Unión Europea*, Dykinson, Madrid, 2002, pp. 39-41.

³⁴ “El grupo (...) observa que algunos países europeos han integrado un derecho fundamental a la protección de datos en su constitución. En otros países la protección de datos ha adquirido estatuto de derecho fundamental a través de la jurisprudencia. En sus decisiones y sentencias, la Comisión Europea y el Tribunal Europeo de Derechos Humanos han elaborado y definido un derecho fundamental basándose en distintos derechos humanos vinculados a la protección de datos de carácter personal. Por último, un nuevo artículo (286) del Tratado de la Unión Europea dispone que los actos comunitarios relativos a la protección de las personas físicas en lo que concierne al tratamiento de los datos de carácter personal son aplicables, a partir del 1 de enero de 1999, a las instituciones y órganos de la Unión Europea. La integración de la protección de datos de carácter personal entre los derechos fundamentales europeos haría aplicable esta protección en el conjunto de la Unión y pondría de relieve la importancia creciente de la protección de estos datos en la Sociedad de la Información”.

hace una proclamación formal del derecho, reconociéndolo a toda "persona", sin especificar si física o jurídica. Ello no podría ser de otro modo, ya que son varios los Estados de la Unión Europea que les reconocen en pie de igualdad la titularidad de este derecho, si bien la Directiva 95/46/CE, el art. 286 TCE y el Reglamento (CE) nº 45/2001 protegen únicamente a las personas físicas.

En segundo lugar, a diferencia de lo que sucede con otros derechos, se opta por identificar lo que podría ser una suerte de contenido esencial del mismo: el principio de licitud, el principio de finalidad, el principio del consentimiento y del fundamento legal del tratamiento, el derecho de acceso y de rectificación. Incomprendiblemente, no se citan otros principios o derechos reconocidos comúnmente como parte integrante del estándar mínimo consagrado en todos los textos jurídicos europeos. No aparece el derecho de información, el principio de calidad, el derecho de cancelación o el principio de seguridad, por mencionar algunos. Tampoco se alude al régimen especial de los datos sensibles, por lo que tal vez hubiera sido más acertado limitarse a proclamar el derecho, sin aludir a las concretas facultades que lo integran.

Sin embargo, BATTAGLIA y DI FEDERICO³⁵ indican que esta crítica puede ser en parte superada recurriendo al art. 53 CDF, en cuya virtud ninguna disposición de la Carta debe ser interpretada como limitativa o lesiva de los derechos reconocidos en otras fuentes del Derecho internacional, el Derecho comunitario o las Constituciones de los Estados miembros. Entonces, si bien reclamados indirectamente, debe afirmarse que se aplican in toto los principios y derechos del Convenio número 108 del Consejo de Europa y de la Directiva 95/46/CE. De tal forma, cuando el art. 8.2 CDF autoriza el tratamiento basado en una causa legal legítima, los criterios que nos permitirían constatar tal legitimidad serían aquéllos a los que hace referencia la Directiva (celebración de un contrato, contactos precontractuales, existencia de una obligación legal, defensa de un interés vital del titular de los datos, etc.).

La CDF tampoco dice nada acerca de los límites del derecho pero, por el reenvío que hace el art. 52.3 CDF, habrán de reunir los requisitos del art. 8.2 CEDH³⁶, tal y como son interpretados por el TEDH. Esto es algo que

³⁵ Cfr. E. BATTAGLIA y G. DI FEDERICO, "La Carta dei diritti e la tutela della riservatezza", en L. SERENA ROSSI (Coord.): *Carta dei diritti fondamentali e costituzione dell'Unione Europea*, Giuffrè, Milán, 2002, pp. 220-221.

