

PRESENTACION DE D. JOSE MANUEL DE FRUTOS GOMEZ*
ADMINISTRADOR PRINCIPAL
UNIDAD DE PROTECCION DE DATOS PERSONALES
DIRECCION GENERAL JUSTICIA, LIBERTAD Y SEGURIDAD
COMISION EUROPEA

**EL REGIMEN DE LA UNION EUROPEA SOBRE LA PROTECCION DE
DATOS PERSONALES**

Es para mí un placer el tomar parte en este Encuentro Iberoamericano de Protección de datos Personales. Quisiera en primer lugar agradecer al Presidente del Instituto de Transparencia y Acceso a la Información Pública del Estado de México su invitación para asistir a este Encuentro.

I. INTRODUCCION

La protección de datos personales es un tema que cobra un interés creciente y una importancia mayor en nuestra sociedad. Todos somos conscientes de que en la sociedad actual nuestra situación personal, patrimonial o profesional es conocida y utilizada por terceras personas con fines diversos. Unas veces somos conscientes de la existencia de estos datos y de su uso, puesto que nosotros mismos hemos proporcionado dicha información con una determinada finalidad, por ejemplo apertura de una cuenta bancaria, compra de un vehículo. En otros casos, sin embargo no somos conscientes de la existencia de dicha información en posesión de terceras personas y aún menos del uso que de la misma se hace. Todos nos hemos extrañado de recibir información comercial acerca de productos o empresas con los que jamás hemos tenido contacto; o quién no ha sido víctima del llamado “spamming” que inunda nuestro correo electrónico o de mensajes comerciales en el teléfono móvil de entidades desconocidas.

A nadie se le oculta la interferencia que estas actividades pueden tener en nuestra privacidad, y en particular en nuestro derecho a la intimidad. ¿Hasta qué punto los terceros pueden disponer de datos que nos afectan e indican cómo somos o nos comportamos? ¿Hasta qué punto las empresas y terceras

* Las opiniones expresadas en el presente trabajo son las del autor y vinculan exclusivamente a su autor. No representan necesariamente la posición oficial de la Comisión Europea.

personas pueden disponer y utilizar estos datos para el ejercicio de su actividad, sin que quede por ello afectado el derecho a nuestra privacidad? ¿Cómo organizar un sistema que permita conciliar los derechos de la persona con el derecho a realizar una actividad comercial o a disponer de información relativa a las personas con miras a la realización de una determinada actividad? ¿En qué condiciones estos datos se pueden recoger, procesar, utilizar? ¿De qué derechos dispone el ciudadano para hacer valer el respeto de su privacidad o de la veracidad de los datos recogidos?

Si todas estas cuestiones son de por sí importantes a nivel de un estado, la creación de la Unión Europea y del espacio sin fronteras interiores que conlleva ponen aún más de manifiesto la importancia que la protección de datos reviste para la Unión Europea.

Por ello no debe extrañar que la Unión Europea haya adoptado un marco jurídico para la protección de datos. Un marco jurídico que tiene por objeto garantizar la protección de los derechos fundamentales de la persona, y en especial el derecho a la privacidad, así como la libre circulación de los datos en ese espacio interior sin fronteras estatales. La libre circulación es un derecho fundamental en el sistema del Tratado de la Unión Europea sobre el que reposa la construcción y el establecimiento del mercado interior. La cuestión a la que la Unión ha tenido que hacer frente no es tanto la prohibición de la libre circulación de datos en el mercado interior, algo que de por sí no sería ni viable ni posible en la práctica, sino cómo garantizar el respeto de los derechos fundamentales de la persona en el caso del trato de datos personales.

II. EL MARCO JURIDICO DE LA PROTECCION DE DATOS EN LA UNION EUROPEA

¿Cuál es ese marco jurídico? En las líneas que siguen intentaré desarrollarlo y hacer hincapié en sus aspectos sustanciales.

1. ANTECEDENTES INTERNACIONALES

El marco jurídico del que se ha dotado la Unión Europea no es sin embargo un régimen innovador y original. Y ello porque la Unión Europea no ha sido el primer organismo internacional que abordó esta cuestión. Me gustaría citar las

“*guidelines*” de la OCDE de 1980 sobre la protección de datos personales y el flujo de datos personales a través de las fronteras. Estas “*guidelines*” siguen siendo un instrumento de referencia en los diferentes foros y diálogos internacionales en los que la cuestión de la protección de datos es evocada.

