

EL DERECHO A LA PROTECCIÓN DE LOS DATOS PERSONALES EN LA CARTA DE DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA: ANÁLISIS CRÍTICO

Por CARLOS RUIZ MIGUEL *

SUMARIO:

I. JUSTIFICACIÓN Y OBJETIVOS DE ESTE ESTUDIO.—II. LA CDF, UNA «IMPOSIBLE CONSOLIDACIÓN NORMATIVA»: 1. LA DISCUTIBLE CONFORMACIÓN DE LA CARTA DE DERECHOS FUNDAMENTALES; 2. EL CEDH Y EL CONVENIO DE 1981: A) *La legislación del Consejo de Europa*; B) *La jurisprudencia de Estrasburgo*; 3. EL DERECHO COMUNITARIO: A) *La jurisprudencia comunitaria*; B) *El Derecho comunitario derivado «autónomo»*; C) *El TCE y la legislación de desarrollo*; D) *El Tratado de la Unión Europea y el tercer pilar*; 4. OTROS INSTRUMENTOS INTERNACIONALES; 5. LAS CONSTITUCIONES DE LOS ESTADOS MIEMBROS, EN ESPECIAL, LA ESPAÑOLA.—III. EL CONTENIDO DEL DERECHO.—IV. CONCLUSIONES.

I. JUSTIFICACIÓN Y OBJETIVOS DE ESTE ESTUDIO

El estudio del derecho a la protección de datos personales, recogido en el art. 8 de la Carta de los Derechos Fundamentales de la Unión Europea nos pone de relieve, de forma agudísima y como muy pocos de los demás derechos de la CDF lo hacen (quizás los derechos de propiedad, igualdad, sufragio, libertad de circulación), una serie de problemas normativos que se derivan de la discutible conformación de los derechos que

* Catedrático de Derecho Constitucional, Universidad de Santiago de Compostela.

resulta de la Carta. La Carta de los Derechos Fundamentales nace en cumplimiento del mandato de la cumbre de Colonia de junio de 1999. En dicha cumbre se acordó, en primer lugar, que «en el presente estado de la Unión Europea, los derechos fundamentales *aplicables en el nivel comunitario* deberían consolidarse en una Carta para hacerse más evidentes» (n.º 44). Además, en segundo lugar, se acordó que el citado documento debiera recoger los derechos de los «ciudadanos europeos».

En este trabajo intentamos argumentar que la CDF no ha constituido un desarrollo adecuado de este mandato y no ha dado una respuesta satisfactoria a las dificultades planteadas. Dejaremos de lado algunas cuestiones, como las de la discutible ubicación sistemática del derecho a la protección de datos en la Carta (como un derecho distinto del de la intimidad, contradiciendo el Derecho del sistema del Consejo de Europa, el propio Derecho comunitario derivado y varias Constituciones nacionales), la titularidad del derecho (con su problemático desarrollo del mandato de la cumbre de Colonia), sus límites y garantías. Tras la crítica del intento de consolidación formal del derecho (a nuestro juicio, fallido) enjuiciaremos el contenido consagrado (en nuestra opinión, insuficiente).

II. LA CDF, UNA «IMPOSIBLE CONSOLIDACIÓN NORMATIVA.»

1. LA DISCUTIBLE CONFORMACIÓN DE LA CARTA DE DERECHOS FUNDAMENTALES

A) La CDF nace bajo un mandato de realizar una «consolidación» (algo así como un «texto refundido») de los derechos fundamentales aplicables en el nivel comunitario. Pero si los capítulos I a V tratan, con más o menos fortuna, de cumplir ese cometido, el capítulo VI introduce unas gravísimas perturbaciones. La fuente principal de todos estos problemas se encuentra en los arts. 52 y 53 CDF. Una lectura de estos dos preceptos nos pone de relieve que, aunque aparentemente la CDF establece «una Carta», «un estatuto» para los derechos, lo cierto es que la CDF no hace sino consagrar la existencia de «varios» estatutos y aun posibilitar la adición de un nuevo estatuto a los anteriores, que sería la propia Carta. De la lectura de estos dos preceptos se desprende que la CDF es un instrumento normativo «complementario» de otros. No cumple, por tanto, la tarea de «consolidar» los derechos «aplicables» en «el nivel comunitario».

Por un lado, el art. 52.2 CDF dice que los derechos que estén reconocidos en la Carta, pero que tengan su fundamento «en los Tratados comunitarios o en el Tratado de la Unión Europea se ejercerán en las condiciones y dentro de los límites determinados por estos». De ello se deduce que cuando un derecho aparezca a la vez en la CDF y en el TCE o en el TUE, serán estos últimos quienes determinarán su régimen jurídico («condiciones» y «límites»). Difícilmente puede «consolidarse» en la CDF un régimen jurídico, cuando la propia CDF consagra la validez comunitaria de regímenes diversos.

Por su parte, el art. 52.3 CDF establece que en la medida en que la Carta contenga derechos «que correspondan a derechos garantizados por el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, su sentido y alcance serán iguales a los que les confiere dicho Convenio». Pero con una salvedad, y es que esto no impedirá «que el Derecho de la Unión conceda una protección más extensa». Esto significa que, si un derecho aparece a la vez en la CDF y en el CEDH, su régimen jurídico («sentido y alcance») será el propio del CEDH a menos que la CDF permita una protección más extensa. El problema es que no está claro que la cláusula del art. 6.2 TUE («la Unión respetará los derechos fundamentales tal y como se garantizan en el Convenio Europeo para la protección de los derechos humanos») signifique que los derechos del CEDH sean «aplicables en el nivel comunitario».

Finalmente, el art. 53 CDF prescribe que ninguna disposición de la Carta se puede interpretar como «limitativa o lesiva de los derechos humanos y libertades fundamentales reconocidos en su respectivo ámbito de aplicación, por el Derecho de la Unión, el Derecho internacional y los convenios internacionales de los que son parte la Unión, la Comunidad o los Estados miembros, y en particular el Convenio Europeo para la protección de las libertades fundamentales, así como por las Constituciones de los Estados miembros». Este precepto significa dos cosas: en primer lugar, que la CDF no abroga los derechos humanos o fundamentales «reconocidos en su respectivo ámbito de aplicación»; y en segundo lugar, que esos derechos no sólo son los que estén reconocidos en el «Derecho de la Unión» (algo próximo al art. 52.2 CDF) y en el «CEDH» (ya dicho en el art. 52.3 CDF), sino también los reconocidos en otros tratados internacionales en los que sean partes la Comunidad o los Estados miembros y los reconocidos en sus Constituciones.

B) El texto últimamente citado del art. 53 CDF nos revela otro pro-

blema planteado por la Carta. Según el mandato de la cumbre de Colonia de junio de 1999, «en el presente estado de la Unión Europea, los derechos fundamentales aplicables *en el nivel comunitario* deberían consolidarse en una Carta para hacerse más evidentes» (n.º 44). El hecho de que el art. 53 introduzca una referencia a los derechos fundamentales de las Constituciones de los Estados (y no ya sólo a las «tradiciones constitucionales comunes», como hizo el anexo IV de las conclusiones de la Cumbre de Colonia) resulta especialmente problemático. En efecto, dado que la Carta tiene como misión consolidar los derechos aplicables «en el nivel comunitario» una de dos: o los derechos fundamentales de las Constituciones de los Estados (y no las «tradiciones constitucionales comunes») se aplican «en el nivel comunitario» o no se aplican en ese nivel.

Si es lo primero, esto es, que los derechos fundamentales de las Constituciones estatales como tales (es decir, no como «tradiciones constitucionales comunes») *sí* se aplican en el nivel comunitario, parece que la Cumbre de Colonia formuló mal su mandato ya que en lugar de inclinarse por el «estándar mínimo» de protección parece que tendría que haberse inclinado por el «estándar máximo» con todos los problemas que ello plantea.

Si es lo segundo, es decir, que los derechos fundamentales de las Constituciones de los Estados *no* se aplican en el nivel comunitario (como parece que se desprende de las conclusiones de la Cumbre de Colonia), carece de sentido la referencia a los derechos de las Constituciones internas que hace el art. 53 CDF pues ¿cómo va una Carta de derechos «en el nivel comunitario» a limitar los derechos que las Constituciones garantizan «en el nivel estatal»?

C) En definitiva, la CDF presenta dos problemas de entrada: por un lado, no establece un estatuto jurídico único para el derecho a la protección de los datos personales, sino más bien una multiplicidad de regímenes, todos ellos válidos, cuya aplicación eventualmente se solapa; por otro lado, es ambigua al determinar la cuestión de si los derechos de las Constituciones estatales tienen fuerza normativa, como tales, «en el nivel europeo».

Todo ello nos obliga a examinar no sólo la CDF en sí, sino también qué regulación existe sobre el derecho a la protección de datos en el Derecho comunitario (originario y derivado), en el sistema del Consejo de Europa, en otros tratados y, finalmente, en las Constituciones de los Estados.

2. EL CEDH Y EL CONVENIO DE 1981 DEL CONSEJO DE EUROPA

A) *La legislación del Consejo de Europa*

La *legislación* del Consejo de Europa sobre este particular se concentra en dos instrumentos fundamentales, aunque se puede añadir algún otro. El primero es el Convenio Europeo de Derechos Humanos (CEDH) de 1950 y el segundo es el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal de 1981 (C1981). Cabe añadir también alguna referencia al Convenio de prevención de la tortura de 1987 (C1987). El examen de estos instrumentos nos revela que en el sistema del Consejo de Europa el derecho a la protección de datos personales no es sino una manifestación específica del derecho al respeto de la vida privada.

a) El *CEDH*, en su artículo 8 dispone en su apartado primero que «toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia» para añadir en el apartado segundo las condiciones en las que ese derecho se puede limitar. De acuerdo con el Convenio, el derecho al respeto de la vida privada puede ser limitado cuando se den varias circunstancias. En primer lugar, que la limitación esté «prevista en la ley»; en segundo lugar, que la misma sea «necesaria» en una «sociedad democrática»; y, en tercer lugar, que pretenda proteger una serie de bienes y derechos («la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás»)¹.

b) Desde 1969 la Asamblea Parlamentaria del Consejo de Europa planteó al Comité de Ministros la cuestión de si el art. 8 CEDH resultaba suficiente para preservar a los individuos frente al uso abusivo de la informática. Ante la respuesta negativa del órgano ministerial, el Comité de Ministros del Consejo de Europa aprobó dos resoluciones sobre la materia² que prepararon el terreno al Convenio. El *Convenio de 1981*

¹ Sobre el derecho del art. 8 CEDH véase mi libro *El derecho a la protección de la vida privada en la jurisprudencia del Tribunal Europeo de Derechos Humanos*, Civitas, Madrid, 1994. La cuestión de los límites se halla desarrollada en pp. 84-121.

² Resolución (73) 22 sobre la protección de la vida privada de las personas físicas respecto a los bancos de datos electrónicos en el sector privado, adoptada por

(C1981)³, entró en vigor el 1 de octubre de 1985 tras recibir el oportuno número de ratificaciones. Este instrumento se concibe como un desarrollo del derecho a la protección de la vida privada en un ámbito específico, el del tratamiento de datos personales. Así se desprende del preámbulo y del art. 1 C1981⁴.