³⁶ Salvo en supuestos tasados que, en cualquier caso, estarán previstos por ley y deberán responder a necesidades legítimas de las sociedades democráticas, no puede haber injerencias por parte de la autoridad pública en su ejercicio.

hemos visto refrendado a nivel jurisprudencial en la STJCE de mayo de 2003. En ella el Tribunal declara que los órganos jurisdiccionales nacionales austriacos deben valorar si la normativa que impone la divulgación del nombre de ciertos trabajadores de entidades sujetas al Tribunal de Cuentas de su país, junto con el importe de sus ingresos anuales, es necesaria en una sociedad democrática y apropiada para lograr el objetivo de buena gestión de los recursos públicos, como obliga a realizar el CEDH.

El precepto se cierra exigiendo la creación de una autoridad independiente que vele por el respeto real a este derecho fundamental, garantía institucional presente igual en la Directiva 95/46/CE y en el art. 286 TCE. Su existencia, aunque no se cite expresamente en la Directiva 95/46/CE como criterio para enjuiciar la adecuación de la tutela a este derecho brindada en terceros Estados, es determinante para obtener semejante reconocimiento.

Por último, el sistema instaurado en la CDF no es especialmente innovador en cuanto al modo en que los derechos fundamentales son tutelados en la Unión Europea. Siguen coexistiendo varios regímenes protectores (art. 52.2 CDF) y, pese a la manera en que los derechos estén conformados en la Carta, siempre se aplicará el estándar más alto (ya sea el de los Tratados, del CEDH —art. 8.1 y Convenio número 108 del Consejo de Europa, en nuestro ámbito de estudio— o de los Ordenamientos nacionales). Esta complejidad, amén de abrir la puerta a conflictos entre Ordenamientos³⁷, puede facilitar la comisión de errores cuando los operadores jurídicos vayan a identificar cuál es el estándar más elevado³⁸.

En suma, aunque en la cumbre de Niza se decidiera proclamar la Carta, sin otorgarle eficacia jurídica, es profundamente positivo que, lo que inicialmente se concibió como un obstáculo para la consecución de ciertos objetivos económicos valiosos, salvaguardándose sólo colateralmente para no frenar el enérgico avance del mercado interior, se haya desprendido de esa servidumbre y se intente tutelar desde las instancias comunitarias como derecho fundamental que es.

³⁷ Cfr. C. RUIZ MIGUEL, "El derecho a la protección de los datos personales...", op. cit., pp. 8-10 y, con más detalle, S. SANZ CABALLERO, "Interferencias entre el Derecho comunitario y el Convenio Europeo de Derechos Humanos (Luxemburgo versus Estrasburgo: ¿quién es la última instancia de los derechos fundamentales en Europa?)", RDCE, núm. 17, Enero-Abril 2004, pp. 117-158.

³⁸ En este sentido, T. FREIXES SANJUÁN y J.C. REMOTTI, *El futuro de Europa. Constitución y derechos fundamentales*, Minim, Valencia, 2002, p. 96.

6. LOS ARTS. I-51 Y II-68 DE LA CONSTITUCIÓN EUROPEA

Llegamos al tramo final de nuestro recorrido. El Tratado por el que se instituye una Constitución para Europa, firmado en Roma en octubre de 2004, al margen de la relevancia que per se posee y de los nuevos aspectos que regula, presenta una doble relevancia desde el punto de vista de la protección de datos personales.

Evidentemente destaca la dación de valor jurídico a la Carta de los Derechos Fundamentales y, con ella, del art. 8 CDF que pasa a ser el art. II-68³⁹. Y, a propósito de los tratamientos de datos personales en la esfera institucional, hay que partir de que la Constitución Europea consagra la desaparición de los pilares y da la posibilidad de que el Tribunal de Justicia de la Unión Europea fiscalice las actividades enmarcadas en el tercer pilar como, al mismo tiempo, reconoce al Parlamento una cierta capacidad de intervención en este ámbito. Además, comienza a ser recurrente citar el art. I-51 (hasta la últimas versiones del Tratado, art. I-50) como expresión de una futura unificación de criterios en cuanto a las garantías de este derecho fundamental, tanto en el ámbito institucional de la Unión como en relación a los Estados miembros, que se augura exitosa. Empero, las últimas modificaciones del texto constitucional obligan a ser más críticos con su presunta ejemplaridad.

