APROXIMACIÓN A LA PROTECCIÓN JURÍDICA INTERNACIONAL DEL DERECHO DE ACCESO Y PROTECCIÓN DE DATOS EN EUROPA

VÍCTOR LUÍS GUTIÉRREZ CASTILLO
Profesor de Derecho Internacional Público
y Relaciones Internacionales
Universidad de Jaén
vlguti@ujaen.es

PALABRAS CLAVE: Derechos Humanos • Privacidad • Protección internacional personal data • Derecho protección de datos personales • Derecho acceso a datos

KEY WORDS: Humans Rights • Privacy • International protection personal data Right to the protection of personal data • Right of access to data.

1.- INTRODUCCIÓN

Las Administraciones Públicas recurren cada vez más a las nuevas tecnologías para el desarrollo de su actividad. La utilización de los nuevos sistemas de información y comunicación para relacionarse con los ciudadanos y para mejorar su funcionamiento interno contribuyen positivamente a la consolidación de su propia legitimidad social. Sin embargo, el desarrollo de la actividad electrónica y la consiguiente acumulación de datos personales por parte de los poderes públicos, así como las trabas burocráticas a su acceso por sus titulares suponen una amenaza para el derecho a la intimidad y otros derechos fundamentales.

Con este trabajo pretendemos hacer un análisis sobre el derecho al acceso y protección de datos personales en el marco de las principales organizaciones internacionales que afectan al continente europeo, razón por la que nos detendremos principalmente en los instrumentos internacionales creados en el marco de estas últimas. Especial atención, como no podría ser de otra forma, prestaremos al Con-

sejo de Europa y la Unión Europea, deteniéndonos en este caso en la Carta de los Derechos Fundamentales contenida en el Tratado por el que se establece una Constitución para Europa.

Tradicionalmente la protección de los datos personales ha estado vinculada al derecho fundamental a la intimidad personal y familiar. Así aparece recogido en diversos textos internacionales que lo configuran como un derecho singular que emerge como facultad de autodeterminación de la persona frente al desarrollo de la informática y la telemática que, como se sabe, permite la recogida masiva de datos de los individuos y su tratamiento[1]. A pesar de esta circunstancia, conviene distinguir entre el derecho a la intimidad personal y familiar, de los derechos relativos al acceso y protección de datos. La diferencia radica en que mientras el primero está dirigido a proteger a la persona frente a cualquier invasión que pueda realizarse en el ámbito de su vida personal y familiar (que la misma desee excluir del conocimiento ajeno), el segundo y el tercero persiguen garantizar al individuo un poder de control o disposición sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para su dignidad y derecho[2].

Especial importancia para ese "poder de control o disposición de datos personales" tienen estos derechos en el marco del Genoma humano pues, como ha señalado el profesor Faramiñán Gilbert[3], "por lo que respecta al hombre, el genoma, que es el código de su identidad genética, deberá también preservarse; dado que afecta a su intimidad más profunda, su conocimiento puede permitir a la medicina predictiva descubrir en el embrión humano la predisposición a determinadas enfermedades, que si bien tiene un aspecto positivo, presenta una cara oscura ante la tremenda presión psicológica que supone para el paciente el conocimiento de la propensión a una enfermedad que aún no tiene cura, o la discriminación de ciertos individuos por parte del Estado, empresas o compañías aseguradoras, ante el conocimiento público de esas circunstancias".

[1] En este sentido se expresa don Juan Manuel Fernández López, Magistrado y ex-director de la Agencia de Protección de Datos, en "El derecho fundamental a la protección de los datos personales. Obligaciones que derivan para el personal sanitario", *Revista de derecho y salud. Extraordinario XI Congreso Derecho y Salud. Asociación Juristas de la Salud,* volumen 11, Pamplona, 2003.

[2] *Vid.* J. Sánchez-Caro y F. Abellán, *Datos de salud y datos genéticos. Su protección en la Unión Europea y en España*, Editorial Comares, Granada, 2004, pp. 9-10.

[3] J.M. de Faramiñán Gilbert, "Los bienes intangibles de la especie humana (el genoma humano como patrimonio común de la humanidad" en AAVV**:** *Héctor Gros Espiell Amicorum Liber. Persona Humana y Derecho Internacional***,** Ed. E. Bruylant, 1997, Bruselas (Bélgica), pp. 311-336. *vid. etiam* del mismo autor "Legislación comunitaria y manipulación genética", *Manipulación genética: metodología, aplicaciones y bioética*, ed. UNED. Centro Asociado Andrés Vandelvira, Jaén 2001, pp. 146-163.

2.- LA PROTECCIÓN JURÍDICA INTERNACIONAL DE DATOS PERSONALES EN EL MARCO DE LA ORGANIZACIÓN DE NACIONES UNIDAS

A pesar de que la "intimidad" puede ser concebida de forma distinta dependiendo del entorno cultural en el que nos encontremos, no podemos ignorar la existencia de un denominador común en todas las legislaciones y ordenamientos jurídicos: el hecho de entenderla como el "respeto a la protección personal y familiar" de todo individuo. Buena prueba de ello es el reconocimiento que de la misma hacen los textos internacionales, como la Declaración Universal de los Derechos Humanos de 1948[4]; el Pacto Internacional de Derechos Civiles y Políticos de 1966[5] y la Declaración Universal sobre el Genoma Humano y los Derechos Humanos, de 16 de noviembre de 1999, que sitúan siempre su protección en la esfera de la vida privada.

Ahora bien, si bien es cierto que ese concepto ha sido valido y útil durante muchos años, no podemos ignorar que en algunos ámbitos, como el que nos ocupa, la realidad social va por delante de las normas. Debido al continuo avance de la técnica y la informática ha sido necesario dotar de una cierta autonomía al derecho de acceso y protección de datos personales. Y es que, aunque los instrumentos tradicionales le han dispensado una cierta protección bajo el amparo del derecho a la intimidad, la naturaleza y especificidad de los derechos afectados demanda una mejor (y mayor) cobertura. A esta demanda han respondido el conjunto de directrices para la regulación de los archivos de datos personales informatizados, adoptadas por la Resolución 45/95 de la Asamblea General, de 14 de diciembre de 1990[6]. En virtud la misma los procedimientos para aplicar las normas relativas a los archivos de datos personales informatizados se dejan a iniciativa de cada Estado, con sujeción a una serie de orientaciones, entre las que cabe destacar la relativa a ciertos principios que deberían observarse en las legislaciones nacionales: principio de legalidad y lealtad[7], de exactitud[8], de especificación de la finalidad[9], de acce-

[4] Adoptada y proclamada por la Resolución de la Asamblea General 217 A (iii) del 10 de diciembre de 1948. *Vid.* http://www.un.org/spanish/aboutun/hrights.htm.