El 8 de noviembre de 2001 se firmó un protocolo adicional al convenio de 1981, que añadía dos nuevos artículos al C1981. Estos dos artículos versan, el primero, sobre la obligación de los Estados partes de establecer una «garantía institucional» u organismo independiente de control para supervisar la aplicación de los derechos reconocidos en el C1981; el segundo, por su parte, pretende establecer una serie de cautelas en relación con el flujo transfronterizo de datos. Este protocolo hasta ahora no ha entrado en vigor.

c) Junto a los textos anteriores, cabe añadir que el Convenio para la prevención de la tortura de 1987 (C1987) crea un «Comité Europeo para la prevención de la tortura y de las penas o tratos inhumanos o degradantes» con competencia para realizar visitas en cualquier centro de detención de un Estado parte (art. 1 C1987). Como parte de sus atribuciones, después de cada visita el Comité realizará un informe. El Convenio establece, sin embargo, que en dichos informes «no se publicará ningún dato personal sin el expreso consentimiento de la persona afectada» (art. 11.3 C1987). Estamos, no obstante ante un caso muy particular de uso de datos personales.

el Comité de Ministros el 26 de septiembre de 1973; Resolución (74) 29 sobre la protección de la vida privada de las personas físicas respecto a los bancos de datos electrónicos en el sector público, adoptada por el Comité de Ministros el 20 de septiembre de 1974.

³ Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, de 28 de enero de 1981 (ratificado por España el 27 de enero de 1984 y publicado en el B.O.E. de 15 de noviembre de 1985).

⁴ Preámbulo: «es deseable ampliar la protección de los derechos y de las libertades fundamentales de cada uno, concretamente el derecho al respeto a la vida privada, teniendo en cuenta la intensificación de la circulación a través de las fronteras de los datos de carácter personal que son objeto de tratamientos automatizados»; art. 1: «El fin del presente Convenio es garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, *concretamente su derecho a la vida privada*, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona («protección de datos»)) (cursiva mía).

B) *La jurisprudencia de Estrasburgo*

La *jurisprudencia* de Estrasburgo fue mucho más lejos de lo que previeron los demás órganos del Consejo de Europa. Así se desprende de los dos principios básicos que ha establecido en esta materia. En primer lugar, que la protección de datos personales forma parte del derecho al respeto de la vida privada (desautorizando así al Comité de Ministros que dio la respuesta contraria a la Asamblea Consultiva) y, en segundo lugar, que en la regulación de ese derecho los Estados gozan de un amplio margen de apreciación.

En primer lugar, de forma constante, el TEDH⁵ ha interpretado el derecho al respeto de la vida privada en un sentido amplio⁶. Según el TEDH «esta interpretación amplia se corresponde con la del Convenio del Consejo de Europa de 28 de febrero de 1981 para la protección de los individuos respecto al tratamiento automatizado de datos personales que entró en vigor el 1 de octubre de 1985, cuyo propósito es ‘asegurar en el territorio de cada Parte a todos los individuos... respeto para sus derechos y libertades fundamentales y en particular su derecho a la intimidad respecto al tratamiento automatizado de datos personales que le afecten’, quedando definidos tales datos personales como ‘cualquier información relativa a un individuo identificado o identificable’»⁷.

De ahí que no se pueda decir que para el TEDH, la protección de datos personales no constituye un «derecho autónomo» y distinto del derecho a la intimidad. Esta afirmación se ha desarrollado de modo paulatino. Inicialmente (en el *caso Gaskin*), el TEDH concedió que en el caso concreto el acceso a ciertos datos (que habían sido objeto de tratamiento automatizado) y que afectaban a la vida privada del recurrente quedaba protegido por el art. 8 CEDH, aunque «esta conclusión se obtiene sin inclinarse por ninguna opinión acerca de si los derechos generales de acce-

⁵ STEDH A 116 Leander v. Suecia, de 26 de marzo de 1987 (1987) 9 *E.H.R.R.* 433 (n.º 48, p. 450).

⁶ Ya la STEDH A 251-B Niemitz v. Alemania, de (1993) 16 *E.H.R.R.* 97 (n.º 56, p. 106) reconocía que el derecho al respeto de la vida privada y del domicilio abarcaba actividades profesionales o comerciales. También es interesante la interpretación amplia que ofrece la STEDH Friedl v. Austria, de 31 de enero de 1995 (1996) 21 *E.H.R.R.* 83 (n.º 44, p. 87),

⁷ STEDH Amann v. Suiza, de 16 de febrero de 2000, (2000) 30 *E.H.R.R.* 843 (n.º 65, p. 871).

so a los datos personales y a la información puede derivarse del artículo 8 (1) del Convenio», ya que el Tribunal «no está llamado a decidir *in abstracto* sobre cuestiones generales de principios en este terreno, sino a solventar el caso concreto de la demanda del Sr. Gaskin»⁸.

Sin embargo, posteriormente, el tribunal ha determinado ya sin ambigüedades que la protección de datos personales «tiene una importancia fundamental para el disfrute por una persona de su derecho al respeto de la vida privada y familiar garantizado en el artículo 8 del Convenio». Este principio general se agudiza aún más si se trata de datos relativos a la salud, ya que en tales casos, según el tribunal, el respeto de la confidencialidad es «crucial no sólo para respetar el sentimiento de intimidad del paciente, sino también para preservar su confianza en la profesión médica y en los servicios sanitarios en general» ya que «sin tal protección aquellos que precisan de asistencia médica podrían disuadirse de revelar tal información de naturaleza personal e íntima para obtener el apropiado tratamiento o incluso de buscar tratamiento médico, con lo que pondrían en peligro su propia salud y, en caso de enfermedades contagiosas, incluso la salud de la comunidad»⁹.

En segundo lugar, el mismo tribunal ha establecido que en las cuestiones relativas al acceso por el público a datos personales, las autoridades nacionales gozan de un «margen de apreciación» para sopesar el alcance de la reserva de los datos personales, que depende de diversos factores, como la naturaleza o entidad de los intereses en juego y la gravedad de la interferencia¹⁰.

3. EL DERECHO COMUNITARIO

El primer peldaño en la investigación es la averiguación de cuales son las «condiciones» y «límites» que «los Tratados comunitarios o (...) el Tratado de la Unión Europea» fundamentan (art. 52.2 CDF) para el dere-

⁸ STEDH A 160 Gaskin v. Reino Unido, de 7 de julio de 1989 (1990) 12 E.H.R.R. 36 (n.º 37, p. 45).

⁹ STEDH Z v. Finlandia, de 25 de Febrero de 1997, (1998) 25 E.H.R.R. 371 (n.º 94, p. 405-406); STEDH MS v. Suecia, de 27 de agosto de 1997 (1999) 28 E.H.R.R. 313 (n.º 41, p. 338).

¹⁰ STEDH Z v. Finlandia, de 25 de Febrero de 1997, (1998) 25 E.H.R.R. 371 (n.º 99, p. 407); STEDH MS v. Suecia, de 27 de agosto de 1997 (1999) 28 E.H.R.R. 313 (n.º 41, p. 338).

cho a la protección de datos personales. El reconocimiento del derecho a la protección de los datos personales en el Derecho Comunitario se ha hecho en etapas diversas, tanto en el nivel jurisprudencial como en el legislativo. A diferencia de lo sucedido con otros derechos, el que protege los datos personales no fue introducido en el ordenamiento comunitario por la jurisprudencia, sino por la legislación.

A) *La jurisprudencia comunitaria*

La *jurisprudencia* se ha enfrentado con cuestiones relativas al derecho a la protección de datos antes de que existiera legislación europea al respecto. Los órganos judiciales comunitarios, han reconocido que el derecho a la intimidad, reconocido en el art. 8 CEDH y derivado de las tradiciones constitucionales a los Estados miembros, es uno de los derechos fundamentales protegidos en el ordenamiento comunitario¹¹. Sin embargo, la jurisprudencia ha rehusado conectar expresamente el derecho a la protección de datos personales con el que protege la vida privada, aunque en algún caso esa conexión pueda parecer implícita.

Quizás el primer caso estudiado por el TJCE que tiene relación con el derecho a la protección de datos es el importante *caso Stauder*¹². En este asunto el tribunal tuvo que decidir si el hecho de supeditar el suministro de mantequilla con precios reducidos al hecho de que se suministrara a los vendedores previamente el nombre de los beneficiarios. Aunque el recurrente no alegó expresamente el derecho a la protección de datos personales era éste, sin embargo, el que se hallaba en juego en esa ocasión. El tribunal afirmó que la directiva admitía varias lecturas en las distintas versiones y que no imponía ni prohibía la identificación nominal de los beneficiarios de ese tipo de ayudas, concluyendo que así no había ningún elemento que permitiera «cuestionar los derechos fundamentales de la persona subyacentes en los principios generales del Derecho comunitario, cuyo respeto garantiza el tribunal». Como se ve, el tribunal eludió claramente identificar un derecho a la vida privada o a la protección de datos personales como tales.

¹¹ Sentencia del Tribunal de Justicia, de 8 de abril de 1992 (C-62/90), Comisión v. Alemania [1992] Rec. I-2575 (párrafo 23).

¹² Sentencia del Tribunal de Justicia de 12 de noviembre de 1969, Erich Stauder v. Stadt Ulm-Sozialamt, de 12 de noviembre de 1969 (C 29/69) Rec. 1969, p. 419.

El derecho a la protección de datos es el objeto (no expresamente invocado pero indudablemente subyacente) de un interesante caso de 1994, el *asunto Campogrande*¹³. En este asunto, como consecuencia de una condena en rebeldía en un litigio civil, la Sra. Campogrande comprobó, en junio de 1989, que su nombre y el de su esposo figuraban en el Registro del Ayuntamiento de Ixelles, en una dirección que desde 1981 ya no era la suya. Tal inscripción obedecía al hecho de que, con arreglo al Acuerdo entre las Instituciones de las Comunidades Europeas radicadas en Bélgica y el Gobierno belga en materia de información relativa a los funcionarios de tales Instituciones, celebrado el 3 de abril de 1987, la Comisión había transmitido la dirección de la Sra. Campogrande a las autoridades belgas, las cuales informaron al municipio afectado (apartado 6). El artículo 1 del Acuerdo prevé que las Instituciones europeas notificarán al ministerio de Asuntos exteriores belga, «dos veces por año, los datos relacionados con sus funcionarios y otros agentes» consistentes en «el nombre y apellidos, así como la residencia principal». El 9 de diciembre de 1987, la administración de la Comisión pidió a los funcionarios de esta Institución radicados en Bélgica que rellenasen un cuestionario destinado a actualizar sus datos personales, a fin de que éstos pudiesen ser transmitidos a las autoridades belgas, de conformidad con el Acuerdo. La Sra. Campogrande no sólo no rellenó dicho cuestionario, sino que además presentó una reclamación mediante la cual negaba el derecho de la Comisión a transmitir su nombre, apellidos y dirección a las autoridades belgas y pedía a aquella Institución que denunciase el Acuerdo. Al tramitar dicha reclamación, la Comisión pudo comprobar que con posterioridad a su mudanza al municipio de Ixelles, el 22 de enero de 1979, la Sra. Campogrande no había comunicado a la administración la modificación de su dirección particular (apartado 7). El Director de Personal pidió en varias ocasiones a la Sra. Campogrande que comunicase a la administración comunitaria su dirección particular, con apercibimiento de incoar un procedimiento disciplinario. Ante su reiterada negativa a facilitar la referida información, se incoó un procedimiento disciplinario contra la Sra. Campogrande. El 13 de febrero de 1991, le fue impuesta la sanción de amonestación (sanción prevista en la letra b del apartado 2 del artículo 86 del Estatuto). Esta sanción fue recurrida al tribunal de primera instancia por la Sra. Campogrande.