La redacción del art. I-51 ha sufrido, tanto en los trabajos de la Convención como posteriormente, sucesivas modificaciones. Vayamos, pues, paso

³⁹ En la Declaración número 12 del Acta final, relativa a las explicaciones sobre la Carta de los Derechos Fundamentales, se reconoce el valor interpretativo de las explicaciones sobre la Carta elaboradas bajo la autoridad del Praesidium de la Convención que redactó la Carta y actualizadas bajo la responsabilidad del Praesidium de la Convención Europea, que a propósito del derecho fundamental a la protección de datos de carácter personal son las siguientes: "Este artículo se ha basado en el artículo 286 del Tratado constitutivo de la Comunidad Europea y en la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DO L 281 de 23.11.1995, p. 31), así como en el artículo 8 del CEDH y en el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, de 28 de enero de 1981, ratificado por todos los Estados miembros. El artículo 286 del Tratado CE ha sido sustituido por el artículo I-51 de la Constitución. Conviene señalar asimismo el Reglamento (CE) nº 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos (DO L 8 de 12.1.2001, p. 1). La Directiva y el Reglamento mencionados establecen condiciones y límites para el ejercicio del derecho a la protección de los datos de carácter personal".

por paso. Al principio lo que el Praesidium se preguntó era si el art. 286 TCE debía introducirse en la sección “Ciudadanía” de la parte II del Tratado⁴⁰. Más adelante al estudiar los preceptos JAI, dedicados al espacio de libertad seguridad y justicia, se puso de relieve la exigencia de unificar el régimen legal en materia de protección de datos personales. La disparidad de criterios la que me referí anteriormente lo justificaba. A propósito del art. II-21, inspirado en el art. 30.1 TUE, se hacía el siguiente comentario: “Conviene señalar que el actual artículo 30 del TUE estipula que el intercambio de información entre los servicios nacionales, así como con Europol, se realice «con sujeción a las disposiciones correspondientes en materia de protección de datos personales». Basándose en esto, se incluyeron disposiciones en materia de protección de datos en los diversos instrumentos del tercer pilar que podían afectar a los datos personales. Se habría podido hacer una mención explícita de este tema con objeto de crear la base jurídica para mantener y desarrollar tales disposiciones. No obstante, parece más lógico, de resultados de la supresión de los pilares, permitir la creación de un régimen general de protección de datos personales, que cubra tanto el régimen comunitario actual (...) como la acción en el tercer pilar actual, sin que haya aún necesidad de dedicar una base jurídica específica en este capítulo a la protección de datos. Así pues, se propondrá un nuevo artículo general sobre la protección de datos personales, en el Título sobre la «Vida democrática», en la primera parte de la Constitución. Este artículo no sólo debería incorporar el actual artículo 286 del TCE, relativo a la acción de las instituciones y órganos de la Unión, sino también prever una base jurídica para la adopción de normas relativas al tratamiento de datos personales por parte de las autoridades de los Estados miembros cuando actúen en el ámbito de aplicación del Derecho de la Unión. Claro está que sería posible que el legislador adopte, en virtud de esta nueva base jurídica general, normas particulares de protección de datos, adaptadas al sector policial”⁴¹. Ahí está el germen del actual art. I-51.

El futuro precepto se materializa primero en la cláusula 292 del Informe del Grupo de Expertos designados por los Servicios Jurídicos del Parlamento Europeo, el Consejo y la Comisión⁴². Muy similar a su modelo (el art. 286 TCE), presentaba el siguiente tenor: “1. Los actos de la Unión relativos a la protección de las personas respecto del tratamiento de datos personales y a la libre circulación de dichos datos serán de aplicación a las instituciones

⁴⁰ CONV 529/03, de 6 de febrero.