[5] Pacto de Derechos Políticos de 1966, adoptado y abierto a la firma, ratificación y adhesión por la Asamblea General en su Resolución 2200 A (XXI), de 16 de diciembre de 1966. *Vid.* http://www.unhchr.ch/spanish/html/menu3/b/a_ccpr_sp.htm.

[6] Adoptada en la 68ª sesión plenaria. Su contenido puede consultarse en http://www.un.org/spanish/documents/ga/res/45/list45.htm.

[7] La información relativa a las personas no debe ser recogida o procesada por métodos desleales o ilegales, ni debe ser utilizada para fines contrarios a los fines y principios de la Carta de Naciones Unidas.

[8] En virtud de dicho principio las personas responsables de la compilación de archivos, o responsables de mantenerlos, tienen la obligación de llevar a cabo comprobaciones periódicas acerca de la exactitud y pertinencia de los datos registrados y garantizar que los mismos se

so de la persona interesada[10], de no discriminación[11], de excepción y de seguridad[12].

Las primeras iniciativas que se vislumbran en el plano internacional se remontan a la Conferencia Internacional de Derechos Humanos celebrada en Teherán el de 13 de mayo de 1968[13], donde se inició el debate sobre la incidencia del uso de la electrónica en los derechos individuales. Como resultado de dicha Conferencia, la Asamblea General adoptó una resolución invitando al Secretario General a iniciar un estudio sobre el uso de la electrónica y su incidencia en los derechos de las personas, así como sobre los límites que la sociedad democrática debía imponer. El Secretario General sometió un estudio preliminar a la Comisión de Derechos Humanos, la cual, delimitó en 1971 las líneas del futuro estudio en dos direcciones: una primera, la que analizaba los posibles peligros que el desarrollo científico podía tener para el disfrute de los derechos humanos; y una segunda, la que discutía las formas en la que dichos desarrollos podrían contribuir a mejorar las condi-

mantengan de la forma más completa posible, con el fin de evitar errores de omisión, así como de actualizarlos periódicamente o cuando se use la información contenida en un archivo, mientras estén siendo procesados.

[9] La finalidad a la que vaya a servir un archivo y su utilización en términos de dicha finalidad debe ser especificada, legitimada y, una vez establecida, debe recibir una determinada cantidad de publicidad o ser puesta en conocimiento de la persona interesada, con el fin de que posteriormente sea posible garantizar que: a) todos los datos personales recogidos y registrados sigan siendo pertinentes y adecuados para los fines especificados; b) ninguno de los referidos datos personales sea utilizado o revelado, salvo con el consentimiento de la persona afectada, para fines incompatibles con aquellos especificados; c) el período durante el que se guarden los datos personales no supere aquel que permita la consecución de dichos fines.

[10] Dicho principio implica que cualquiera que ofrezca prueba de su identidad tiene derecho a saber si está siendo procesada información que le concierna y a obtenerla de forma inteligible, sin costes o retrasos indebidos; y a conseguir que se realicen las rectificaciones o supresiones procedentes en caso de anotaciones ilegales, innecesarias o inexactas, y, cuando sea comunicada, a ser informado de sus destinatarios.

[11] En virtud de dicho principio no deben ser recogidos datos que puedan dar origen a una discriminación ilegal o arbitraria, incluida la información relativa a origen racial o étnico, color, vida sexual, opiniones políticas, religiosas, filosóficas y otras creencias, así como la circunstancia de ser miembro de una asociación o sindicato.

[12] Deben adoptarse medidas adecuadas para proteger los archivos tanto contra peligros naturales, pérdida o destrucción accidental, el acceso no autorizado, uso fraudulento o la contaminación mediante virus informáticos.

[13] En su declaración 18 ya se vislumbraba una preocupación por la amenaza de los nuevos cambios y el avance de las tecnologías en el plano de los derechos humanos. En dicho apartado afirma que " Si bien los recientes descubrimientos científicos y adelantos tecnológicos han abierto amplias perspectivas para el progreso económico, social y cultural, esta evolución puede, sin embargo, comprometer los derechos y las libertades de los individuos y por ello requerirá una atención permanente". Para consultar el texto integro en español *vid.* http://www.acnur.org/biblioteca/pdf/1290.pdf.

ciones de vida y el disfrute de los derechos económicos sociales y culturales en la comunidad internacional. Estas iniciativas y directrices lejos de caer en el olvido han sido tenidas en cuenta por numerosos Estados y por las organizaciones internacionales de carácter restringido cuyo ámbito de actuación afectan al continente europeo.

3.- EN EL MARCO DE LA ORGANIZACIÓN PARA LA COOPERACIÓN Y EL DESARROLLO ECONÓMICO

Junto a la actividad inicial, que como veremos, realizó el Consejo de Europa a finales de los años sesenta sobre los avances tecnológicos informáticos, la Organización para la Cooperación y el Desarrollo Económico (OCDE) inició una labor importante sobre este tema. El desarrollo del tratamiento automático de datos, que permite la transmisión de enormes cantidades de ellos en segundos a través de las fronteras nacionales, constituyó un motivo de preocupación en los Estados parte de la OCDE[14], los cuales introdujeron importantes reformas en sus legislaciones con el fin impedir el almacenamiento ilícito de datos personales y su revelación no autorizada; circunstancias éstas, consideradas vulneraciones de derechos humanos.

Esta situación provocó con el tiempo una lógica preocupación por proteger la intimidad de los ciudadanos, lo que dio lugar a un desarrollo asimétrico de normas nacionales y, por consiguiente, un inevitable obstáculo a la libre circulación transfronteriza de datos. Por esta y otras razones, en el seno de la OCDE se han elaborado todo un conjunto de directrices que armonizan la normativa nacional relativa a la intimidad y tratan de impedir interrupciones en la circulación internacional de datos. Estas directrices son, en buena medida, resultado de los trabajos realizados por el subgrupo de la OCDE de Bancos de Datos en el Sector Público, el cual comenzó a articular soluciones políticas en este sentido, constituyendo, en 1978, un Grupo de Expertos encargado de estudiar esta problemática. Las directrices mencionadas se llevaron a cabo a través de tres instrumentos internacionales: a) la Recomendación de 23 de septiembre de 1980 en la se que insta 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"[15], b) la Declaración de 11 de abril de 1985 "sobre flujos transfronterizos de

[14] Alemania, Austria, Bélgica, Dinamarca, España, Finlandia, Francia, Grecia, Hungría, Irlanda, Islandia, Italia, Luxemburgo, Noruega, Países Bajos, Polonia, Portugal, Reino Unido, República Checa, República Eslovaca, Suecia, Suiza, Turquía, Canadá, Estados Unidos, México, Australia, Japón, Nueva Zelanda, República de Corea.