¹³ Sentencia del Tribunal de Justicia (Sala Quinta), de 21 de abril de 1994 (C-22/93), Anna-Maria Campogrande v Comisión de las Comunidades Europeas [1994] Rec. I-1375.

grande alegando, entre otros motivos que que ella habría estado dispuesta a comunicar a la Comisión su dirección particular si esta Institución le hubiera garantizado que tal información no se transcribiría en las Oficinas de Empadronamiento del Reino de Bélgica. Esta pretensión fue rechazada por el Tribunal de primera instancia¹⁴. El TJ también rechazó la pretensión de Campogrande aplicando en su literalidad el párrafo segundo del artículo 16 del Protocolo que dispone que «periódicamente se comunicará a los Gobiernos de los Estados miembros el nombre, función y dirección de los funcionarios [...]». Según el tribunal, «del texto mismo de esta disposición se desprende que la Comisión no sólo tenía el derecho, sino también la obligación de comunicar a las autoridades belgas la dirección particular de la Sra. Campogrande». De esta sentencia, cabe concluir, en definitiva, que el TJ no se cuestionó en ningún momento si el Acuerdo entre las instituciones europeas y el gobierno belga vulneraba el derecho a la protección de datos personales al permitir la transferencia al gobierno belga de datos personales de los funcionarios europeos sin contar con su consentimiento.

De forma menos clara, el derecho a la protección de datos subyace en el caso *X contra Comisión*¹⁵, en el que el TJ invoca el derecho a la intimidad para anular un acto de la Comisión. En este asunto, una persona aduce que, en el examen médico requerido para acceder a un empleo por las Comunidades, el servicio médico le practicó sin su consentimiento unos tests que permitían conocer si padecía SIDA. La Comisión, sin su consentimiento, utilizó los datos obrantes en los tests médicos con la consecuencia de que no se le admitió para el trabajo solicitado.

El problema de la eventual relación del derecho a la protección de datos con el derecho a la intimidad también ha tenido cierto tratamiento jurisprudencial. En otros órdenes normativos (Consejo de Europa, ordenamientos constitucionales finlandés, holandés y español) o en la legislación comunitaria el llamado derecho a la protección de datos aparece expresamente vinculado al derecho a la vida privada o a la intimidad. Sin embargo, la jurisprudencia comunitaria no ha mencionado esta conexión, aunque la misma fue convenientemente recordada en vía de informe. En efecto, en

¹⁴ Sentencia del Tribunal de Primera Instancia de las Comunidades Europeas (Sala Tercera) el 19 de noviembre de 1992, Campogrande/Comisión (T-80/91) [1992] Rec. II-2459).

¹⁵ Sentencia del Tribunal de Justicia, de 5 de octubre de 1994, X contra Comisión (C-404/92) [1994] Rec. I-4737.

el caso *Reina v. Ministerio de Agricultura*, el Gobierno británico afirmó que la protección de datos con arreglo al artículo 9 del reglamento impugnado también se refería a la confidencialidad de los datos, amparados por el artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos (protección de la vida privada)¹⁶, si bien la sentencia omite cualquier referencia a ese precepto del Convenio¹⁷.

B) *El Derecho comunitario derivado «autónomo»*

La legislación sobre este derecho, en un primer momento, se realizó a través de una serie de directivas y, más tarde mediante el reconocimiento por el propio TCEE y el TUE y legislación concordante. El derecho a la protección de los datos personales aparece, en primer lugar, en una directiva de 1995, a la que se sumó después otra de 1997, recientemente sustituida por una reciente de 2002. Todas ellas conectan el derecho a la protección de datos personales con el derecho al respeto de la vida privada. Antes de examinar las directivas, procede, sin embargo, estudiar la cuestión de la legitimidad competencial de las mismas.

a) Al tratarse de directivas, sus destinatarios son, lógicamente, los Estados miembros. Esto nos obliga a plantear una cuestión previa, y muy importante, que es la de si la CE tenía (tiene) competencia para aprobar tales directivas que afectaban a un derecho fundamental, pues en ese momento los tratados ni habían consagrado específicamente el derecho a la protección de datos personales cuyo destinatario fueran los Estados, ni siquiera habían otorgado a las Comunidades o a la Unión competencia en materia de derechos fundamentales. En definitiva, ¿tenían las directivas cobertura suficiente en el Derecho primario o suponían (suponen) una invasión de competencias de los Estados por parte de la CE? La Dir95 y la Dir97 afirman que «el establecimiento y funcionamiento del mercado interior, dentro del cual está garantizada, con arreglo al artículo 7 A del Tratado, la libre circulación de mercancías, personas, servicios y capita-

¹⁶ Así se recoge en las Conclusiones del Abogado General Siegbert Alber presentadas el 10 de febrero de 2000, Asunto C- 369/98, *The Queen v Minister of Agriculture, Fisheries and Food*, ex parte Trevor Robert Fisher and Penny Fisher.

¹⁷ Sentencia del Tribunal de Justicia (Sala Cuarta) de 14 de septiembre de 2000 (C- 369/98), *The Queen v Minister of Agriculture, Fisheries and Food*, ex parte Trevor Robert Fisher and Penny Fisher [2000] Rec I-6751

les, hacen necesaria no sólo la libre circulación de datos personales de un Estado miembro a otro, sino también la protección de los derechos fundamentales de las personas». Este mismo texto procura evitar acusaciones de invasión de competencias declarando que «los principios de la protección deben aplicarse a todos los tratamientos de datos personales cuando las actividades del responsable del tratamiento entren en el ámbito de aplicación del Derecho comunitario» excluyendo únicamente «el ejercicio de actividades exclusivamente personales o domésticas» (párrafo 12 del Preámbulo de la Dir95). Ahora bien, ¿es esta una justificación convincente?

Aunque las directivas sobre protección de datos no han sido recurridas, encontramos en la jurisprudencia un caso de gran proximidad en el que se planteó ante el TJ la cuestión de si la competencia para aprobar un reglamento sobre asistencia entre administraciones (que preveía la creación de un sistema automatizado de información, denominado «Sistema de información aduanera», SIA)¹⁸, correspondía sólo al Consejo o debía corresponder también al Parlamento. Según el artículo 34, apartado 1, del Reglamento impugnado, el partícipe en el SIA que quiera obtener o introducir datos personales en el SIA debe adoptar, como muy tarde en el momento de la aplicabilidad del Reglamento mencionado, una legislación nacional o normas internas que se apliquen en la Comisión, que garanticen la protección de los derechos y libertades de las personas en lo que se refiere al tratamiento de los datos personales.

En su argumentación, el Tribunal consideró que «según el decimoquinto considerando del Reglamento impugnado, con el fin de poder participar en el SIA, los Estados miembros deben adoptar disposiciones legales relativas a los derechos y libertades de las personas en lo que se refiere al tratamiento de datos personales». A la espera de la aplicación de las medidas nacionales que incorporaron la Directiva 95/46/CE, según el reglamento los Estados miembros debían garantizar un nivel de protección que se inspirara en los principios contenidos en dicha Directiva. El tribunal estimó que el SIA (establecido en el reglamento 515/97) no tenía, en sí mismo, la vocación de proceder a un acercamiento de las legislaciones nacionales, por lo que era de aplicación el artículo 95 (antiguo 100 A) del Tratado, ya que tal aproximación de las legislaciones nacionales sólo

¹⁸ Reglamento (CE) n. 515/97 del Consejo, de 13 de marzo de 1997, relativo a la asistencia mutua entre las autoridades administrativas de los Estados miembros y a la colaboración entre éstas y la Comisión con objeto de asegurar la correcta aplicación de las reglamentaciones aduanera y agraria (DO L 82, p. 1).

era un efecto accesorio de la reglamentación mencionada¹⁹. En definitiva, el Tribunal de Justicia venía a decir que el establecimiento del «mercado interior» (art. 95 TCE en conexión con el art. 14 TCE) constituía título suficiente para introducir legislación comunitaria en materia de protección de datos personales.

Esta argumentación resulta, a nuestro juicio, extraordinariamente discutible. Y lo es tanto por razones, digamos «sustantivas» que «formales».

Sustantivamente, esta normativa es discutible porque si la armonización de legislaciones en materia del derecho a la protección de datos personales es un elemento para el establecimiento del «mercado interior», ¿qué impediría a la Comunidad legislar en materia de inviolabilidad del domicilio o del secreto de las comunicaciones arguyendo que la misma se aplicaría únicamente a «actividades del responsable que entren en el ámbito de aplicación del Derecho comunitario»? En efecto, es sabido que ha habido varios casos en los que se ha puesto de manifiesto como la legislación nacional sobre estos derechos interfería con las normas comunitarias sobre Derecho de la competencia²⁰. Por lo demás, la aceptación de este razonamiento nos llevaría muy lejos: ¿tendría también la Comunidad competencia para dictar una normativa sobre el derecho a la libertad religiosa? No olvidemos que el ejercicio de esta libertad afecta a cuestiones que entran en el ámbito de aplicación del Derecho comunitario (consumo y prohibición de ciertos alimentos [p. ej., carne en general o carnes porcinas o vacunas en especial], prohibición de ciertos tráfico de capitales, prohibición de trabajar en ciertas fechas, etc.). Las mismas consideraciones podrían hacerse respecto a otros derechos como la libertad de asociación, la libertad sindical, el derecho de huelga, ... En definitiva, la consideración del derecho a la protección de datos personales como un elemento del «mercado interior» resulta, cuando menos discutible.

Sucede además, desde un punto de vista sustantivo, que el propio TJ sostuvo que la Comunidad Europea *no* tenía competencia sobre regulación de derechos fundamentales en su dictamen sobre la adhesión de las Co-

¹⁹ Sentencia del Tribunal de Justicia (Sala Sexta), de 18 de noviembre de 1999 (C-209/97), Comisión de las Comunidades Europeas v. Consejo de la Unión Europea [1999] Rec I-8067

²⁰ Sentencia del Tribunal de Justicia, de 26 de junio de 1980 (C-136/79), National Panasonic Ltd. v. Comisión, Rec. 1980, p. 2033 ss.; Sentencia del Tribunal de Justicia, de 18 de mayo de 1982 (C-155/79), AM&S Europe Ltd. v. Comisión, Rec. 1982, p. 1575 ss.; Sentencia del Tribunal de Justicia, de 21 de septiembre de 1989 (C-46/87 y 227/88), Hoechst AG v. Comisión, Rec. 1989, p. 2919 ss.

munidades al CEDH²¹ y está claro que no encontraremos en los tratados esa competencia para regular el derecho fundamental a la intimidad o a la protección de datos personales.