⁴¹ CONV 614/03, de 14 de marzo.

⁴² CONV 618/03, de 17 de marzo.

y organismos establecidos por la Constitución o sobre la base de la misma. 2. El Parlamento Europeo y el Consejo adoptarán, por el procedimiento legislativo, las medidas por las que se crea un organismo de vigilancia independiente, responsable de controlar la aplicación de los actos mencionados en el apartado 1 a las instituciones y organismos de la Unión, así como cualesquiera otras medidas pertinentes”. Naturalmente, la sustitución de los términos “Comunidad” por “Unión” y “Tratado” por “Constitución” implicaba extender el alcance del art. 286 TCE a los ámbitos cubiertos por el segundo y tercer pilar, mas el texto sería modificado poco después.

Ubicado en el Título VI de la Parte I del Proyecto de Tratado (“De la vida democrática de la Unión”), capital para reflejar la preocupación expuesta en la Declaración de Laeken por aumentar la legitimidad democrática y la transparencia de las instituciones de la Unión, y tras un cambio en su numeración, el art. 36 bis⁴³ establece que: “1. Toda persona tiene derecho a la protección de los datos personales que la conciernan. 2. El Parlamento y el Consejo adoptarán, por el procedimiento legislativo, las normas sobre protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos”. Hay una modificación, pues, en la estructura del precepto. El apartado 1 vuelve a recoger el derecho consagrado en el art. 8.1 CDF. La duplicación, que se mantendrá a partir de este momento, fue tachada de innecesaria en varias propuestas de articulado⁴⁴, mas desde el Praesidium se insiste en conservarla. El derecho de acceso a los documentos y el derecho a la protección de los datos personales son juzgados por numerosos miembros de la Convención como componentes clave del particular modo de vida democrática de la Unión a nivel supranacional y parecerían incompletos si sólo contuvieran normas sobre las modalidades, límites y bases jurídicas en relación con la transparencia y la protección de datos. Al mismo tiempo, se entiende que no resulta ilógica su reaparición en la Parte II del Proyecto, puesto que así se hace hincapié en que también pertenecen a los derechos genuinamente fundamentales de la Unión⁴⁵. Por lo demás, el apartado 2 se basa en el actual régimen comunitario.

⁴³ CONV 650/03, de 2 de abril.

⁴⁴ CONV 779/03, de 4 de junio, Reacciones al proyecto de artículos del texto revisado de la Parte I.

⁴⁵ CONV 726/03, de 26 de mayo. También en el CONV 724/03, de 24 de mayo, se había advertido que a fin de introducir el apartado 2, que trata la adopción de una ley europea sobre protección de datos personales, habría que mantenerlo.

Posteriormente el precepto, que cambia al art. 50-I⁴⁶, volvería a ser retocado para adaptar la referencia al procedimiento legislativo (ley europea), añadir la mención a las agencias como destinatarias de la futura ley (buscando mantener la coherencia con los artículos anteriores del Proyecto) y prever la existencia de un órgano independiente de control. Y tampoco sería ésta la última redacción del artículo. En junio de 2003, al dar la (entonces aparente) redacción final del Proyecto de Tratado por el que se instituye una Constitución para Europa, quedaba como sigue⁴⁷: “Artículo 50: Protección de datos personales. 1. Toda persona tiene derecho a la protección de los datos personales que la conciernan. 2. Se establecerán mediante leyes europeas⁴⁸ las normas sobre protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, organismos y agencias de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. El respeto de dichas normas estará sometido al control de una autoridad independiente”.