[15] En un principio, algunos Estados se abstuvieron en la votación para la adopción de directrices. Posteriormente todos los Estados se han terminado adhiriendo al texto, e incluso algunos gobiernos han desarrollado unas actividades, tanto normativas y no normativas, como no, destinadas a promover la adopción de las mismas en el sector privado. *Vid.* D. Fernández

datos" y c) la Declaración de 9 de octubre de 1988 "sobre protección de la intimidad en las redes globales"[16].

Las directrices recogidas en estas declaraciones y recomendaciones del Consejo de Ministros representan un consenso sobre principios básicos que en muchos casos se han incorporado a las legislaciones nacionales existentes, sirviendo de fundamento para aquellos países que todavía no disponen de este tipo de regulación. Entre estos principios destacan: el principio de limitación de la recogida de datos[17], el de calidad de datos[18], el de especificación del fin[19], de seguridad[20], transparencia[21], participación del individuo[22] y el de responsabilidad[23].

Todos ellos han sido reafirmados, si bien de forma implícita, en posteriores declaraciones e instrumentos internacionales realizados en el marco de la OCDE, como puede deducirse de la Recomendación relativa a las directrices de política criptográfica, adoptada por el Consejo de la OCDE el 2 de marzo de 1997 y la Declaración Ministerial relativa a la protección de la intimidad en las redes globales adoptado por el Grupo de Trabajo sobre Seguridad de la Información e Intimidad en Ottawa el 7 y 9 de octubre de 1998[24].

---

de Gatta Sánchez, "El régimen jurídico de la protección de datos personales: aspectos internacionales, comunitarios e internos", *Noticias de la Unión Europea*, nº. 149, junio 1997, p. 76.

[16] Para más información sobre éstas y otras Declaraciones *vid.* OCDE, http://www.oecd.org/home.

[17] Dicha obtención se debe realizar por medios legales y legítimos. No se exige que sean dados por el interesado pero sí que en los casos en que sea procedente exista el conocimiento y consentimiento del mismo. *Vid. idem.*

[18] Los datos han de ajustarse a los fines del fichero y deberán ser exactos y completos y, por ello, deberán estar actualizados. *Vid. idem.*

[19] La utilización que se vaya a hacer de los datos debe ser manifestada al obtenerlos y no se podrán usar para fines distintos, salvo aquellos que sin ser incompatibles por los mismos se especifiquen cada vez que sean modificados. *Vid. idem.*

[20] Deberán establecerse las medidas adecuadas para proteger los datos contra los diversos tipos de riesgos, tales como pérdida, acceso, destrucción, uso, modificación de los mismos sin la oportuna autorización. *Vid. idem.*

[21] Deberán adoptarse medidas en relación a la transparencia sobre el procedimiento y forma de recogida de datos y deberá ser posible disponer de medios que permitan determinar fácilmente la existencia y naturaleza de tales datos, su finalidad, la identidad del responsable de los datos y la sede habitual de sus actividades.

[22] Este principio hace referencia al derecho de toda persona física de obtener confirmación sobre la posesión de datos concernientes a su persona por parte del responsable del fichero, el derecho a requerir la comunicación de los datos que le conciernen, así como el de ser informada de los motivos por los que se le deniegue una petición de conformidad con los derechos anteriores, así como impugnar datos que le refieran a ella misma. *Vid. idem.*

[23] El responsable del fichero deberá responder de la observancia de las medidas tendentes al cumplimiento de los principios que se establecen. *Vid. idem.*

[24] La Declaración relativa a la Protección de la Intimidad en las Redes Globales fue adoptada por los Ministros en la Conferencia Ministerial de Ottawa celebrada los días 7 a 9 de octubre

4.- EN EL MARCO DEL CONSEJO DE EUROPA.

La preocupación del Consejo de Europa en esta materia puede considerarse pionera en el ámbito de las organizaciones internacionales; ya en 1967, se constituyó en su seno una Comisión consultiva para estudiar el impacto de las nuevas tecnologías en la esfera de los derechos humanos. Resultado de ese incipiente interés fue la Resolución 509 de la Asamblea del Consejo, adoptada en el año 1968, sobre "los derechos humanos y los nuevos logros científicos"[25], la Resolución del Comité de Ministros de 26 de septiembre de 1973, relativa a "la protección de la vida privada de las personas físicas a los bancos de datos electrónicos en el sector privado"[26], y un año más tarde, el 20 de septiembre de 1974, otra resolución relativa al sector público.

En el marco del Consejo de Europa la protección de los datos personales se articula fundamentalmente a través de tres instrumentos internacionales: el Convenio Europeo de Derechos Humanos de 1950 (CEDH)[27], el Convenio para la protección de las personas con respecto al tratamiento de datos de carácter personal 1981 (C1981)[28] y, en menor medida, el Convenio de prevención de la tortura de 1987 (C 1987)[29]. Otros instrumentos internacionales dignos de destacar son el Convenio para la Protección de los Derechos Humanos y la Dignidad del Ser Humano con respecto a las aplicaciones de la Biología y la Medicina, firmado en

---

de 1998, titulada "Un mundo sin fronteras: comprender el potencial del comercio electrónico global". En su 934 sesión, celebrada el 19 de octubre de 1998, el Consejo adoptó una Resolución en virtud de la cual se integra la presente Declaración en los instrumentos de la Organización.

[25] Adoptada el 31 de enero de 1968 (16ª sesión) (Doc. 2326). *Vid.* http://www.coe.int/PortailEN_Search.asp.

[26] Dicha Resolución es fruto de los trabajos y propuestas de la Comisión de expertos creada en 1971 por decisión del Comité de Ministros del Consejo de Europa.

[27] Convenio Europeo Derechos Humanos, quedó abierta a la firma, en Roma el 4 de noviembre de 1950 y entró en vigor el 3 de septiembre 1953. El texto integro se encuentra en http://conventions.coe.int/Treaty/EN/cadreprincipal.htm

[28] Firmado en Estrasburgo el 28 de enero de 1981 y con entrada en vigor el 1 de octubre de 1985. El texto íntegro se encuentra en http://conventions.coe.int/Treaty/EN/cadreprincipal.htm.

[29] Firmado en Estrasburgo el 26 de noviembre 1987, entrada en vigor el 1 de febrero de 1989. El texto íntegro se encuentra en http://conventions.coe.int/Treaty/EN/cadreprincipal.htm

Oviedo el 4 de abril de 1997[30] y la Convención sobre el Cibercrimen, aprobado en Budapest el 23 de noviembre del 2001[31].