El primer texto vinculante, y en el que la Unión Europea se ha inspirado para el establecimiento de su marco normativo, es el **Convenio 108 del Consejo de Europa de 1981 sobre la protección de las personas con respecto al tratamiento automatizado de datos personales** El Convenio fija los principios básicos de la protección de datos que hoy rigen en los diferentes países europeos.

2. LA DIRECTIVA 95/46 SOBRE LA PROTECCION DE LAS PERSONAS FISICAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES Y A LA LIBRE CIRCULACIÓN DE ESTOS DATOS

El primer texto adoptado por la Unión Europea en materia de protección de datos es la Directiva 95/46 de 24 de octubre de 1995. Esta directiva constituye el pilar sobre el que se asienta la normativa comunitaria sobre protección de datos desarrollada a lo largo de estos últimos años. Posteriormente, **la Directiva sobre privacidad en las telecomunicaciones (2002/58/EC) y el Reglamento 2001/45/8EC que aplica la normativa europea a las propias instituciones comunitarias** han completado este régimen.

La protección de datos personales derecho fundamental de la persona en la UE

Es preciso indicar que la protección de datos personales ha adquirido en la actualidad el rango de derecho fundamental en la Unión Europea. La Carta de los Derechos Fundamentales de la Unión Europea contempla en su artículo 8 el derecho a la protección de datos personales en los términos siguientes :

"1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.

2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda

persona tiene derecho a acceder a los datos recogidos que la conciernan y a obtener su rectificación.

3. El respeto de estas normas estará sujeto al control de una autoridad independiente."

En este mismo orden de ideas, el proyecto de Tratado por el que se establece la Constitución Europea, prevé en su artículo I-51 refuerza el carácter de derecho fundamental de la protección de datos personales al extenderlo al conjunto de actividades comprendidas en el ámbito de aplicación del Derecho de la Unión.

Tampoco puedo dejar de referirme al Convenio para la Protección de los Derechos Humanos y Libertades Fundamentales del Consejo de Europa, cuyo artículo 8, relativo al derecho a la vida privada, ha servido al Tribunal de los Derechos Humanos del Consejo de Europa para abordar los temas relativos a la protección de datos personales. Los criterios que establece la jurisprudencia de este Tribunal para analizar la validez de las limitaciones y restricciones al derecho a la vida privada en lo que respecta a la protección de datos personales se han convertido en la pauta que aplican los organismos nacionales así como el propio Tribunal de Justicia de la Unión Europea.

La Directiva 95/46 retoma el tratamiento jurídico previsto en el Convenio 108 del Consejo de Europa y lo amplía a fin de establecer un nivel de protección elevado. La Directiva instituye un marco jurídico considerado el más avanzado del mundo en la materia.

Ambito de aplicación

La Directiva rige las operaciones de tratamiento de datos que se llevan a cabo en el territorio comunitario, con independencia del hecho de que tales operaciones sean puramente nacionales o por el contrario conlleven un aspecto de libre circulación entre los Estados miembros. El Tribunal de Justicia así lo ha confirmado en dos sentencias de 2003 al indicar que la aplicación de la Directiva no depende del hecho de si las operaciones de tratamiento de datos personales presentan un vínculo con las libertades de circulación garantizadas por el Tratado, sino de la necesidad de establecer un régimen jurídico apropiado para garantizar la protección de las personas y que suprima los obstáculos al funcionamiento del mercado interior que derivan de las diferencias entre las

legislaciones nacionales. La Directiva no se aplica sin embargo a las cooperaciones en el ámbito policial y judicial penal y de seguridad que forman parte del llamado Tercer Pilar de la Unión Europea. En estos supuestos, es la legislación de los Estados miembros sobre protección de datos personales la que resulta aplicable al tratamiento de los datos personales. A ello me referiré al final de esta comunicación.