Formalmente, la asunción de competencias en materia de protección de datos personales es difícilmente compatible con el principio de subsidiariedad (art. 5 TCE), tal y como lo interpretan los tratados y la propia jurisprudencia del TJ.

Si tomamos como criterio el «Protocolo sobre la aplicación de los principios de subsidiariedad y proporcionalidad» anejo con el n.º 7 al Tratado de Amsterdam, la regulación comunitaria, aun dando por sentado que tuviera alguna base competencial, habida cuenta de que opera sobre una materia que *sí* es de los Estados (regulación de un derecho fundamental) requeriría comprobar que el asunto «presenta aspectos transnacionales que no pueden ser regulados satisfactoriamente mediante la actuación de los Estados miembros», que «las actuaciones de los Estados miembros únicamente, o la ausencia de actuación comunitaria entrarían en conflicto con los requisitos del Tratado (tales como la necesidad de corregir distorsiones de la competencia o evitar restricciones encubiertas del comercio o reforzar la cohesión económica y social)» y que «la actuación comunitaria proporcionaría claros beneficios debido a su escala o a sus efectos en comparación con la actuación a nivel de los Estados miembros». Es importante advertir que basta con que *uno* de estos requisitos esté ausente para que la actuación comunitaria pierda su justificación. En el presente caso, basta acudir a las leyes sobre protección de datos aprobadas en varios Estados miembros *antes* de la primera directiva comunitaria (por ejemplo, la LORTAD española de 1992) para darse cuenta de que falta el primer requisito pues estas legislaciones atendían satisfactoriamente los aspectos transnacionales de la protección de datos. Pero además dista de estar cuantitativa o cualitativamente probado el segundo requisito. En definitiva, no creemos que el principio de subsidiariedad pueda justificar esta regulación comunitaria.

Por su parte, la jurisprudencia del tribunal en el caso de la directiva sobre publicidad del tabaco²² ha dejado sentado que:

²¹ Dictamen del Tribunal de Justicia de 28 de marzo de 1996 (2/1994), sobre Adhesión de la Comunidad al Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales [1996] Rec. I-1759.

²² Sentencia del Tribunal de Justicia, de 5 de octubre de 2000 (C-376-98), República Federal de Alemania v. Parlamento y Consejo de la Unión Europea [2000] Rec. I-2247.

«las medidas contempladas en el artículo 100 A, apartado 1, del Tratado están destinadas a mejorar las condiciones de establecimiento y funcionamiento del mercado interior. Interpretar este artículo en el sentido de que atribuye al legislador comunitario una competencia general para regular el mercado interior sería no sólo contrario al propio tenor literal de las disposiciones antes citadas, sino también incompatible con el principio establecido en el artículo 3 B del Tratado CE (actualmente artículo 5 CE), según el cual las competencias de la Comunidad son competencias de atribución».

El tribunal añade que,

«un acto adoptado sobre la base del artículo 100 A del Tratado debe tener efectivamente por objeto la mejora de las condiciones de establecimiento y funcionamiento del mercado interior. Si la mera comprobación de disparidades entre las regulaciones nacionales y de un riesgo abstracto de aparición de obstáculos a las libertades fundamentales o de distorsiones de la competencia que puedan resultar de tales disparidades bastase para justificar la elección del artículo 100 A como base jurídica, el control jurisdiccional del respeto de la base jurídica podría quedar privado de toda eficacia. Se impediría entonces al Tribunal de Justicia ejercer la función, que le incumbe en virtud del artículo 164 del Tratado CE (actualmente artículo 220 CE), de garantizar el respeto del Derecho en la interpretación y aplicación del Tratado.»

Resulta más que discutible afirmar que estas directivas sobre protección de datos «contribuyen efectivamente a eliminar obstáculos a la libre circulación de mercancías y a la libre prestación de servicios, así como a suprimir distorsiones de la competencia». La razón fundamental es que el derecho de la protección a los datos personales ya existe en el marco del Consejo de Europa (el art. 8 CEDH interpretado por el TEDH más el C1981) y presenta un nivel suficiente de homogeneidad como para considerar poco convincente la tesis de que sea necesario intervenir en este campo para «mejorar las condiciones de establecimiento y funcionamiento del mercado interior». La propia legislación comunitaria no sólo es consciente de este hecho, sino que incluso pretende «precisar y ampliar» la protección que el C1981 del Consejo de Europa proporciona (párrafo

11 del Preámbulo de Dir95). Pero, es que hay más. Las normas dictadas por la Unión Europea en el marco del «tercer pilar» (de las que se hablará más adelante) estableciendo sistemas de bases de datos ¡establecen como marco de protección el C1981 del Consejo de Europa en lugar de la Dir95 comunitaria! ¿Cabe mayor demostración de que los argumentos para dictar la Dir95 carecen de base?

b) El derecho a la protección de los datos personales aparece por primera vez en la legislación comunitaria en un instrumento de Derecho derivado, la *Directiva 95/46/CE* (Dir95). Esta directiva, como se ha dicho, pretende «precisar y ampliar» la protección que brinda el C1981. Lo mismo que el C1981, la Dir95 considera al derecho a la protección de datos personales en relación con el derecho al respeto de la vida privada. Así se desprende del art. 1.1 de la misma: «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».

La normativa de la Dir95, que se dictó para «precisar y ampliar» las garantías que ya había previsto el C1981 del Consejo de Europa, tiene una posición especialmente relevante en el Derecho comunitario de la protección de datos personales, ya que ha sido considerada como una especie de «directiva marco» cuyos principios probablemente requerirán una futura elaboración para satisfacer las necesidades de algunos sectores económicos particulares²³. Esto es lo que ha sucedido en materia de telecomunicaciones, donde los principios de la Dir95 han sido objeto de un ulterior desarrollo a través de la *Directiva 97/66/CE* (Dir97), en la que se pretendió adaptar su contenido a un sector concreto y con especificidades propias, el de las telecomunicaciones, como así se declara expresamente²⁴. Igual que la Dir95, la Dir97 reitera, en los mismos términos que la anterior, la conexión del derecho a la protección de datos con el derecho a la intimidad (art. 1.1 Dir97).

Esta Dir97 ha sido recientemente sustituida por otra nueva, la *Directi-*

²³ Fergus GLAVEY, «Accountability, the Right to Privacy and Third Pillar Arrangements», en Eugene REGAN (ed.), *The new Third Pillar. Cooperation against crime in the European Union*, Institute of European Affairs, Dublín, 2000, p. 134 ss. (p. 141).

²⁴ Art. 1.2 Dir97: «las disposiciones de la presente Directiva especificarán y completarán la Directiva 95/46/CE».

va 2002/58/CE (Dir2002), que continúa apoyándose en la conexión entre derecho a la protección de datos personales y derecho a la intimidad (art. 1.1 Dir2002). Esta nueva directiva ha sido muy criticada porque introduce un nuevo artículo (que no figuraba en 1997) que amplía, no el derecho del individuo a la protección de sus datos personales, sino la obligación de los proveedores de servicio de conservar (a su costa) los datos personales para facilitar a las autoridades públicas su eventual control (vid. *infra*).

C) *El tratado CE y la legislación de desarrollo*

La reforma del Tratado CE operada en Amsterdam supuso la introducción de un nuevo precepto, el art. 286 (antiguo 213b), para responder a la paradoja de que el ordenamiento comunitario hasta entonces vigente (las Directivas que hemos calificado como «Derecho comunitario derivado ‘autónomo’») reconociera el derecho a la protección de datos frente a los Estados, pero no frente a la Comunidad. Es importante advertir que el derecho a la protección de datos personales opera como un límite a otro derecho introducido en el TCE en Amsterdam: el derecho de acceso a los documentos del Parlamento, del Consejo y de la Comisión (art. 255, antiguo 191A)²⁵.

El desarrollo del art. 286 TCE planteó serias dudas doctrinales. Se sostuvo, con buenos argumentos, que este precepto significaba que las directivas 95/46 y 97/66 resultaban aplicables (en el sentido de «obligatorias en todos sus términos») a los organismos comunitarios sin necesidad de que se adoptara ninguna medida de transposición a partir de 1999. Sin embargo, esta interpretación no fue pacífica²⁶. Finalmente, la situación jurídica se ha normalizado en el año 2001 con la aprobación de un

²⁵ Art. 4 del Reglamento (CE) n.º 1049/2001 del Parlamento Europeo y del Consejo de 30 de mayo de 2001 relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión (DO L 145 de 31.5.2001, p. 43). Sobre esta cuestión, cfr. Elena F. PÉREZ CARRILLO, «La transparencia en el funcionamiento de la Unión Europea: el acceso público a los documentos de sus instituciones y órganos», *Revista Vasca de Administración Pública* n.º 56 (2000), pp. 349 ss.

²⁶ Francesco MAIANI, «Le cadre réglementaire des traitements de données personnelles effectués au sein de l'Union européenne», *Revue Trimestrielle de Droit Européenne* n.º 2-2002, pp. 283 ss. (pp. 292-293).

Reglamento que no sólo asume todo el acervo comunitario en materia de protección de datos (en ese momento, de forma destacada, las Dir95 y Dir97), y en particular la conexión con el derecho a la intimidad (art. 1.1 Dir2002), sino que introduce algunos elementos nuevos, ciertamente interesantes, como el establecimiento de una autoridad independiente europea de control, el «Supervisor europeo de protección de datos» (arts. 41 ss. R2001) y la posibilidad de un «amparo», inicialmente ante el «Supervisor» y, después, en vía de recurso, ante el TJ (art. 32 R2001).

D) *El Tratado de la Unión Europea y el tercer pilar*

El art. 286 TCE y el R2001 sólo afectan a los tratamientos de datos personales realizados por las instituciones y órganos comunitarios en el ejercicio de actividades que entren dentro del ámbito de aplicación del «Derecho comunitario». Ahora bien, estas normas no cubren las actuaciones de esos mismos órganos en el marco de los pilares segundo (PESC) y tercero (política de interior y justicia). La cuestión del derecho a la protección de datos personales resulta especialmente relevante en este tercer pilar, pues alberga tres sistemas de información sumamente potentes que operan con datos personales: el Sistema de Información Schengen (SIS), el Sistema de Información Europol (SIE) y el Sistema de Información Aduanero (SIA).

a) En virtud de lo dispuesto en la primera frase del segundo párrafo del apartado 1 del artículo 2 del Protocolo anejo al Tratado de la Unión Europea y al Tratado constitutivo de la Comunidad Europea, se integra el *acervo de Schengen* en el marco de la Unión Europea (con el nombre de ‘Protocolo sobre Schengen’). La definición de en qué consistía el acervo de Schengen se llevó a cabo en una decisión del Consejo²⁷, aunque la publicación en el DOCE de ese acervo es posterior²⁸. En virtud de la misma, el acervo de Schengen, en el que se encuentra el SIS, inicialmen-

²⁷ Decisión del Consejo del 20 de mayo de 1999 sobre la definición del acervo de Schengen a efectos de determinar, de conformidad con las disposiciones pertinentes del Tratado constitutivo de la Comunidad Europea y del Tratado de la Unión Europea, la base jurídica de cada una de las disposiciones o decisiones que constituyen dicho acervo (1999/435/CE).