El primero de ellos, el CEDH, no protege de forma autónoma los derechos de acceso y protección de datos, pero si le proporciona su protección, ya que reconoce de forma expresa el "derecho a la vida privada y familiar, de su domicilio y correspondencia". Este derecho, como veremos a continuación, ha sido interpretado de forma amplia por el Tribunal Europeo de Derechos Humanos, dando cabida en él a los derechos de acceso y protección de datos. Esto se ha conseguido mediante una interpretación amplia del concepto "vida privada", incluyendo no solo los aspectos realmente privados e íntimos de la vida de una persona, sino también su integridad física y psicológica, el desarrollo de su personalidad, sus relaciones personales y sociales -incluidas las relativas al contexto empresarial y laboral-, su nombre, sus orígenes biológicos y su identidad sexual. Ahora bien, esta protección derivada del concepto "vida privada" ha supuesto en la práctica una negación de la autonomía del derecho al acceso y protección de datos, ya que la jurisprudencia ha interpretado tradicionalmente que para que una persona pueda exigir estos derechos debe enmarcar su defensa en el ámbito del artículo 6 y 8 del Convenio, debiendo demostrar su vínculo directo e inmediato con su vida privada y familiar[32]. Prueba de lo expuesto son las sentencias recaídas en los casos Leander *versus* Suecia (sentencia del 26 de marzo de 1987, serie A, número 116)[33], Z *versus* Finlandia (sentencia del 25 de febrero de 1997, Informes (*Reports*) 1997-I)[34], M.S. *versus* Sue-

[30] La protección a la vida privada y derecho a la información se recoge en el capítulo III del dicho Convenio y, en concreto, en su artículo 10, donde se establece que "toda persona tendrá derecho a que se respete su vida privada cuando se trate de informaciones relativas a la salud"; firmado en Oviedo el 4 de abril de 1997, con entrada en vigor el 1 de diciembre de 1999. El texto íntegro se encuentra en http://conventions.coe.int/Treaty/EN/cadreprincipal.htm

[31] Entrada en vigor el 1 de julio del 2004. Para más información *vid.* http://conventions.coe.int/Treaty/EN/cadreprincipal.htm.

[32] *Vid.* J. Darcy, "Acceso a los datos y su protección en la era de la Administración Electrónica, desde la perspectiva del Convenio Europeo de Derechos Humanos", en *Revista de la Agencia de Protección de Datos de la Comunidad de Madrid*, (datospersonales.org n.º 13 - 27 enero 2005).

[33] El caso surgió cuando se denegó al solicitante un puesto de trabajo en el sector público que requería permisos de seguridad que, en este caso, no se concedieron. La policía reunió un expediente sobre él que nunca se le permitió ver. El Tribunal afirmó que se trataba de una cuestión al amparo del artículo 8, puesto que el archivo secreto contenía información sobre la vida privada del señor Leander: *"Tanto el registro como la difusión de dicha información, combinados con el hecho de no dar al señor Leander la oportunidad de refutarlos, constituyen una interferencia con su derecho al respeto a la vida privada de acuerdo con lo garantizado según el artículo 8, párrafo 1"* (párrafo 48, la cursiva es nuestra).

[34] En este caso los datos en cuestión eran de carácter médico. Z era una mujer finlandesa que se casó con un hombre (X) a quien conoció cuando vivía en el extranjero. Ambos fueron a vivir a Finlandia. Él fue acusado de varias agresiones sexuales. Cuando se descubrió que tenía

cia (sentencia del 27 de agosto de 1997, Informes (*Reports*) 1994-IV) [35], Amann *versus* Suiza ([GC], número 27798/95, párrafo 65, CEDH 2000-II)[36], Rotaru *versus* Rumania ([GC], número 28341/95, CEDH 2000-V)[37], etc.

---

el VIH, se cambiaron los cargos por los de intento de asesinato. Para demostrar los cargos, fue necesario establecer la fecha en la que él se había enterado de la enfermedad. Z se negó a testificar en contra de su marido. Por esta razón, el tribunal que lo juzgaba ordenó la revelación del expediente médico de X, en el que se incluía información sobre el estado de Z con relación al VIH. Además, el tribunal obligó a los médicos y al psiquiatra de Z a que prestaran declaración sobre el historial médico de Z. Ella protestó pero al final decidió testificar, puesto que la información ya se había divulgado. Presentó dos quejas sobre esta fase de las diligencias penales: relativa al hecho de que sus médicos se habían visto obligados a revelar sus datos médicos y al hecho de que se habían incluido copias de su expediente médico en el archivo de la acusación. X fue condenado y apeló. El caso llegó ante el Tribunal de Apelación. Z presentó otras dos quejas ante el Tribunal de Estrasburgo por dos aspectos de la fase de apelación: en primer lugar, el tribunal finlandés dictaminó que el archivo procesal, que contenía sus datos, debía mantenerse en secreto sólo durante 10 años, en lugar de 30. En segundo lugar, en su sentencia, el Tribunal de Apelación la identificó por su nombre y describió su situación médica con cierto grado de detalle. En su sentencia, el Tribunal de Derechos Humanos no tuvo que dedicar tiempo a estudiar si se trataba de una cuestión sobre la vida privada: todas las partes aceptaron que sí lo era y que se habían producido interferencias. Las cuestiones de legitimidad y de finalidad legítima tampoco admitían dudas. El Tribunal declaró que *"tendría en cuenta que la protección de los datos personales, y entre ellos los datos médicos, es de importancia fundamental para que una persona pueda ejercer su derecho al respeto a la vida privada y familiar tal y como se garantiza en virtud del artículo 8 del Convenio. La legislación nacional debe, pues, incluir los mecanismos de protección necesarios para evitar cualquier comunicación o revelación de datos de salud personal que no se correspondan con las garantías del artículo 8 del Convenio (art. 8) (véanse, adaptando lo que proceda, los artículos 3, párrafo 2 (c), 5, 6 y 9 de la Convención para la protección de las personas físicas en lo que respecta al tratamiento automático de los datos personales (Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data), del Tratado Europeo serie número 108, Estrasburgo, 1981"* (párrafo 95, la cursiva es nuestra).