Régimen de la Directiva

En sustancia, el régimen de protección de datos comunitario instaurado por la Directiva se articula alrededor de los siguientes principios:

a) **El tratamiento de los datos y los derechos de las personas interesadas**

i) calidad y exactitud de los datos objeto de tratamiento: los datos personales han de ser tratados de *manera leal y lícita*; recogidos con *finés determinados, explícitos y legítimos*, no han de ser tratados posteriormente de manera incompatible con dichos fines; han de ser datos *adecuados, pertinentes, exactos y no excesivos* con relación a los fines para los que se recaben y para los que se traten posteriormente, cuando sea necesario, deberán ser *actualizados; suprimidos o rectificadas* si fueran inexactos; por último han de ser *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. La Directiva prevé asimismo un *régimen de protección especial para los datos personales particularmente sensibles*, 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.

ii) principio del consentimiento del interesado: el tratamiento de datos personales **sólo** puede efectuarse si el interesado ha dado su *consentimiento de forma inequívoca*; aunque tal consentimiento no es preciso en determinados supuestos expresamente previstos por la Directiva; por ejemplo, cuando el tratamiento de tales datos es necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento. La Directiva permite también la ausencia de prestación del consentimiento del interesado cuando el

tratamiento de datos es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección. Se trata de un supuesto que la legislación española no contempla y que ha de ser tenido en cuenta para poder hablar de una correcta transposición. En todos estos supuestos la legitimidad para el tratamiento de datos personales se fundamenta en una disposición legal que reemplaza el consentimiento del interesado.

iii) derecho de información del interesado: el responsable del tratamiento de los datos personales ha de informar al interesado, al tiempo de recoger dichos datos, acerca de los elementos esenciales de esta operación, como son la identidad del responsable, de la existencia de un fichero en el que dichos datos serán incorporados, la finalidad de la recogida de estos datos, del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas y de las consecuencias eventuales que resultan de la negativa a suministrarlos, y sobre todo de la posibilidad del interesado de ejercitar los derechos de acceso, rectificación, cancelación y oposición. En el supuesto de que los datos no hayan sido recabados del interesado, éste deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o su representante, al tiempo de la incorporación de los datos personales al fichero, o, en el supuesto de que vayan a ser comunicados a un tercero, en el momento en que la primera comunicación se lleva a cabo.

iv) derechos de acceso, rectificación, cancelación y oposición del interesado y derecho a la reparación del perjuicio sufrido: estamos ante los derechos subjetivos esenciales que el interesado tiene para hacer valer la protección efectiva de sus datos personales. Estos derechos confieren al interesado, primero, la posibilidad de *acceder a sus datos personales* contenidos en un fichero y obtener información sobre la existencia o inexistencia del tratamiento de datos que le conciernen, la comunicación en forma inteligible, de los datos objeto de los tratamientos, así como toda la información disponible sobre el origen de los datos, de los fines de dichos tratamientos, las categorías de datos a que se refieran y los destinatarios o las categorías de destinatarios a quienes se comuniquen dichos datos. El derecho de acceso a los datos

personales es la base para el ejercicio por la persona interesada de los *derechos de rectificación, cancelación y oposición o bloqueo* de los datos personales cuyo tratamiento no es conforme a la normativa aplicable o cuando éstos sean inexactos o incompletos. Además toda rectificación, cancelación o bloqueo ha de notificarse a terceros a quienes se hayan comunicado los datos, salvo que resulta imposible o suponga un esfuerzo desproporcionado. De nuevo, toda excepción al ejercicio de estos derechos ha de ser predeterminada por la Ley en base a consideraciones de seguridad pública, defensa, la detección y la represión de infracciones penales o de las infracciones de la deontología en las profesiones reglamentadas o un interés económico y financiero importante de un Estado miembro o de la Unión Europea, incluidos los asuntos monetarios, presupuestarios y fiscales. La Directiva obliga a los Estados miembros a que introduzcan en su ordenamiento jurídico el derecho del interesado que sufra un perjuicio como consecuencia de un tratamiento ilícito a obtener del responsable del tratamiento la reparación del perjuicio sufrido.

b) El régimen de control de los ficheros y la creación de autoridades nacionales de control