Sin embargo, el retardo en la aprobación y firma de la Constitución Europea, tuvo algunas consecuencias inicialmente imposibles de vaticinar. Pese a que las buenas críticas que había recibido el art. I-50 no permitían prever un ulterior cambio del mismo y pese a que éste no era uno de los artículos que estaba provocando problemas en la negociación de los Estados miembros, se dio una vuelta de tuerca más. El apartado 2 del definitivo art. I-51 de la Constitución fue modificado: “Se establecerán mediante ley o ley marco europea las normas sobre protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. El respeto de dichas normas estará sometido al control de autoridades independientes”. Pasamos, entonces, al análisis del precepto.

⁴⁶ CONV 724/03, de 24 de mayo.

⁴⁷ CONV 850/03, de 18 de julio.

⁴⁸ Existía una discrepancia entre la versión española y la francesa. En la primera el art. I-50.2 anunciaba que las leyes europeas marcarían los principios de la protección de datos, mientras que la segunda reconocía que “la loi européenne fixe les règles”. El matiz no era trivial. Atendiendo a la versión española habría que deducir que se promulgarán varias leyes europeas, en función quizás de ciertas especialidades del tratamiento realizado por las instituciones y con fines policiales. Y de la versión auténtica cabría concluir que habrá una sola ley, al margen de que puedan recogerse especificidades dentro de ella.

Del primer apartado del art. I-51, aquel que proclama el derecho a la protección de datos, parece que habría poco que decir; reitera el enunciado del art. II-68 de la Constitución Europea. Mas, puesto en relación con su párrafo segundo, sí que aporta ciertas novedades en cuanto a la titularidad del derecho. No debe olvidarse que el art. II-112.2 (antes, 52.2 CDF), referido al alcance e interpretación de los derechos y principios, obliga a que los derechos de la Carta mencionados en otras partes de la Constitución se ejerzan en las condiciones y dentro de los límites determinados en éstas. Pues bien, mientras que el art. II-68 reconoce este derecho fundamental a “toda persona”, respetando que en algunos Estados miembros sean titulares del mismo las personas jurídicas, en el art. I-51.2 se introduce un matiz: habla expresamente de las personas físicas. De ahí que pueda anticiparse que las futuras normas a las que el art. I-51 remite no protegerán a las personas jurídicas.

En otro orden de consideraciones, según el anterior art. I-50 la norma que debía regular la materia era una ley, fuente equivalente al actual reglamento y, por tanto, obligatoria en todos sus elementos. No obstante, ahora podría ser también una ley marco, que, como la actual directiva, es más flexible y obliga en cuanto al resultado. Entonces surge la duda de quién elegirá el tipo de norma a utilizar y las razones que le llevarán a ello. Eso sí, dado que la Constitución Europea habla de “ley” y no utiliza el plural, debemos seguir pensando que habrá una única norma, del tipo que sea, en materia de protección de datos personales para toda la Unión, al margen de que contemple ciertas —necesarias— especificidades.

Tampoco la referencia a las autoridades de control parece muy lograda. Recordemos que hasta ahora subsisten el Supervisor Europeo y las Autoridades de Control de Schengen, del SIA, de Europol y de Eurojust. En el anterior art. I-50 se imponía la creación de una autoridad de control para todos, reforzándose así la idea de ligar esta garantía institucional al contenido mismo del derecho. Ahora, por contra, se opta definitivamente por no unificar a las autoridades de control, lo que es verdaderamente disfuncional porque seguirán multiplicándose las autoridades de control común, como las de los sistemas de información del tercer pilar, y tendrán que reunificarse sucesivamente sus secretarías. Lo más lógico hubiera sido optar por unas mismas normas, una única autoridad y un mismo procedimiento ante ella.