[35] La solicitante sufrió una lesión como resultado de la cual desarrolló una propensión a padecer dolores crónicos en la espalda. Su estado se deterioró aún más cuando quedó embarazada en 1981. Aunque sólo tenía 30 años, nunca más pudo trabajar a jornada completa y se le otorgó una pensión de invalidez algunos años después. El caso se planteó cuando MS reclamó indemnización por el accidente de 1981, que tuvo lugar en la escuela donde trabajaba. Sin que ella lo supiera, la Oficina de la Seguridad Social se puso en contacto con el hospital donde la habían tratado y pidió los archivos médicos de aquella época. El hospital los entregó, puesto que la ley se lo exigía. La solicitante se enteró de ello más tarde, cuando pidió una copia del archivo de la Oficina sobre su reclamación. Entre los detalles comunicados por el hospital, se encontraba el hecho de que MS se había sometido a un aborto en 1985, puesto que un nuevo embarazo habría hecho insoportable el dolor de la espalda. La Administración argumentó que, al realizar la reclamación de indemnización, la solicitante puso en marcha, a sabiendas, un procedimiento que conllevaría la revelación. Sin embargo, el Tribunal lo rechazó porque la revelación no era algo automático; dependía de la Oficina y únicamente debía incluir los datos que fueran relevantes para la reclamación. Por consiguiente, no existía renuncia a la protección del artículo 8. ¿Constituía la revelación a otra autoridad pública, que estaría obligada a respetar la confidencialidad de la información, una interferencia con la vida privada?. El Tribunal conside-

ró que sí, dado el carácter personal y sensible de los datos, por el hecho de que se hubieran dado a conocer a un grupo más amplio de funcionarios públicos y debido a que se habían recogido y guardado para otro fin. El Tribunal aceptó que la revelación era legítima y que servía al propósito legítimo de proteger el bienestar económico del país. En cuanto a la necesidad, el Tribunal destacó la necesidad de que existan mecanismos de protección apropiados para los datos médicos. Existían normas estrictas sobre la revelación de datos, respaldadas por sanciones de carácter civil y penal, que eran de aplicación al hospital y a la Oficina. Ninguno de los datos comunicados eran irrelevantes para la reclamación efectuada. El Tribunal concluyó que, puesto que había limitaciones importantes que restringían la revelación, así como mecanismos de protección eficaces y adecuados contra el abuso, no existía violación del artículo 8.

[36] El solicitante era un comerciante que vendía distintos artículos, incluido un aparato para depilación. En 1981, recibió una llamada de una mujer de la embajada soviética que estaba interesada en comprar uno. La llamada se interceptó y la policía decidió investigar al solicitante. Introdujeron sus datos básicos y la información sobre el producto en una tarjeta que, a continuación, se almacenó en el listado nacional. En 1990, la existencia de este listado salió a la luz pública. Muchas personas, incluido el solicitante, preguntaron si estaban en él. Recibió una fotocopia de la tarjeta, aunque algunas palabras estaban tachadas. Pidió que se le comunicara el texto omitido, pero las autoridades se negaron alegando motivos de seguridad. Emprendió diligencias legales para pedir daños y perjuicios, así como con el fin de que se dictase una orden judicial que exigiera que el archivo fuera bloqueado y nunca volviera a utilizarse sin su consentimiento. El Tribunal Federal desestimó sus reclamaciones por entender que la infracción de sus derechos era menor, sobre la base de que el término "vida privada" incluye las relaciones sociales en un contexto empresarial o profesional. El Tribunal optó por hacer hincapié sobre una interpretación más amplia de dicho término vinculándolo al extenso ámbito de la Convención de protección de los datos. Se trataba de determinar si el simple hecho de crear y guardar una tarjeta constituye una interferencia con la vida privada del solicitante. El Tribunal fue muy claro sobre este particular: no se trataba de establecer si la existencia de la tarjeta suponía algún tipo de inconveniente para el solicitante. El siguiente paso del análisis era considerar si esta interferencia era conforme con la ley. El Tribunal falló que el fundamento jurídico no era suficiente: los textos aplicables eran demasiado vagos. No establecían el alcance ni las condiciones para el ejercicio de la facultad de obtener, registrar y guardar información por parte de las autoridades. No especificaban las condiciones para la creación de estas tarjetas, los procedimientos que debían seguirse, la información que se podía guardar ni los comentarios que podían estar prohibidos. Todos estos errores en el fundamento jurídico significaban que la interferencia no era legítima a los efectos del artículo 8. Además, la legislación nacional estipulaba que las tarjetas de datos que no fueran necesarias debían ser destruidas, lo que no se había hecho en este caso.

[37] Esta sentencia muestra de forma palpable la evolución de la jurisprudencia, desde la visión limitada de que los datos personales sólo estaban cubiertos por el artículo 8 si se referían a un aspecto genuinamente privado e íntimo de la vida de una persona -como los datos médicos), o si se habían obtenido por algún medio que violase la intimidad (intercepción de llamadas telefónicas, filmación secreta...)-, hasta nuestros días. Evidentemente, la definición de datos personales en la Convención de protección de los datos es mucho más amplia: significa cualquier información relacionada a una persona identificada o identificable. Y es mucho más amplia que la intimidad.

En este orden de ideas cabe señalar que el propio Comité de Ministros del Consejo de Europa ha reconocido que la protección de dicho Convenio no resulta suficiente para preservar los individuos frente al uso abusivo de la informática[38]. Esta ha sido una de las principales razones por las que se aprobara el Convenio núm. 108, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal[39], el cual entraría en vigor el 1 de octubre de 1985[40].

El objeto de este Convenio, según su artículo 1, no es otro que garantizar en el territorio de cada Estado parte el respeto de los derechos y libertades fundamentales de cualquier persona física en relación con el tratamiento automatizado de sus datos de carácter personal[41]. Su ámbito de aplicación abarca, pues, todos los bancos de datos personales existentes en el sector público y privado. Esta circunstancia hace que, por deducción, deba entenderse susceptible de protección la "intimidad" (y por ende, "la vida privada") ante las actuaciones de poderes públicos y de entidades privadas. Desde el punto de vista del sujeto protegido, el Convenio incluye a las personas físicas, pudiendo los Estados partes extender la tutela sobre la intimidad a las personas jurídicas mediante su propia normativa.

Sobre este Convenio, se ha señalado con acierto, que es el primer instrumento internacional dirigido de manera específica a proteger el derecho a la libertad informática; además, se trata de un texto que pretende compaginar el principio de libertad de circulación de información con el de la protección de datos persona-

[38] En efecto, ante la cuestión planteada por la Asamblea Parlamentaria del Consejo de Europa en 1969 sobre si el artículo 8 del CEDH resultaba suficiente para preservar a los individuos frente al uso abusivo de la informática, el Comité de Ministros del Consejo de Europa aprobó dos resoluciones sobre la materia: 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 el Comité de Ministros el 26 de septiembre de 1973 y la 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.

[39] Ratificado por España el 27 de enero de 1984 y publicado en el BOE de 15 de noviembre de 1985.

[40] Veinte años más tarde, el 8 de noviembre del 2001, se firmaría un protocolo adicional, que introduciría dos nuevos artículos, uno sobre la obligación de los Estados partes de establecer una "garantía institucional" de control para supervisar la aplicación de los derechos reconocidos en el Convenio para la protección de las personas con respecto al tratamiento de datos de carácter personal de 1981 y otro referente al establecimiento de cautelas en relación con el flujo transfronterizo de datos. Dicho convenio fue modificado para permitir el acceso de las Comunidades Europeas en Estrasburgo el 15 de junio de 1999.