La creación de un sistema jurídico de protección de datos que no contemple el establecimiento de un mecanismo destinado a velar por su cumplimiento y a garantizar la tutela de los derechos otorgados a los interesados contiene en sí mismo el riesgo fundamental de su inaplicación o funcionamiento incorrecto de modo que haría vanos los objetivos perseguidos con su creación. Por ello, la Directiva establece todo un mecanismo de control público de los ficheros destinado a garantizar su funcionamiento que pivota en torno a dos piezas esenciales.

i) la creación de autoridades nacionales de protección de datos personales

La Directiva exige a los Estados miembros la creación de autoridades públicas independientes encargadas del control de los ficheros de datos personales, vigilar la aplicación de la legislación nacional en materia de protección de datos y de garantizar la protección de los interesados. Estas autoridades han de estar dotadas de los poderes necesarios para cumplir su función, ya se trate de poderes de investigación o de intervención, en particular en los casos de reclamaciones presentadas a la autoridad o de poder comparecer en juicio. Estas autoridades son una pieza fundamental en el sistema establecido en la

Unión Europea, ya que están encargadas de tratar las reclamaciones de los interesados con respecto a protección de sus derechos y libertades respecto del tratamiento de datos personales. La Directiva impone a las autoridades de control una obligación de actuación, ya que deben atender tales reclamaciones e informar de la actuación llevada a cabo al respecto. Toda decisión adoptada por la autoridad nacional ha de ser susceptible de recurso ante los órganos jurisdiccionales competentes de acuerdo con el ordenamiento jurídico nacional. La Directiva organiza un *mecanismo de tutela efectiva* de los derechos otorgados al interesado para hacer valer la protección de sus datos personales. Se trata de una acción comunitaria original que impone a los Estados miembros una obligación de creación de un sistema específico destinado a garantizar el cumplimiento efectivo del régimen jurídico establecido. Me gustaría elogiar la labor ejemplar de la Agencia Española de Protección de Datos en su misión de hacer cumplir la legislación española, también en lo que atañe al régimen de transferencias internacionales de datos personales a países terceros.

La creación en 2001 de la Autoridad Europea de Protección de Datos por el Reglamento 45/2001, competente para garantizar la protección de los datos personales contenidos en ficheros de las instituciones comunitarias ha venido a completar el sistema europeo de protección de datos personales. El régimen aplicable al tratamiento de estos datos personales es el previsto en la Directiva 95/46.

ii) la notificación de los ficheros a la autoridad de protección de datos

Es evidente que si las autoridades nacionales son responsables del control de los ficheros, poder ejercer esta tarea han de tener conocimiento de la existencia de los mismos. Por ello, la Directiva 95/46/CE establece un régimen de notificación de los ficheros nacionales a la autoridad nacional de protección de datos previamente a su creación y puesta en práctica. La Directiva prevé, no obstante, ciertas derogaciones a esta obligación, y ello para evitar una carga burocrática excesiva o formalidades que pudieran ser desproporcionadas al fin perseguido. Es el caso, por ejemplo, de ficheros en el que el tratamiento de los datos personales no atenta contra los derechos y las libertades de los interesados, o en el supuesto de ficheros o registros públicos. Pero sobre todo, la exención de notificación es también posible en aquellos supuestos en que el

responsable del fichero designe *un encargado interno de protección de los datos personales* que tenga por cometido hacer aplicar, de manera independiente, las disposiciones nacionales relativas a la protección de datos personales y llevar un registro de los tratamientos efectuados por el responsable del tratamiento. Se trata de una figura inspirada en el derecho alemán.

La Comisión ha reconocido también en su informe de 2003 sobre la aplicación de la Directiva la conveniencia de simplificar el sistema de notificación haciendo para ello uso de las exenciones previstas en la Directiva. Desde nuestro punto de vista, es conveniente que los Estados Miembros se acojan a dicho precepto para eximir de la obligación de notificación ciertos ficheros que no atentan contra los derechos y las libertades de los interesados. También parece apropiado, como ya es el caso de muchos otros países Europeos, prever la posibilidad de designar un encargado de protección de los datos personales que tenga por cometido hacer aplicar, de manera independiente, las disposiciones nacionales relativas a la protección de datos personales y llevar un registro de los tratamientos efectuados por el responsable del tratamiento. Por lo tanto lo lógico sería que, antes de proceder a una modificación del texto de la Directiva las autoridades nacionales adoptaran pautas u recomendaciones interpretativas comunes al respecto. Este método es más rápido que el largo y complejo procedimiento legislativo comunitario. Y en la mayoría de los casos permite llegar a una solución satisfactoria. Se trata de un tema que forma parte del Programa de Trabajo en curso de la Comisión y del grupo de autoridades de protección de datos.