²⁸ Las normas del sistema Schengen, incorporadas al tercer pilar, fueron publicadas en el DOCE L 239, de 22 de septiembre de 2000.

te surgió al margen de la Comunidad Europea. Se compone, fundamentalmente, de una serie de instrumentos «originarios»²⁹ y de otros textos jurídicos «derivados»³⁰. Una parte importantísima, esencial, del acervo de Schengen es el SIS. El Acuerdo de Schengen de 1985 contiene numerosas referencias al C1981 del Consejo de Europa que queda configurado así como el canon de protección de datos personales³¹.

b) Por su parte, el SIE, o Sistema de Información de *Europol* es la razón de ser del Convenio *Europol*³². Así se pone de manifiesto en el análisis de las funciones que el Convenio asigna a *Europol* (art. 3.1). En la realización de estas funciones, el tratamiento de datos personales es, por tanto, una necesidad ineludible. Igual que sucedía en el Sistema de

²⁹ El Acuerdo, firmado en Schengen el 14 de junio de 1985, entre los Gobiernos de los Estados de la Unión Económica Benelux, la República Federal de Alemania y la República Francesa, relativo a la supresión gradual de los controles en las fronteras comunes; el Convenio, firmado en Schengen el 19 de junio de 1990 entre el Reino de Bélgica, la República Federal de Alemania, la República Francesa, el Gran Ducado de Luxemburgo y el Reino de los Países Bajos, para la aplicación del Acuerdo, firmado en Schengen el 14 de junio de 1985, relativo a la supresión gradual de los controles en las fronteras comunes junto con su Acta Final y declaraciones; los acuerdos y protocolos sobre la adhesión al Acuerdo de Schengen de 1985 y al Convenio de Schengen de 1990 de la República Italiana (firmados en París el 27 de noviembre de 1990), del Reino de España y la República Portuguesa (firmados en Bonn el 25 de junio de 1991), de la República Helénica (firmados en Madrid el 6 de noviembre de 1992), de la República de Austria (firmados en Bruselas el 28 de abril de 1995) y del Reino de Dinamarca, la República de Finlandia y el Reino de Suecia (firmados en Luxemburgo el 19 de diciembre de 1996), junto con sus actas finales y declaraciones.

³⁰ Decisiones y declaraciones del Comité Ejecutivo de Schengen y Decisiones del Grupo central para cuya adopción éste haya sido facultado por el Comité Ejecutivo.

³¹ Art. 126.1 del Convenio del Acuerdo de 1985 dice que: «Por lo que se refiere al tratamiento automatizado de datos de carácter personal transmitidos en aplicación del presente Convenio, cada Parte contratante adoptará, a más tardar en el momento de la entrada en vigor del presente Convenio, las disposiciones nacionales que sean necesarias para conseguir un nivel de protección de los datos de carácter personal que sea al menos igual al que se desprende de los principios del Convenio del Consejo de Europa de 28 de enero de 1981 para la protección de las personas en lo referente al tratamiento automatizado de datos de carácter personal».

³² Acto del Consejo, de 26 de julio de 1995, relativo al establecimiento del Convenio, basado en el artículo K.3 del Tratado de la Unión Europea, por el que se crea una Oficina Europea de Policía (Convenio *Europol*) [DOCE C 316, de 27 de noviembre de 1995]. El Convenio *Europol* aparece como anexo al Acto del Consejo.

Schengen, en el Sistema Europol se contempla también la necesidad de que esta actividad tenga que ser compatible con el derecho a la protección de datos personales, e igual que en Schengen el canon elegido es el Convenio de 1981, al que se añade una Recomendación del Consejo de Europa sobre utilización de datos personales en el sector de la policía³³.

c) Finalmente, en el Sistema de Información *Aduanero* (SIA) encontramos también disposiciones similares. Este sistema es un importante elemento del Convenio relativo a la utilización de la tecnología de la información a efectos aduaneros³⁴. Igual que sucedía en el SIS y el SIE, aquí también el C1981 y la Recomendación 87 del Consejo de Europa se erigen en el criterio de protección de datos personales³⁵.

Hay una circunstancia que debe ser expresamente señalada. A diferencia de lo que ocurría con el Convenio Schengen (de 1985), los Convenios Europol y de Información Aduanera son de 1995, es decir, se elaboran cuando la Comunidad Europea está elaborando su Directiva 95/46 e incluso se publican en el DOCE *después* de la Dir95. Esta circunstancia suscita varias preguntas inevitables: ¿por qué el SIE y el SIA eligen como criterio de protección de datos personales el C1981 del Consejo de Europa y no la Dir95 de la Comunidad Europea?, si el C1981 constituye un criterio suficiente para proteger los datos personales ¿por qué la Comunidad decide aprobar la Dir95 con lo que ello supone, a nuestro juicio, de invasión de competencias del Estado? Y si el C1981 no constituye protección suficiente para los datos personales, ¿no resulta incongruente, cuando no hipócrita, que la Unión Europea rechaze el criterio de protección de datos personales en el «tercer pilar» que ella misma establece para el «primer pilar»?

³³ Art. 14.3 del Convenio Europol: «En la recogida, el tratamiento y la utilización de datos personales, Europol respetará los principios del Convenio del Consejo de Europa de 28 de enero de 1981 y la Recomendación R(87)15, de 17 de septiembre de 1987, del Comité de ministros del Consejo de Europa».

³⁴ Acto de Consejo de 26 de julio de 1995 por el que se establece el Convenio relativo a la utilización de la tecnología de la información a efectos aduaneros (95/C 316/02) [DOCE C 316, de 27 de noviembre de 1995]. El Convenio de Información Aduanera aparece como anexo al Acto del Consejo.

³⁵ Art. 18.2 el Convenio relativo a la utilización de la tecnología de la información a efectos aduaneros: «La Autoridad de Supervisión Común desempeñará sus funciones de acuerdo con las disposiciones del presente Convenio y del Convenio de Estrasburgo de 1981 y tomando en consideración la Recomendación R (87) 15, de 17 de septiembre de 1987, del Comité de Ministros del Consejo de Europa».

4. OTROS INSTRUMENTOS INTERNACIONALES

A) Dejando al margen otros instrumentos internacionales (como el Pacto Internacional de los Derechos Civiles y Políticos de 1966) que reconocen el derecho a la intimidad, pero no incluyen una cláusula específica sobre el derecho a la protección de datos personales, existe una organización internacional en la que se han elaborado importantes instrumentos relacionados con la intimidad y la protección de datos personales. Esa organización es la Organización para la Cooperación y el Desarrollo en Europa (OCDE). En el marco de la OCDE se han aprobado tres importantes instrumentos sobre este asunto.

En primer lugar, el 23 de septiembre de 1980, antes de que el Consejo de Europa aprobara el Convenio 108, la OCDE aprobó una recomendación en la que instaba a los Estados miembros a tener en cuenta en su legislación interna las «Directrices sobre la protección de la intimidad y los flujos transfronterizos de datos de carácter personal» que aparecen como anexo de la misma. No obstante, debe tenerse en cuenta que estas «directrices» de la OCDE sólo representan un consenso mínimo (n.º 6 de las «Directrices») ya que, en efecto, el propósito fundamental de las mismas es evitar que la alegación del derecho a la intimidad suponga obstáculos excesivos al flujo internacional de datos personales (n.º 2 de la recomendación) que la OCDE parece considerar como algo positivo para el desarrollo económico.

En segundo lugar, los Gobiernos de la OCDE aprobaron el 11 de abril de 1985 una «Declaración sobre flujos transfronterizos de datos» que confirma la reticencia de este organismo frente al derecho a la protección de datos ya que en este documento los gobiernos de la organización manifiestan su intención de «promover los servicios de datos e información y de evitar la creación de barreras injustificadas al intercambio internacional de datos e informaciones».

Finalmente, en tercer lugar, la Conferencia de ministros de la OCDE reunida en Ottawa del 7 al 9 de octubre de 1998, aprobó una «Declaración sobre la protección de la intimidad en las redes globales» en la que la OCDE parece modificar sus anteriores planteamientos al otorgar al respeto a la intimidad un peso mayor que en sus anteriores documentos. En esta declaración de 1998, los gobiernos de la OCDE reafirman su compromiso de proteger la intimidad en las redes globales para conseguir mayor

confianza en las mismas y prevenir innecesarias restricciones al tráfico transnacional de datos personales. Además, «animan a los gobiernos» a adoptar «políticas protectoras de la intimidad, ya se ejecuten legalmente o mediante técnicas de autoregulación», a «asegurarse de que se dispone de mecanismos efectivos para hacer frente a las conductas incumplidoras de las políticas de intimidad», a promover «la notificación on-line de las políticas de intimidad a los usuarios», y a «incorporar tecnologías protectoras de la intimidad». Es más, en este documento los propios Estados miembros de la OCDE «invitan» a los demás Estados de la comunidad internacional así como a las organizaciones internacionales y a las grandes empresas a tomar en cuenta lo dispuesto en esta Declaración.

B) El derecho a la intimidad y la protección de datos personales ha sido contemplado por la OMC con similares prevenciones a las que hemos visto en la OCDE. En el «Acuerdo General sobre el Comercio de Servicios» aprobado en la «Ronda Uruguay» del GATT, y que aparece como Anexo I B del Acuerdo de Marrakech, de 15 de abril de 1994, estableciendo la Organización Mundial del Comercio, se contiene implícita la idea de que la protección de la intimidad y de los datos personales es sospechosa de ser un mecanismo de restricción encubierta del libre comercio³⁶.

5. LAS CONSTITUCIONES DE LOS ESTADOS MIEMBROS, EN ESPECIAL, LA ESPAÑOLA

Un repaso a los textos constitucionales de los Estados miembros de la UE nos revela que no todas sus Constituciones recogen el derecho a la protección de datos personales, por lo que este derecho no puede extraer-

³⁶ Art. 14.c.ii del Acuerdo General sobre el Comercio de Servicios: «A reserva de que las medidas enumeradas a continuación no se apliquen en forma que constituya un medio de discriminación arbitrario o injustificable entre países en que prevalezcan condiciones similares, o una restricción encubierta del comercio de servicios, ninguna disposición del presente Acuerdo se interpretará en el sentido de impedir que un Miembro adopte o aplique medidas: (...) c) necesarias para lograr la observancia de las leyes y los reglamentos que no sean incompatibles con las disposiciones del presente Acuerdo, con inclusión de los relativos a: (...) ii) la protección de la intimidad de los particulares en relación con el tratamiento y la difusión de datos personales y la protección del carácter confidencial de los registros y cuentas individuales».

se de las «tradiciones constitucionales comunes» europeas. Si esto es así, la inclusión de este derecho en la Carta contravendría el mandato de Colonia. En cualquier caso, es importante referirse a aquellas Constituciones que sí recogen este derecho ya que la CDF (y, por tanto también su art. 8) no puede interpretarse en un sentido «limitativo o lesivo de los derechos humanos reconocidos ... por las Constituciones de los Estados miembros» (art. 53 CDF).