[41] V. Manteca Vaidelante, "Normativa comunitaria y española sobre protección de datos personales en las telecomunicaciones", *Unión Europea*, Aranzadi, Año XXX, núm. 11, 2003, p. 5.

les[42], siendo uno de los puntos de mayor confusión la posibilidad que ofrece a los signatarios de excluir su aplicación en lo que se refiere a determinadas clases de datos personales[43].

5.- LA PROTECCIÓN JURÍDICA EN LA UNIÓN EUROPEA.

5.1.- LAS PRIMERAS INICIATIVAS.

La protección jurídica de los datos personales en el marco de la Unión Europea no constituye ninguna novedad. De hecho, son numerosas las referencias que encontramos en el derecho originario (artículo 6 del Tratado de la Unión Europea, modificado por el Tratado de Ámsterdam de 1997, y el artículo 286 introducido también por éste último en el Tratado Constitutivo de la Comunidad Europea), el derecho derivado (o institucional), y la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas.

Hay que remontarse a los años setenta para encontrar las primeras iniciativas de las instituciones comunitarias relativas al procesamiento de datos y su protección. De hecho, fue en 1973 cuando el Consejo adoptó una resolución para llevar a cabo ciertas actividades en el terreno de la política informática y, en julio de 1974, otra sobre la política comunitaria en el procesamiento de datos. Durante aquellos años la actividad del Consejo y la Comisión fue incrementando progresivamente en el sector de la informática con la adopción de programas, tales como ESPRIT, RACE y EUREKA que, aunque no se preocupaban en demasía por la protección de datos[44], constituyeron un paso importante en dicho ámbito.

Ahora bien, no son pocos los que consideran que la iniciativa de mayor calado ha sido la "Comunicación sobre protección de las personas en relación al tratamiento de datos personales y la seguridad de los sistemas de información", presentada por la Comisión el 18 de julio de 1990[45] y que incluía una propuesta de Directiva sobre la materia[46]. Dicha propuesta, modificada tras las enmiendas presentadas por el Parlamento Europeo[47] y el Comité Económico[48], ampliaba el abanico de principios en lo relativo a la protección de datos que había contemplado el Convenio del Consejo de Europa. Entre sus aportaciones cabe destacar la regulación diferenciada de los ficheros de datos del sector público y del sector

[42] El Convenio define "datos de carácter personal" como aquella "información relativa a una persona identificada o identificable.

[43] V. Manteca Vaidelante, *cit.*, p. 6.

[44] D. Fernández de Gatta Sánchez, *op. cit.*, p. 81.

[45] DOCE de 5 de noviembre 1990.

[46] COM (90) 314 final, 27 de julio 1990.

[47] Dictamen de 11 de marzo de 1992. DOCE de 27 de noviembre de 1992.

[48] Dictamen de 24 de abril de 1991. DOCE de 7 de junio de 1991.

privado, así como la introducción del concepto de "tratamiento de datos" como fundamento referencial de toda la regulación en esta materia.

Tras un largo *iter*[49] ,y algunas modificaciones, esta iniciativa llegó a convertirse en la Directiva 95/46/CE, de 24 de octubre, relativa a la protección de las personas físicas respecto del tratamiento de datos de carácter personal y de la libre circulación de esos datos[50]. De esta forma, la UE establece por primera vez un instrumento por el que se obliga a los Estados miembros a garantizar la protección de las personas físicas de estos derechos, estableciendo a su vez la no restricción de la libre circulación de datos por razones de protección[51].

5.2.- La directiva 95/46/CE y otros instrumentos de derecho derivado

Dentro de lo que podemos definir como "derecho derivado o institucional" la Directiva 95/46/CE pretende "precisar y ampliar" la protección que brinda el Consejo de Europa con el C1981, ya que extiende la protección de datos personales al ámbito de la vida privada. Así se desprende de su artículo 1.1. de la misma al afirmar que

> "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 Directiva parte de la consideración básica de que las diferencias entre los niveles de protección de los derechos y libertades de las personas y, en particular, los relativos a los datos personales, pueden llegar a impedir su transmisión del territorio de un Estado a otro, y que por ello estas diferencias pueden constituir un obstáculo para el ejercicio de una serie de actividades económicas a escala comunitaria, falseando, por lo tanto, la libre competencia. Por esta razón, prohíbe que la protección a la intimidad y a los datos personales pueda constituir una limitación a su libre circulación.

Ahora bien, dado que esta situación puede producir una clara indefensión o vulneración de derechos, la Directiva reconoce la confidencialidad del tratamiento y su seguridad, obligando a aplicar medidas técnicas y de organización adecuadas

[49] El 20 de febrero de 1995, el Consejo adoptó una posición común (DOCE de 13 de abril 1995), comunicando la Comisión su dictamen al Parlamento Europeo el 24 de febrero de 1995 [SEC (95) 303 final], votando este último 7 enmiendas el 15 de junio de 1995, obligando a la Comisión a modificar su propuesta [COM (95) 375 final, 18 de julio de 1995], aceptando dichas enmiendas y siendo formalmente adoptada por el Consejo y el Parlamento Europeo el 24 de octubre de 1995.

[50] DOCE de 23 de noviembre de 1995.

[51] V. Manteca Valdelante, *op. cit.*, pp. 7-8.

para la protección de los datos contra la destrucción accidental o ilícita y contra la alteración, difusión o acceso no autorizados, incluyendo los riesgos del tratamiento y la naturaleza de los datos a proteger. Por estas razones dicha norma se ha considero como una especie de "directiva marco" cuyos principios requieren una futura elaboración atendiendo a las exigencias de la sociedad y del mercado[52]. Esto es lo que ha sucedido en materia de telecomunicaciones, donde los principios de la Directiva del 95 han sido objeto de un ulterior desarrollo a través de la Directiva 97/66/CE, en la que se pretendió adaptar su contenido al sector de las telecomunicaciones[53].

La finalidad que persigue esta directiva es armonizar la normativa de los Estados miembros en tres aspectos fundamentales: derecho a la intimidad en lo relativo al tratamiento de datos personales en el sector de las telecomunicaciones, libre circulación de dichos datos, y la libre circulación de los equipos y servicios de telecomunicaciones. Esta directiva declara de aplicación subsidiaria la Directiva 95/46/CE antes citada, y amplía el ámbito subjetivo de aplicación a las personas jurídicas[54]. Asimismo, dispone su no aplicación a las actividades que tengan por objeto la seguridad pública, la defensa, la seguridad del Estado y las actividades del Estado en materia penal. No existe, por tanto, una derogación de la Directiva 95/46/CE, pero en aquellos aspectos particulares relativos a la transmisión de datos a través de una red pública de telecomunicaciones será de aplicación preferente la Directiva 2002/58/CE, de 12 julio 2002, relativa al tratamiento de datos personales y a la tutela de la vida privada en el sector de las comunicaciones electrónicas[55].