En su informe sobre la aplicación de la Directiva de 2003, la Comisión ha puesto de relieve, la existencia de divergencias nacionales en la transposición de la Directiva, las cuales son especialmente perjudiciales a los operadores económicos que actúan a nivel internacional. La Comisión es consciente que las estas divergencias en las legislaciones nacionales no siempre implican que haya una violación de la Directiva; se trata en muchos casos de una aplicación del margen de discreción que la Directiva deja a los Estados miembros a la hora de proceder a su transposición al derecho nacional. En otros casos, tales divergencias derivan de la manera en que la legislación nacional es aplicada en la práctica. Con el objeto de resolver estos problemas, la Comisión pidió a los

Estados Miembros que hicieran un esfuerzo en ajustar sus respectivas legislaciones nacionales al marco comunitario.

En ciertas ocasiones, la Directiva da un margen de interpretación que permite diferentes soluciones, todas ellas probablemente justificables en la Directiva. No obstante, no por ello dichas diferencias dejan de causar un obstáculo a los operadores económicos, además de crear un marco legal confuso para los ciudadanos. Por ello, la Comisión pidió a las autoridades nacionales, reunidas a través del Grupo de Trabajo de Autoridades Nacionales de Protección da Datos, conocido como el Grupo del Artículo 29, que adoptaran pautas u recomendaciones interpretativas comunes al respecto. Por lo tanto lo lógico sería que, antes de proceder a una modificación del texto de la Directiva las autoridades nacionales adoptaran pautas u recomendaciones interpretativas comunes al respecto. Este método es más rápido que el largo y complejo procedimiento legislativo comunitario. Y en la mayoría de los casos permite llegar a una solución satisfactoria. Se trata de un tema que forma parte del Programa de Trabajo en curso de la Comisión y del grupo de autoridades de protección de datos.

Acabo de referirme al Grupo del Artículo 29. Ahora bien, ¿qué es exactamente el Grupo de Trabajo del Artículo 29?

III LA APLICACIÓN DE LA DIRECTIVA LOS MÉTODOS PARA GARANTIZAR SU APLICACIÓN EFECTIVA Y COHERENTE. EL GRUPO DE TRABAJO DE AUTORIDADES NACIONALES DE PROTECCIÓN DA DATOS (GRUPO “ARTÍCULO 29”)

Una Directiva es un instrumento del ordenamiento jurídico comunitario que impone a los Estados miembros una obligación de resultado. En nuestro caso esta obligación es doble, por un lado, establecer un sistema jurídico nacional que transcriba y responda a los principios estipulados en la Directiva; por otro, hacer que las autoridades nacionales de control (Agencias de Protección de Datos) apliquen este sistema, aseguren su cumplimiento y contribuyan a la tutela y garantía del derecho fundamental de la protección de los datos personales. Además una Directiva implica una aplicación convergente por parte de las autoridades nacionales para garantizar la eficacia del sistema establecido

y evitar la aparición de fallas en el mismo. A tal fin, la colaboración entre las autoridades nacionales es imprescindible.

Con este motivo, la Directiva crea un Grupo de Trabajo constituido por las autoridades nacionales encargadas de la protección de datos personales, la autoridad Europea de protección de datos y representantes de la Comisión. Se trata del llamado Grupo de Trabajo del Artículo 29, en referencia a la disposición de la Directiva 95/46 que lo establece.

El cometido del Grupo de Trabajo del Artículo 29 es vario. No sólo procede a examinar las cuestiones relativas a la aplicación de la directiva en los Estados miembros, con miras a facilitar una interpretación y aplicación convergentes. También informa acerca de cuestiones cruciales para el funcionamiento del sistema de la Directiva. Por ejemplo, emite dictámenes acerca de la adecuación de las legislaciones de países terceros con miras a permitir la exportación de ficheros, o informa a la Comisión sobre los proyectos de modificación de la Directiva o sobre toda otra cuestión relativa a la protección de datos personales en la Comunidad.