Los países miembros de la UE se pueden agrupar en dos grandes sectores: por un lado, aquellos que expresamente reconocen el derecho a la protección de datos en sus textos constitucionales como un derecho independiente; por otro, los que lo recogen como una consecuencia o derivación del derecho a la intimidad; y, finalmente, los que no contienen alusiones al mismo.

A) El reconocimiento del derecho a la protección de datos como un derecho autónomo aparece en la Constitución de *Portugal* de 1976, que en su art. 35 contempla, entre otros aspectos, el derecho de «todo ciudadano» a «tener conocimiento de lo que conste en forma de registros informáticos acerca de él y de la finalidad a que se destinan esos datos, y podrá exigir su rectificación, así como su actualización». Es preciso advertir, no obstante, que si bien la Constitución portuguesa establece este derecho en un artículo propio, por un lado, lo hace en el inmediatamente correlativo al destinado a proteger sendas manifestaciones de la vida privada como la inviolabilidad de domicilio y el secreto de las comunicaciones y, por otro, que no hay ningún precepto que consagre el derecho a la intimidad como tal. En esta situación también se halla *Suecia*, donde tampoco encontramos ningún precepto dedicado al derecho a la intimidad en sentido estricto. La Constitución sueca dispone que «todo ciudadano quedará protegido, en la medida que se disponga en detalle por la ley, contra la violación de su integridad personal resultante del registro de información sobre él mediante tratamiento electrónico de datos».

B) Otras Constituciones de los Estados miembros de la UE, sin embargo, se hacen eco del derecho a la protección de datos personales como un derecho que no es sino la consecuencia o derivación del derecho a la intimidad. Es el caso de la Constitución de *Finlandia* que en su actual art. 10.1 (tras la reforma de 2000) establece que «se garantiza a todos la intimidad, honor y la inviolabilidad del domicilio. La ley establecerá normas de detalle sobre la salvaguardia de los datos de carácter personal». La misma situación se da en *Holanda*, donde su Constitución establece en su

art. 10.2 que «la ley establecerá las normas de protección de la intimidad personal en relación con la indagación y difusión de datos personales» y que «la ley dictará normas sobre el derecho de toda persona a que se le dé conocimiento de los datos recogidos sobre ella y del uso que se hiciera de los mismos» (art. 10.3).

C) En otros casos, como en *Alemania*, la Constitución no recoge un derecho a la protección de datos, como tampoco un derecho a la intimidad. El Tribunal Constitucional alemán, en un momento dado, se vio enfrentado a la cuestión cuando tuvo que resolver un recurso de inconstitucionalidad contra la ley del censo, que admitía la posibilidad de recoger y tratar electrónicamente datos personales sin consentimiento de los afectados. Al tratar de dar una solución al caso, el Tribunal Constitucional Federal Alemán no podía razonar la eventual inconstitucionalidad de esa ley por contradicción con el derecho a la intimidad, ya que éste no está consagrado en la Ley Fundamental de Bonn. La consecuencia es que tuvo que crear un nuevo derecho, que dio en llamar el «derecho a la autodeterminación informativa»³⁷.

D) En *España* el artículo 18.4 CE se limita a declarar que «la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos».

a) El derecho a la intimidad (art. 18.1 CE) en su relación con el uso de la informática (art. 18.4 CE) fue desarrollado en España inicialmente por la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD). Esta ley consideraba que «en desarrollo de lo previsto en el apartado 4 del artículo 18 de la Constitución» debía tener por objeto «limitar el uso de la informática y otras técnicas y medios de tratamiento automatizado de los datos de carácter personal para garantizar el honor, la intimidad personal y familiar de las personas físicas y el pleno ejercicio de sus derechos» (art. 1 LORTAD). Después de la aprobación de la LORTAD, en el ámbito de la UE se dictó la Dir95 que obligó a España a dictar una nueva legislación. Así surgió la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPD) que se propone «garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente su honor e intimidad personal y familiar» (art. 1 LOPD). Esta

³⁷ Sentencia del Tribunal Constitucional Federal Alemán, de 15 de diciembre de 1983 (BverfGE 65, 1).

ley reproduce en una gran medida las provisiones de la Dir95, aunque como bien advierte Glavey, esto no tiene necesariamente que ser así. Según Glavey, la Dir95 sólo obliga al Estado a trasponer sus normas para las relaciones jurídicas que estén cubiertas por el «Derecho comunitario» (primer pilar)³⁸. Esto significa que el Estado tiene libertad para establecer una doble legislación en materia de datos personales: una sobre las situaciones afectadas por el Derecho comunitario y otra para las que se hallan fuera del mismo (seguridad y justicia, por ejemplo) que no tienen por qué regirse por los preceptos de la Dir95. Sin embargo, en España la normativa de la Dir95, traspuesta en la LOPD, se aplica a todas las situaciones jurídicas sin distinguir las que caen bajo el ámbito «comunitario» de las demás.

III. EL CONTENIDO DEL DERECHO

1. Se ha discutido ampliamente por la doctrina acerca de cuál es el contenido del derecho a la intimidad o a la protección de la vida privada. No es este el momento de reproducir esa discusión³⁹; valga decir a estos efectos que a nuestro modesto entender las diversas manifestaciones jurídicas protectoras del ámbito privado o íntimo de la persona (intimidad en sentido estricto, vida privada, secreto de las comunicaciones, inviolabilidad del domicilio, secreto profesional, intimidad genética) son reconducibles a un contenido último, a saber, la autodeterminación informativa o poder del sujeto de determinar qué información sobre su persona y sus circunstancias puede ser comunicada a terceros, bien porque en ese momento aún no es pública o bien porque no deba serlo. Este control del sujeto, esta autodeterminación informativa en que consiste *toda* intimidad se traduce en un conjunto de derechos (con sus correlativas obligaciones) que, no sólo tienen una naturaleza de «derechos subjetivos», sino que también tienen una vertiente objetiva, de tipo orgánico-procedimental y aun una tercera dimensión valorativa, a la que a veces incluso se añade una dimensión cultural-nacional⁴⁰. Estas ideas aplicadas al uso de ficheros se

³⁸ GLAVEY, «Accountability, ...», cit., p. 140.

³⁹ Carlos RUIZ MIGUEL, *La configuración constitucional del derecho a la intimidad*, Tecnos, Madrid, 1995, pp. 76 ss.

⁴⁰ Sobre esta cuestión me remito a mi trabajo «La naturaleza jurídica multidimensional de los derechos fundamentales», en Miguel Ángel APARICIO (coord.), *Derechos Constitucionales y Formas Políticas*, Cedecs/Diputación de Tarragona, Barcelona, 2001, pp. 165-179.

traducen en el llamado derecho a la protección de datos personales. Esos derechos y deberes se sintetizan en cinco principios: consentimiento, información, control, calidad y lealtad, y seguridad y confidencialidad.

2. Como acabamos de decir, el contenido del derecho a la protección de datos aparece vertebrado en torno a una serie de principios de los que se desglosan a su vez una serie de derechos y obligaciones. El C1981 establece algunos de estos principios que, posteriormente, se considerarán como un acervo irrenunciable para cualquier regulación de este derecho, sin perjuicio de que otros ordenamientos añadan nuevas exigencias. Así, en primer lugar, se consagra el principio de *consentimiento*, del que emana el reconocimiento del derecho a cancelar aquellas informaciones que el sujeto no desee que sigan figurando en un fichero⁴¹; en segundo lugar, el principio de *información*, del que se desprende el derecho a conocer qué datos del sujeto obran en el fichero⁴²; en tercer lugar, el principio de *control*, del que se desglosan los derechos a la rectificación de los que considere erróneos y al borrado (cancelación) de los poseídos irregularmente y a disponer de un recurso para hacer efectivas sus pretensiones⁴³; en cuarto lugar, el principio de calidad y lealtad (correlativos de los derechos antecitados), según el cual los datos serán exactos y actualizados, se obtendrán y tratarán lealmente y de forma proporcionada a la finalidad para la que se recogieron⁴⁴.

⁴¹ Art. 8.c C1981: «Cualquier persona deberá poder: (...) c) obtener, llegado el caso, el borrado de los (datos), cuando se hayan tratado con infracción de las disposiciones del derecho interno que hagan efectivos los principios básicos enunciados en los artículos 5 y 6 del presente Convenio».

⁴² Art. 8.a C1981: «Cualquier persona deberá poder: a) Conocer la existencia de un fichero automatizado de datos de carácter personal, sus finalidades principales, así como la identidad y la residencia habitual o el establecimiento principal de la autoridad controladora del fichero».

⁴³ Art. 8.c y d C1981: «Cualquier persona deberá poder: c) obtener, llegado el caso, la rectificación de dichos datos (...) cuando se hayan tratado con infracción de las disposiciones del derecho interno que hagan efectivos los principios básicos enunciados en los artículos 5 y 6 del presente Convenio; d) disponer de un recurso si no se ha atendido a una petición de confirmación o, si así fuere el caso, de comunicación, de ratificación o de borrado, a que se refieren los párrafos b) y c) del presente artículo».

⁴⁴ Art. 5 C1981: «Los datos de carácter personal que sean objeto de un tratamiento automatizado: a) Se obtendrán y tratarán leal y legítimamente; b) se registrarán para finalidades determinadas y legítimas, y no se utilizarán de una forma incompatible con dichas finalidades; c) serán adecuados, pertinentes y no excesivos

Finalmente, se establece el principio de seguridad y confidencialidad en el tratamiento de los datos⁴⁵.

3. En el marco del Derecho Comunitario el contenido del derecho, si bien está inspirado en el C1981, generalmente queda detallado y ahondado. En efecto, en las directivas comunitarias los principios básicos o ejes del C1981 son «precisados» y «ampliados», por más que en algún supuesto (como la nueva directiva de 2002) se haya introducido algún precepto (inexistente en la directiva anterior de 1997) que amplía, no el derecho del individuo a la protección de sus datos personales, sino la obligación de los proveedores de servicio de conservar (a su costa) los datos personales para facilitar a las autoridades públicas su eventual control⁴⁶.

En primer lugar, el principio de *consentimiento*, que no sólo opera en el momento «final» (como derecho a cancelar datos que el sujeto no quiera que figuren tal y como sucedía en el C1981), sino también en el momento «inicial» imponiendo el principio general de que el tratamiento de los datos sólo pueda emprenderse si el afectado otorga su consenti-

en relación con las finalidades para las cuales se hayan registrado; d) serán exactos y si fuera necesario puestos al día; e) se conservarán bajo una forma que permita la identificación de las personas concernidas durante un período de tiempo que no exceda del necesario para las finalidades para las cuales se hayan registrado».

⁴⁵ Art. 7 C1981: «Se tomarán medidas de seguridad apropiadas para la protección de datos de carácter personal registrados en ficheros automatizados contra la destrucción accidental o no autorizada, o la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizados».