Hasta aquí los principales instrumentos de derecho derivado que constituyen el marco básico en este tema, marco que se completa con mas directivas, reglamentos y decisiones[56] que, si bien no se refieren directamente a este derecho, sí que perfeccionan su régimen.

[52] F. Glavey, "Accountability, the Right to Privaty and Tirad 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).

[53] DOCE de 30 de enero de 1998.

[54] El respeto que esta Directiva pretende asegurar tanto de los derechos de las personas físicas como de los intereses legítimos de las jurídicas, viene justificado en tanto éstas y aquéllas asumen la condición de "abonado" o de "usuario" de una red pública de telecomunicación. Además, las garantías que ofrece a los intereses legítimos de las personas jurídicas no podrá implicar la obligatoriedad para los Estados miembros de ampliar el ámbito de aplicación de la Directiva 95/46/CE.

[55] Esta directiva deroga la Directiva 97/66/CE. DOCE de 31 de julio del 2002.

[56] Además de las Directivas mencionadas dicho marco lo completan, entre otras, la Directiva 2000/31/CE, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de la sociedad de la información, y especialmente del comercio electrónico, en el mercado interior (DOCE 17 de julio de 2000). En cuanto a los reglamentos destaca el Reglamento 45/2001 de 18 de diciembre del 2000 relativo a la protección de las personas físicas en lo que respecta al

En otro orden de ideas, una de las medidas más eficaces para garantizar la protección del derecho a la intimidad, en general, y los datos personales, en particular, ha sido la creación de una figura independiente para tal fin, nos referimos a la figura del Supervisor Europeo de Protección de Datos (SEPD)[57], instituida por el Reglamento (CE) 45/2001 18 de diciembre de 2000 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a su libre circulación[58].

El SEPD está dirigido por un supervisor y un adjunto[59], designados por el Parlamento Europeo y el Consejo de la Unión Europea por un periodo renovable por cinco años; con la responsabilidad de garantizar el respeto al derecho a la intimidad de las personas en el procesamiento de datos personales por parte de las instituciones y organismos de la UE[60]. Trabaja con los responsables de la protección

tratamiento de datos personales por las instituciones y organismos comunitarios y a la libre circulación de datos (DOCE de 12 de enero 2001), el Reglamento 407/2002 de 28 de diciembre del 2002, por el que se establecen determinadas normas de desarrollo del Reglamento nº. 2725/2000 relativo a la creación del sistema "Eurodac" para la comparación de las impresiones dactilares para la aplicación efectiva del Convenio de Dublín (DOCE de 5 de abril 2002); Reglamento 2725/2000 de 11 de diciembre del 2000, relativo a la creación del sistema "Eurodac" para la comparación de las impresiones dactilares para la aplicación efectiva del Convenio de Dublín (DOCE de 15 diciembre 2000). Para más información sobre normativa comunitaria *vid.* J. F. Durán Alba, "El derecho a la libertad informática (según el artículo 18.4 CE) como límite al correo electrónico no solicitado («Spam»)", en *Actas VIII Congreso Iberoamericano de Derecho Constitucional*, Sevilla 3-5 diciembre 2003, pp. 7-8.

[57] Se creó de conformidad con el artículo 286 del Tratado de la Comunidad Europea.

[58] DOCE de 12 de enero 2001

[59] En 2004, se designó al Sr. Peter Hustin como SEPD y al Sr. Joaquín Bayo Delgado como Supervisor Adjunto. El Supervisor cuenta con una Secretaría, designada por él y que trabaja exclusivamente para él. El SEPD actúa con total independencia, sin pedir ni aceptar instrucciones de nadie. Tanto él como su personal están obligados a guardar como secreta la información confidencial. El Supervisor y el Supervisor Adjunto pueden ser destituidos por el Tribunal de Justicia si no ejercen adecuadamente sus funciones o si son culpables de conducta indebida grave.

[60] Cuando las instituciones u organismos de la UE procesan datos personales sobre una persona que pueda ser identificada, deben respetar el derecho de esa persona a la intimidad. El SEPD se asegura de que así se haga y les aconseja sobre todos los aspectos del procesamiento de los datos personales. El "procesamiento" cubre actividades tales como la recogida, el registro, la organización y el almacenamiento de la información, recuperándola para la consulta, enviándola o poniéndola a disposición de otras personas, así como bloqueando, borrando o destruyendo datos. Existen estrictas normas de protección de la intimidad que regulan estas actividades. Salvo en circunstancias muy específicas no se permite que las instituciones y los organismos de la UE procesen los datos personales que revelan el origen racial o étnico, opiniones políticas, creencias religiosas o filosóficas o la afiliación a algún sindicato. Tampoco pueden procesar datos sobre su vida sanitaria o sexual, a menos que estos datos sean necesarios a efectos sanitarios. Incluso en ese caso los datos deben ser procesados por un profesional sanitario u otra persona que deba atenerse al secreto profesional.

de datos de dichos organismos e instituciones para garantizar que se apliquen las normas de confidencialidad de los mismos[61], publicando cada año un informe en el que se reflejan los resultados obtenidos, discutido en el Parlamento Europeo. Sus funciones han sido desarrolladas recientemente por la decisión del Consejo de 13 de septiembre de 2004[62].

5.3.- LA CARTA DE LOS DERECHOS FUNDAMENTALES (CDF)

Una de las novedades introducidas en el (por ahora inaplicado)Tratado por el que se establece una Constitución para Europa ha sido la incorporación en su texto de la Carta de los Derechos Fundamentales (en la Parte II), lo que supone, a nuestro juicio, un acertado cumplimiento del mandato de la cumbre de Colonia de junio de 1999[63].

Por lo que se refiere a su contenido, entendemos que la Carta dispensa una adecuada protección del derecho a la intimidad y al derecho de acceso y protección de datos al consagrar en su artículo II 68 del derecho a la protección de los datos de carácter personal, la obligación de su tratamiento legal sobre la base del consentimiento del afectado u otro fundamento legítimo previsto en la ley, así como el derecho de acceso y, en su caso, rectificación de datos.

Ahora bien, a pesar de que la Carta ha dado, a nuestro juicio, un paso más en materia de protección al reconocer autonomía a estos derechos, no establece un estatuto jurídico único para los derechos fundamentales (y, en concreto, para el derecho a la protección de datos personales), ya que, toma como referencia a la hora de determinar su alcance (y, en definitiva, su régimen jurídico) la regulación existente en otros instrumentos internacionales y nacionales. Así lo establecen los artículos 52 (apartados 2 y 3) y 53.