Para finalizar, he de aludir a la Declaración número 10 del Acta final de la Constitución Europea, que concierne al art. I-51⁴⁹: “La Conferencia decla-

⁴⁹ CIG 86/04 ADD2, de 25 de junio, referida al art. I-50 y después actualizada como Declaración número 10 al Acta final de la Constitución Europea.

ra que, siempre que las normas sobre protección de datos de carácter personal que hayan de adoptarse con arreglo al artículo I-51 puedan tener una repercusión directa en la seguridad nacional, habrán de tenerse debidamente en cuenta las características específicas de la cuestión. Recuerda que la legislación actualmente aplicable (véase, en particular, la Directiva 95/46/CE) incluye excepciones”. Como también se han introducido ciertas matizaciones en otros tantos preceptos del texto constitucional que vienen a recalcar que, en materia de seguridad nacional⁵⁰, los Estados miembros podrán establecer las restricciones oportunas al derecho fundamental a la protección de los datos de carácter personal.

Llama la atención que el derecho fundamental a la protección de datos sea “preocupante” desde el punto de vista de la seguridad nacional. Sabemos que los derechos fundamentales no son ilimitados y tampoco éste lo es. Tendrá que ceder, en bastantes ocasiones, frente a otros derechos fundamentales, intereses generales o bienes constitucionalmente protegidos, no sólo frente a la seguridad nacional. La indicación que se hace por medio de la Declaración al art. I-51 no es sino expresión del prejuicio actual que, en la lucha contra el terrorismo internacional, tienen los Estados. Tienden a percibir el derecho fundamental a la protección de datos personales como un obstáculo para la seguridad nacional, cuando no lo es.

Con todo, a pesar las críticas, no soy pesimista. Es profundamente positivo el avance hecho en cuanto al reconocimiento del valor jurídico de la Carta de los Derechos Fundamentales (y la futura adhesión al CEDH) y la mención expresa al derecho fundamental a la protección de datos, cuya

⁵⁰ En el Anexo 56 (Varios) del documento CIG 81/04, de 16 de junio, encontramos el apartado h), dedicado a la seguridad nacional y protección de datos. Las sugerencias para alcanzar un consenso en estos puntos fueron aprobadas y afectaban al: Apartado 1 del artículo I-5: 1. La Unión respetará la identidad nacional de los Estados miembros, inherente a las estructuras fundamentales políticas y constitucionales de éstos, también en lo referente a la autonomía local y regional. Respetará las funciones esenciales del Estado, en particular las que tienen por objeto garantizar su integridad territorial, mantener el orden público y salvaguardar la seguridad nacional. Artículo III-163: El presente Capítulo se entenderá sin perjuicio del ejercicio de las responsabilidades que incumben a los Estados miembros respecto del mantenimiento del orden público y de la salvaguardia de la seguridad interior. Artículo III-283: En el ejercicio de sus atribuciones por lo que respecta a las disposiciones de las Secciones 4 y 5 del Capítulo IV del Título III relativas al espacio de libertad, seguridad y justicia, el Tribunal de Justicia de la Unión Europea no será competente para comprobar la validez o proporcionalidad de operaciones efectuadas por la policía u otros servicios con funciones coercitivas de un Estado miembro, ni sobre el ejercicio de las responsabilidades que incumben a los Estados miembros respecto del mantenimiento del orden público y de la salvaguardia de la seguridad interior.

naturaleza jurídica ha sido en ocasiones puesta en discusión por la doctrina, que no terminaba de ver claro si es un derecho fundamental autónomo o sólo una faceta del derecho a la intimidad que requiere un especial desarrollo normativo. Después de un reconocimiento como el brindado ex Constitución europea, debieran despejarse las dudas que sobre esta cuestión todavía pudieran albergarse. Y también tiene que valorarse el esfuerzo realizado en pro de la unificación, en los ámbitos estatal e institucional, de los diferentes estándares existentes sobre protección de datos personales dentro de la Unión Europea.