⁴⁶ El polémico art. 15 Dir2002 dispone que: «Los Estados miembros podrán adoptar medidas legales para limitar el alcance de los derechos y las obligaciones que se establecen en los artículos 5 y 6, en los apartados 1 a 4 del artículo 8 y en el artículo 9 de la presente Directiva, cuando tal limitación constituya una medida necesaria proporcionada y apropiada en una sociedad democrática para proteger la seguridad nacional (es decir, la seguridad del Estado), la defensa, la seguridad pública, o la prevención, investigación, descubrimiento y persecución de delitos o la utilización no autorizada del sistema de comunicaciones electrónicas a que se hace referencia en el apartado 1 del artículo 13 de la Directiva 95/46/CE. Para ello, *los Estados miembros podrán adoptar, entre otras, medidas legislativas en virtud de las cuales los datos se conserven durante un plazo limitado justificado por los motivos establecidos en el presente apartado*. Todas las medidas contempladas en el presente apartado deberán ser conformes con los principios generales del Derecho comunitario, incluidos los mencionados en los apartados 1 y 2 del artículo 6 del Tratado de la Unión Europea» (cursiva mía).

miento⁴⁷. Esta exigencia de consentimiento «inicial» aparece desarrollada en la normativa sectorial sobre telecomunicaciones que la prescribe para cuatro aspectos: los datos de tráfico («cuando se ofrezca la posibilidad de visualizar la identificación de la línea de origen, el proveedor del servicio deberá ofrecer al usuario que efectúe la llamada la posibilidad de impedir en cada llamada, mediante un procedimiento sencillo y gratuito, la presentación de la identificación de la línea de origen»), los datos de localización distintos de tráfico, los contenidos en la facturación desglosada y los que se hallan en las guías de abonados⁴⁸. Sin embargo, este principio general no es llevado a sus últimas consecuencias por la normativa comunitaria sectorial de comercio electrónico⁴⁹. En esta última, a pesar de la declaración general de la Dir95, se admite la posibilidad de que en su momento «inicial», se puedan tratar datos sin consentimiento del afectado. La consecuencia de esto es que el Derecho comunitario sobre comercio electrónico no prohíbe el «spam» o correo basura en las comunicaciones electrónicas⁵⁰.

⁴⁷ Art. 7.a Dir95: «Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si: a) el interesado ha dado su consentimiento de forma inequívoca»; art. 8 Dir95: «1. Los Estados miembros prohibirán el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad. 2. Lo dispuesto en el apartado 1 no se aplicará cuando: a) el interesado haya dado su consentimiento explícito a dicho tratamiento, salvo en los casos en los que la legislación del Estado miembro disponga que la prohibición establecida en el apartado 1 no pueda levantarse con el consentimiento del interesado».

⁴⁸ Arts. 7 Dir2002 («Facturación desglosada»), 8 Dir2002 («Presentación y restricción de la identificación de la línea de origen y de la línea conectada»), 9 Dir2002 («Datos de localización distintos de los datos de tráfico»), 12 Dir2002 («Guías de abonados»).

⁴⁹ Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico) (DOCE L 178 de 17 de julio de 2000, p1ss.) [Dir2000].

⁵⁰ Art. 7 Dir2000: «Comunicación comercial no solicitada. 1. Además de otros requisitos establecidos en el Derecho comunitario, los Estados miembros que permitan la comunicación comercial no solicitada por correo electrónico garantizarán que dicha comunicación comercial facilitada por un prestador de servicios establecido en su territorio sea identificable de manera clara e inequívoca como tal en el mismo momento de su recepción. 2. Sin perjuicio de lo dispuesto en las Directivas

En segundo lugar, también el principio de *información* resulta ampliado ya que no sólo se prescribe el derecho del sujeto a «demandar» información sobre sus datos, sino también a «recibir» esa información al establecer la obligación que tiene el responsable del tratamiento de informar al afectado, en el caso de la que la persona afectada no hubiera sido ya previamente informada, sobre los datos que posea acerca de su persona⁵¹.

En tercer lugar, el principio de *control*, también aparece mejorado ya que, si bien no se introducen novedades significativas respecto a la posibilidad de rectificación que ya contemplaba el C1981⁵², sí que se facilita mucho más la posibilidad de tener un recurso para hacer efectiva la pretensión, configurando el «derecho de oposición» incluso como un derecho gratuito⁵³. No sólo eso, sino que se añade una nueva modalidad de

97/7/CE y 97/66/CE, los Estados miembros deberán adoptar medidas para garantizar que los prestadores de servicios que realicen comunicaciones comerciales no solicitadas por correo electrónico consulten regularmente las listas de exclusión voluntaria («opt-out») en las que se podrán inscribir las personas físicas que no deseen recibir dichas comunicaciones comerciales, y las respeten». El art. 13.3 Dir2002 sigue dejando abierta la posibilidad al «correo basura»: «Los Estados miembros tomarán las medidas adecuadas para garantizar, que, sin cargo alguno, no se permitan las comunicaciones no solicitadas con fines de venta directa (...), bien sin el consentimiento del abonado, bien respecto de los abonados que no deseen recibir dichas comunicaciones. La elección entre estas dos posibilidades será determinada por la legislación nacional».

⁵¹ Art. 10 Dir95: «Los Estados miembros dispondrán que el responsable del tratamiento o su representante deberán comunicar a la persona de quien se recaben los datos que le conciernan, por lo menos la información que se enumera a continuación, salvo si la persona ya hubiera sido informada de ello: a) la identidad del responsable del tratamiento y, en su caso, de su representante; b) los fines del tratamiento de que van a ser objeto los datos; c) cualquier otra información tal como: — los destinatarios o las categorías de destinatarios de los datos, — el carácter obligatorio o no de la respuesta y las consecuencias que tendría para la persona interesada una negativa a responder, — la existencia de derechos de acceso y rectificación de los datos que la conciernen, en la medida en que, habida cuenta de las circunstancias específicas en que se obtengan los datos, dicha información suplementaria resulte necesaria para garantizar un tratamiento de datos leal respecto del interesado».

⁵² Sobre el derecho de rectificación: art. 12.b Dir95.

⁵³ Art. 14 Dir95: «Los Estados miembros reconocerán al interesado el derecho a: a) oponerse, al menos en los casos contemplados en las letras e) y f) del artículo 7, en cualquier momento y por razones legítimas propias de su situación particular, a que los datos que le conciernan sean objeto de tratamiento, salvo cuando la legislación nacional disponga otra cosa. En caso de oposición justificada, el tratamiento que

control no prevista en el C1981 (y que, de hecho, se pretende incorporar al C1981 con la incorporación de un protocolo adicional), a saber, un organismo independiente con poderes inspectores y sancionadores⁵⁴.

En cuarto lugar, el principio de calidad y lealtad (correlativos de los derechos antecitados), según el cual los datos serán exactos y actualizados, se obtendrán y tratarán lealmente y de forma proporcionada a la finalidad para la que se recogieron, se encuentra mucho más detallado⁵⁵.

Finalmente, en quinto lugar, el principio de seguridad y confidencialidad en el tratamiento de los datos se halla muchísimo más detallado en la directiva que establece el marco «general» de la protección de datos que en el Convenio de 1981⁵⁶. La normativa sectorial sobre telecomunicaciones ahonda en las exigencias de seguridad y confidencialidad en el tratamiento de los datos⁵⁷.

La jurisprudencia comunitaria, aunque hasta ahora no contiene pronunciamientos acerca del contenido de este derecho, en un futuro próximo sí

efectúe el responsable no podrá referirse ya a esos datos; b) oponerse, previa petición y sin gastos, al tratamiento de los datos de carácter personal que le conciernan respecto de los cuales el responsable prevea un tratamiento destinado a la prospección; o ser informado antes de que los datos se comuniquen por primera vez a terceros o se usen en nombre de éstos a efectos de prospección, y a que se le ofrezca expresamente el derecho de oponerse, sin gastos, a dicha comunicación o utilización».

⁵⁴ Art. 28 Dir95 («Autoridad de control»).

⁵⁵ Art. 6.1 Dir95: «Los Estados miembros dispondrán que los datos personales sean: a) tratados de manera leal y lícita; b) recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines; no se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando los Estados miembros establezcan las garantías oportunas; c) adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente; d) exactos y, cuando sea necesario, actualizados; deberán tomarse todas las medidas razonables para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificadas; e) conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente. Los Estados miembros establecerán las garantías apropiadas para los datos personales archivados por un período más largo del mencionado, con fines históricos, estadísticos o científicos».

⁵⁶ Art. 16 Dir95 («Confidencialidad del tratamiento») y art. 17 Dir95 («Seguridad del tratamiento»).

⁵⁷ Art. 4 Dir2002 («Seguridad») y 5 Dir2002 («Confidencialidad de las comunicaciones»).

lo hará cuando se dicte sentencia en una importante cuestión prejudicial, recientemente planteada, y que afecta directamente a la determinación del contenido del derecho a la protección de los datos personales⁵⁸. En el caso Bodil Lindqvist, el tribunal nacional ha formulado al TJ siete cuestiones, todas ellas importantísimas.

4. En el Derecho Español se recogieron estos cinco principios básicos del derecho a la protección de datos personales en la normativa general de protección de datos: así ocurría en la LORTAD de 1992 y así se ha reiterado en la LOPD de 1999: consentimiento (arts. 6.1 y 6.4 LOPD), información (derecho a demandar y a recibir la misma, arts. 5.1 y 5.4 LOPD), control (rectificación y cancelación mediante un recurso individual y una garantía orgánico-procedimental, arts. 15.1, 16.2 y 37.1 LOPD), calidad y lealtad (exactitud y actualidad de los datos, tratamiento proporcionado, art. 4.1 LOPD), y seguridad y confidencialidad (arts. 9.1 y 10 LOPD). La normativa sectorial de telecomunicaciones traslada fielmente a España lo previsto en las disposiciones comunitarias, ya referidas, en materia de protección de datos personales (concretamente, en relación con las facturas desglosadas, los datos de tráfico, los datos de localización y las guías de abonados)⁵⁹.

Sin embargo, el Derecho español ha ido más allá de lo previsto en el Derecho comunitario, y la normativa especial en materia de comercio electrónico⁶⁰ ha precisado los principios de consentimiento y de calidad y lealtad. Por lo que hace al del consentimiento, la ley española incorpora la exigencia del mismo en el momento «inicial» de la recogida de los datos y, en consecuencia, prohibiendo el «correo basura» (art. 21 LSSI). En

⁵⁸ Asunto C-101/01: Petición de decisión prejudicial presentada mediante resolución del Göta Hovrätt, de fecha 23 de febrero de 2001, en el asunto entre Bodil Lindqvist v. Kammaråklagaren (Ministerio público), Jönköping (DOCE C 118/2001, de 20 de abril, p. 19). Por cierto, la transcripción del nombre del caso en la edición española del DOCE sólo se puede calificar de lamentable.