El primero de ellos dispone que los derechos reconocidos en la Carta 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

[61] Los responsables de las distintas instituciones son: Parlamento europeo (Jonathan Steele), Consejo de la Unión Europea (Pierre Vernhes), Comisión Europea (Dieter König), Tribunal de Justicia de las Comunidades Europeas (Marc Schauss), Tribunal de Cuentas (Jan Kilb), Comité Economico y social europeo (Vasco de Oliveira), Comité de las Regiones (Petra Karlsson), Banco Europeo (Jean-Philippe Minnaert), Mediador Europeo (Alessandro del Bon), Banco Central Europeo (Wolfgang Sommerfeld), Oficina Europea de Lucha anti-fraude (Louis Smeets), Centro de traducción de órganos de la Unión (Benoît Vitale), oficina de la armonisación en el mercado interior (Joël Bastie), observatorio europeo de fenómenos racistas y xénofobos (Niraj Nathwani).

[62] DOCE de 21 de septiembre del 2004.

[63] Según en el cual "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" (nº. 44).

estos"; de lo que se deduce que cuando exista un mismo derecho reconocido en la Carta y en el TUE o en los tratados comunitarios, serán estos últimos los que determinarán los límites y condiciones de su aplicación.

Una misma idea es la que encontramos en el artículo 52.2, pero referida, en este caso, al CEDH. Según dicho artículo cuando en la Carta y en el CEDH se reconozca un mismo derecho habrá que estar a lo dispuesto en este último para determinar su sentido y alcance, a no ser que aquella permita una interpretación más extensa. Finalmente, el artículo 53 de la CDF introduce una cláusula de "interpretación favorable", ya que 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 forma parte la Unión, la Comunidad o los Estados miembros, así como por las Constituciones de estos últimos.

Teniendo en cuenta lo expuesto hasta el momento y la circunstancia de que estos derechos son objeto del Convenio para la protección de las personas con respecto al tratamiento de datos de carácter personal de 1981 y de forma más indirecta por el TCE (art. 286) y el TUE, parece que a la hora de aplicarlo habrá que hacer un ejercicio comparativo entre el alcance y régimen jurídico que le dispensan dichos instrumentos internacionales y el que le proporciona la Carta. Habría que estar, en este caso, a lo dispuesto en el texto que le reconozca un mayor alcance y protección; empresa que no es fácil en la práctica. En muchas ocasiones la jurisprudencia comunitaria y la de Estrasburgo pueden servir como inestimables criterios hermenéuticos para determinar el alcance de los derechos fundamentales y libertades. Sin embargo, existen supuestos, como el de estos derechos objeto de estudio, en los que la interpretación de los tribunales internacionales no es pacífica. Así, mientras la jurisprudencia del Tribunal Europeo de Derechos Humanos no parece reconocer un carácter autónomo al derecho de protección de datos, considerándolo como una manifestación más del derecho a la protección a la vida privada y la intimidad[64], la jurisprudencia comunitaria ha rehusado por lo general a conectarlos expresamente, por lo que puede afirmarse que estamos ante un reconocimiento implícito de su autonomía. Esta idea parece deducirse de algunas sentencias, como las recaídas en los casos Erich Satuder *versus* Stadt Ulm-Sozialamt[65], Anna-Maria Campogrande *versus* Comisión de las Comunidades Europeas y caso X *versus* Comisión[66].

[64] *Vid.* notas 27 a la 31.

[65] Sentencia de 12 de noviembre de 1969 (C 29/69) Rec. 1969, p. 419

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

6.- CONCLUSIONES

El desarrollo de la actividad electrónica y la consiguiente acumulación por parte de los poderes públicos de datos personales, así como las trabas burocráticas al acceso de los mismos por sus titulares supone una amenaza al derecho de la intimidad y a otros derechos fundamentales. Tradicionalmente la protección de estos datos ha estado vinculada al derecho fundamental a la intimidad personal y familiar. Así lo manifiestan diversos textos internacionales.

La protección de los derechos de acceso y protección de datos ha quedado garantizada tradicionalmente en el marco de las organizaciones internacionales, como demuestran las Resoluciones de Naciones Unidas y en los instrumentos internacionales adoptados al amparo de otras organizaciones internacionales, entre las que destaca el Consejo de Europa. En el ámbito de este último merece especial atención la jurisprudencia del Tribunal Europeo de Derechos Humanos, el cual ha interpretado de forma amplia el concepto "vida privada", incluyendo no solo los aspectos realmente privados e íntimos de la vida de una persona, sino también su integridad física y psicológica, el desarrollo de su personalidad, sus relaciones personales y sociales -incluidas las relativas al contexto empresarial y laboral-, su nombre, sus orígenes biológicos y su identidad sexual. Dicha jurisprudencia, sin embargo, no le ha reconocido plena autonomía a dichos derechos, ya que ha interpretado tradicionalmente que para que una persona pueda exigirlos debe enmarcar su defensa en el ámbito del artículo 6 y 8 del Convenio, debiendo demostrar su vínculo directo e inmediato con su vida privada y familiar.

Por lo que respecta a la Unión europea, cabe señalar que es, sin duda, la que mayor pasos ha dado para la defensa de los derechos de acceso y protección de datos. En este sentido, especial atención merecen la protección que dispensa la Directiva 95/46/CE de 24 de octubre de 1995 y el Reglamento (CE) 45/2001 18 de diciembre de 2000, por el que se instituye el Supervisor Europeo de Protección de Datos.

Esta protección se ve reforzada, como ya hemos señalado, por la inclusión de estos derechos en el Tratado por el que establece una Constitución para Europa, en concreto en su Parte II referida a la Carta de los Derechos Fundamentales de la Unión. A partir de su incorporación, la Carta pasará, una vez que entre en vigor el Tratado, a ser parte del derecho originario, y por tanto gozará de eficacia directa e inmediata en los ordenamientos jurídicos nacionales. Esto significa que los derechos que en ella se recogen se verán protegidos por vía de recursos ante el Tribunal de Justicia de las Comunidades Europeas y el procedimiento de la cuestión prejudicial.

Ahora bien, a pesar de lo expuesto no podemos dejar de reconocer que la Carta no establece un estatuto jurídico único para los derechos fundamentales (y, en concreto, para el derecho a la protección de datos personales), ya que, toma como

referencia a la hora de determinar su alcance, la regulación existente en otros instrumentos internacionales y nacionales.

RESUMEN.- Derecho de protección de datos personales y el derecho al acceso a los mismos se encuentran hoy garantizados en Europa gracias a los instrumentos internacionales adoptados en el marco de las Naciones Unidas, Organización para la Cooperación y Desarrollo Económico, Consejo de Europa y la Unión Europea. El autor hace un análisis de dichos instrumentos internacionales en el artículo.

ABSTRACT.- The right to personal data protection and the right to access to data are today protected in Europe thanks to legal international instruments which have been carried out by United Nations, Organisation for Economic Co-operation and Development, Council of Europe and European Union. The article analyses these legal international instruments.