7. RECAPITULACIÓN

La Comunidad Europea, obviando sobre todo la preocupación de su Parlamento por los peligros anejos al desarrollo tecnológico, retrasa la creación de normas sobre la protección de los datos de carácter personal. Tampoco a partir de los asuntos planteados ante el Tribunal de Justicia se había creado una doctrina jurisprudencial concerniente a este derecho fundamental. El desarrollo indirecto (y detallado) del derecho a la protección de los datos de carácter personal en el ámbito comunitario se lleva a cabo, a partir de la década de los noventa, a través de normas de Derecho derivado que se proyectan en dos ámbitos: a) el estatal, para favorecer el mercado interior sin perjudicar la tutela a los derechos fundamentales, toma de posición que obedecía a la lógica de la integración económica; b) el institucional, como modo de fomentar la transparencia en el seno de la Unión.

Gracias a estas normas puede decirse que la Unión Europea ha hecho avanzar de forma considerable el establecimiento de un sistema normativo protector de los datos personales coherente y razonablemente armonizado en Europa. Los tratamientos de datos personales han de respetar todo un elenco de principios que van a determinar su licitud con independencia de que se cuente con el consentimiento de la persona concernida. Ésta dispone, además, de una serie de derechos instrumentales que la ayudarán a saber quién detenta información suya, en qué términos la utiliza y con qué fines, y todo ello completado con otra serie de garantías como el recurso no sólo a las autoridades judiciales, sino a autoridades independientes de control, que tienen por cometido velar por la correcta aplicación de las normas sobre esta materia.

Teniendo en cuenta todo ello, es un éxito que, en primer lugar, la Unión haya abordado directamente el reconocimiento pleno y la tutela de los derechos y libertades de sus ciudadanos por medio de la Carta de los Derechos Fundamentales, a la que la Constitución Europea dota de eficacia

jurídica. Y, en segundo lugar, que el art. II-68 de la Carta Magna europea reconozca expresamente el derecho fundamental a la protección de datos personales, dándole entidad propia y desvinculándolo de otros, confirmando de forma definitiva la autonomía dogmática de un derecho fundamental cuya naturaleza jurídica ha sido puesta en discusión por parte de la doctrina.

Por otra parte, al atender al tratamiento de los datos personales en el ámbito del tercer pilar, se evidencia hasta qué punto falla el legislador en su propósito de igualar los criterios que orienten los tratamientos de datos personales realizados por las instituciones y organismos de la Unión Europea. Los grandes sistemas de información de la Unión presentan regímenes jurídicos diversos y a menudo bastante laxos en cuanto a la protección de datos personales se refiere, abiertos al intercambio de información personal con países u organizaciones que no garantizan el nivel de protección adecuado que se exige a los Estados miembros y con una falta evidente de control democrático externo, ya fuera éste ejercido por el Parlamento Europeo o por el Tribunal de Justicia de la Comunidad Europea.

En este sentido, la supresión de los pilares que preconiza la Constitución Europea genera bastantes expectativas acerca de su mejora. Muchos han sido los que entre 2003 y 2004 declararon que el art. I-51 es, en materia de protección de datos, expresión lograda de la unificación que se anhelaba mas, en mi modesta opinión, el resultado al que se ha llegado no es óptimo. No será una necesariamente una ley la que establezca las normas a seguir en toda la Unión (podría optarse por una ley marco), como tampoco se instituye una única autoridad de control y, por contra, se remarca la posibilidad de restringir este derecho fundamental por razones de seguridad nacional.

En la actualidad se subraya que el desarrollo del derecho fundamental a la protección de los datos de carácter personal, además de verse condicionado por el avance tecnológico, se halla constreñido por exigencias derivadas de la necesidad de seguridad. No está de más, entonces, recordar los términos en que el Tribunal Europeo de Derechos del Hombre se pronunció en el Asunto Klass en 1978: “Los Estados no deben (...) en nombre de la lucha contra el espionaje y el terrorismo, adoptar cualesquiera medidas consideren apropiadas... El peligro es debilitar o incluso destruir la democracia alegando defenderla”. Confiamos en que las libertades publicas en general y la protección de datos personales en particular dejen de considerarse un lastre para la seguridad de los ciudadanos lo más pronto posible.