⁵⁹ Art. 50 de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones, desarrollado por los arts. 62 ss. del Real Decreto 1736/1998, de 31 de julio, por el que se aprueba el Reglamento por el que se desarrolla el Título III de la Ley General de Telecomunicaciones en lo relativo al servicio universal de telecomunicaciones, a las demás obligaciones de servicio público y a las obligaciones de carácter público en la prestación de los servicios y en la explotación de las redes de telecomunicaciones.

⁶⁰ Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico [LSSI].

cuanto al principio de de calidad y lealtad, la normativa hispana, acogién-dose a la posibilidad abierta por el Derecho comunitario (art. 15 Dir2002), impone el deber de retener los datos de tráfico por un período máximo de doce meses a los operadores de redes y servicios de comunicaciones electrónicas, los proveedores de acceso a redes de telecomunicaciones y los prestadores de servicios de alojamiento de datos (art. 12.1 LSSI). Ahora bien, esta recogida de datos debe ser proporcionada a la finalidad legal (calidad y lealtad) y, por eso, los datos que deban conservar los operado-res de redes y servicios de comunicaciones electrónicas y los proveedores de acceso a redes de telecomunicaciones serán únicamente los necesarios para facilitar la localización del equipo terminal empleado por el usuario para la transmisión de la información. Por su parte, los prestadores de servicios de alojamiento de datos deberán retener sólo aquéllos impres-cindibles para identificar el origen de los datos alojados y el momento en que se inició la prestación del servicio. Esto significa que «en ningún caso, la obligación de retención de datos afectará al secreto de las comunica-ciones». Los operadores de redes y servicios de comunicaciones electrón-icas y los prestadores de servicios «no podrán utilizar los datos reteni-dos para fines distintos de los indicados en el apartado siguiente u otros que estén permitidos por la Ley» (art. 12.2 LSSI).

5. La Carta, en lugar de «consolidar» esos cinco principios, supone un paso atrás en alguno de ellos. Tienen una recepción aceptable los prin-cipios de consentimiento y de calidad y lealtad que están recogidos de forma sucinta pero suficiente. No sucede lo mismo con los principios de información, de control y de seguridad y confidencialidad. El principio de información tal y como se recoge en la CDF sólo abarca el derecho a «demandar» información («derecho a acceder a los datos que le concier-nan»), pero no parece que incluya el derecho a «recibir» información (es decir, deber del poseedor del responsable del fichero de comunicar al inter-esado los datos que obren en el mismo si antes no lo hubiera hecho ya). En cuanto al principio de control, el art. 8.2 CDF sólo alude a la posibilidad de «rectificación» de datos, pero omite la referencia a su bor-rado o cancelación. Por su parte, la CDF carece de cualquier alusión al principio de seguridad y de confidencialidad que ya estaba contemplado en el Convenio del Consejo de Europa de 1981⁶¹. En definitiva, el conte-

⁶¹ Coincidimos con Battaglia en que el art. 8.2 CDF no incorpora el principio de «seguridad», pero no tanto en la falta los principios de «exactitud» de las infor-

nido del derecho a la protección de los datos personales tal y como aparece en la CDF presenta graves deficiencias.

IV. CONCLUSIONES

1.º La Carta de los Derechos Fundamentales está lejos de cumplir con el objetivo propuesto en la cumbre de Colonia de 1999 ya que ni facilita la consolidación de un estatuto jurídico único para los derechos fundamentales (y, en concreto, para el derecho a la protección de datos personales aquí estudiado), ni elimina la ambigüedad (o disputa) acerca de la relación de los derechos fundamentales constitucionales con el Derecho Comunitario.

2.º El sistema normativo del Consejo de Europa reconoce el derecho a la protección de los datos personales como un contenido específico del derecho a la protección de la vida privada. Así, se desprende del Convenio de 1981 y de la jurisprudencia de Estrasburgo. El TEDH reconoce a los Estados un amplio margen de apreciación en la regulación de este derecho.

3.º A diferencia de otros derechos, el que protege los datos personales, entendido como algo distinto del derecho a la intimidad, no fue introducido en la Unión Europea por la jurisprudencia (pese a que ésta sí ha reconocido el derecho a la intimidad y ha tenido oportunidad de confirmar expresamente el derecho a la protección de datos en algún caso —el *Campogrande*—), sino por la legislación comunitaria.

4.º La regulación del derecho a la protección de los datos personales por el ordenamiento comunitario derivado plantea el problema de cuál es la base jurídica sobre la que la Comunidad realiza esta legislación. La legislación y la jurisprudencia aducen como fundamento legitimador de la normativa comunitaria el título «establecimiento del mercado interior». Sin embargo, consideramos que este título no es suficiente para sustraer al Estado su competencia exclusiva de regulación de los derechos fundamentales.

maciones recogidas y de «proporcionalidad» en la recogida de datos. Cfr. Elisa BATTAGLIA y Giacomo DI FEDERICO, «La Carta dei diritti e la tutela della riservatezza», en Lucia SERENA ROSSI (ed.), *Carta dei diritti fondamentali e Costituzione dell'Unione Europea*, Giuffrè, Milán, 2002, p. 205 ss. (p. 220). A nuestro entender, sin embargo, ese principio de «exactitud» está, al menos parcialmente, cubierto por la posibilidad expresamente prevista de «rectificación». En cuanto al que Battaglia llama principio de «proporcionalidad», lo consideramos incluido en lo que denominamos principio de calidad y lealtad que sí está recogido en la CDF.

5.º El derecho a la protección de datos en la legislación comunitaria se encuentra fundamentalmente en sendas directivas de 1995 y de 2002 (que sustituye a otra de 1997). Además, es preciso mencionar un reglamento de 2001 que, en desarrollo del art. 286 del TCE, establece el régimen jurídico de este derecho respecto a los datos tratados por los organismos comunitarios. Todas estas normas presuponen la vinculación del derecho a la protección de datos con el derecho a la intimidad.

6.º En el llamado «tercer pilar» se produce la paradoja de que la protección de datos personales no se instrumenta a través de las normas emanadas en el «primer pilar» (comunitario), sino del Derecho del Consejo de Europa.

7.º El derecho a la protección de datos aparece en otros instrumentos internacionales, mayormente en el marco de la OCDE y de la OMC. Aunque la OCDE inicialmente promovió unos instrumentos muy reticentes ante el derecho a la protección de datos personales, a partir de 1998 ha modificado su postura patrocinando la adopción de políticas favorables a este derecho.

8.º Varias Constituciones de los Estados acogen el derecho a la protección de los datos personales, bien expresamente y de forma autónoma (Portugal, Suecia), bien como una derivación del derecho a la intimidad (o a la vida privada) ya consagrado (España, Finlandia, Holanda). Donde no se dan estas circunstancias la jurisprudencia crea *ex novo* el derecho (Alemania).

9.º El contenido del derecho típico se suele vertebrar en torno a los principios que ya se consagraron en el C1981 del Consejo de Europa. El Derecho comunitario derivado, fundamentalmente, las directivas de 1995 y 1997, ha llevado a cabo un desarrollo generoso del Convenio de 1981, con algún retroceso en la directiva de 2002. El Derecho Español ha ampliado en algún aspecto (consentimiento «inicial») el contenido del derecho a la protección de datos reconocido en el ámbito comunitario y, si bien también ha optado por imponer el deber de retención de datos de tráfico en las comunicaciones electrónicas, lo ha hecho con respeto al principio de calidad y lealtad. Sin embargo, la Carta de Derechos Fundamentales ha consagrado el derecho a la protección de datos con una redacción desafortunada que, si bien mantiene los principios de consentimiento, control y calidad, cercena el principio de información e ignora el de confidencialidad y seguridad.

ABSTRACT

This paper wants to dress a sharp criticism on two points: the way in which the human rights have been recognised in the European Charter with reference to the consequences for the right of data protection and, second, the way in which the content of the right to data protection is drafted. The first point of this article is the idea that the European Charter of Human Rights, was not a proper implementation of the conclusions reached in the Summit of Colony where a mandate was given to draft a single statute of the human rights consolidated in the European level. On the contrary, the European Charter consecrates various status and levels of protection of human rights. As the right of the protection of personal data is concerned this means that any study of it, as contained in the European Charter, should refer to all those normative levels, recognised in the Charter, which acknowledge the right of data protection. This is why, on the first part of the paper we try to show what are all those normative systems, whose reception is made by the Charter, and what is the meaning that they give to the data protection. The systems referred at are, first, the Council of Europe (the European Convention of Human Rights and the case law rendered by the European Court of Human Rights); second, the «Community Law» («first pillar») whose legitimacy to enact directives on data protection is questioned here; third, the Law of the European Union as the «third pillar» is concerned; fourth, the law of the ODCE and the WTO; and, fifth, the Constitutions of the member States. The second point of this article deals with the content of the right of data protection. The study leads us to say that some of the «typical contents» of the right are not or are improperly recognised in the Charter. Taking into consideration the five principles considered as basic contents of the right, we are of the opinion that, although the principles of consent, control and quality are properly drafted, the principle of information has been cut down and the principle of confidentiality and security is ignored. Hence, before the incorporation of the Charter to an eventual new legal instrument were decided, should the Charter be re-drafted.

RESUMÉE

Cet article veut habiller une forte critique sur deux points : la manière dont les droits de l'homme ont été identifiés dans la charte européenne concernant les conséquences pour le droit à la protection des données et, en second lieu, la manière dans lesquelles la teneur du droit à la protection des données est rédigée. Le premier point de cet article est l'idée que la charte européenne des droits de l'homme, n'était pas une exécution appropriée des conclusions atteintes dans le sommet de Cologne qui avait donné un mandat pour rédiger un statut simple des droits de l'homme consolidés au niveau européen. Au contraire, la charte européenne consacre des divers statuts et niveaux de la protection des droits de l'homme. Pour ce qui concerne au droit à la protection des données personnelles, tout étude du même, selon son contenu dans la charte européenne, devrait se rapporter à tous ces niveaux normatifs, identifiés

dans la Charte, qui reconnaissent le droit à la protection de données. C'est pourquoi, dans la première partie de l'article nous essayons de montrer ce qui sont tous ces systèmes normatifs, dont la réception est faite par la charte, et ce qui est la signification qu'ils donnent à la protection de données. Les systèmes référés par la Charte sont, premier, le Conseil de l'Europe (la convention européenne des droits de l'homme et la jurisprudence rendue par la cour européenne des droits de l'homme); en second lieu, le «droit communautaire» («premier pilier») dont la légitimité pour légiférer des directives concernant la protection de données est remis en cause ici; troisièmement, le Droit de l'union européenne en ce qui concerne le «troisième pilier»; quatre, le Droit de l'ODCE et la WTO; et, cinquième, les constitutions des Etats membres. Le deuxième point de cet article traite la teneur du droit de la protection de données. L'étude nous mène à dire que certaines «des contenus typiques» du droit ne sont pas ou sont incorrectement reconnues dans la charte. Prenant en compte les cinq principes considérés comme contenu de base du droit, nous sommes de l'opinion que, bien que les principes du consentement, du contrôle et de la qualité soient correctement rédigés, le principe d'information a été réduit et le principe de la confidentialité et de la sécurité est ignoré. Par conséquent, avant l'incorporation de la charte à un nouvel instrument juridique, la charte devrait-elle être reformulée.