El Grupo de Trabajo del Artículo 29 lleva a cabo una tarea inestimable ya que, debido a la independencia de sus autoridades y del conocimiento de los problemas que plantea la protección de datos en la práctica cotidiana, contribuye a una visión coherente y actualizada de la protección de datos en la Comunidad y sus informes y recomendaciones son altamente estimados. Aunque se trata de un grupo de carácter consultivo, sus resoluciones e informes gozan de una gran autoridad. Mediante sus interpretaciones, el Grupo contribuye a una aplicación dinámica y actualizada del sistema de la Directiva para tomar en consideración las evoluciones tecnológicas que se han producido desde la adopción de la Directiva en 1995, como es el caso de internet o de los correos electrónicos.

Junto a este Grupo de Trabajo, la Directiva ha creado también un Comité (Comité del Artículo 31) compuesto por representantes de los Estados miembros, en general de los Ministerios de Justicia, y que asiste a la Comisión en el desarrollo de los poderes de ejecución otorgados por la Directiva. Se trata de uno de los muchos Comités creados para asistir a la Comisión y cuyo funcionamiento está regulado por la Decisión del Consejo 1999/468/EC. Este Comité ha asistido por ejemplo en la adopción de las decisiones relativas al

reconocimiento de la adecuación de los regímenes de protección de datos de los países terceros.

IV. LA DIMENSION EXTERIOR DEL MERCADO INTERIOR. LA PROBLEMÁTICA DE LA TRANSFERENCIA DE DATOS A PAÍSES TERCEROS.

Nadie ignora que un sistema jurídico destinado a regular las operaciones llevadas a cabo en el territorio en el que está vigente puede convertirse en papel mojado y dar al traste con las finalidades pretendidas si no se prevén mecanismos específicos que contemplen las relaciones de ese sistema con otros sistemas vigentes en otros países. Las diferencias entre el sistema implantado por la Directiva en la Comunidad y aquéllos vigentes en países terceros conllevan el riesgo evidente de que el nivel de protección garantizado en la Comunidad se pierda con la transferencia de esos datos a los países terceros con un nivel de protección inferior o incluso inexistente. Pero tampoco es posible que, en aras del buen funcionamiento de este régimen, la Comunidad se “aísle” e impida toda relación con los países terceros. La Unión Europea es un actor de primer orden en el desarrollo de las transacciones comerciales internacionales, el flujo de transacciones comerciales de empresas europeas con países terceros o de empresas multinacionales con establecimientos en el territorio comunitario es impresionante. Por lo tanto la reglamentación comunitaria ha tenido que abordar la cuestión de las transferencias a países terceros de datos personales tratados en el territorio comunitario.

La Directiva 95/46 estipula que la transferencia a un país tercero de datos personales que sean objeto de tratamiento únicamente puede efectuarse cuando el país tercero garantice un nivel de protección adecuado. En caso contrario las autoridades nacionales no autorizarán esta transferencia. La dificultad reside en la determinación del nivel de adecuación presentado por el sistema de países terceros. Esto ha dado lugar a innumerables y largas discusiones entre las autoridades de control nacionales y la Comisión. Hasta la fecha la Comisión ha adoptado varias decisiones reconociendo la adecuación de los sistemas vigentes en Argentina, Canadá, Suiza, o la Islas de Man y Guernesey, o el sistema de Puerto Seguro de los Estados Unidos (Safe Harbor).

El rigor de la prohibición de transferencias queda en cierta medida dulcificado por las posibilidades que reconoce la propia Directiva (art. 26) para proceder a esta exportación de datos personales a países que no garanticen un nivel de protección adecuado. De manera esquemática, esta transferencia puede efectuarse cuando el interesado haya dado su consentimiento inequívoco a la misma; cuando la transferencia sea necesaria en relación con un contrato entre el interesado y el responsable del fichero; cuando así lo exija la protección de un interés público importante, por ejemplo en casos de transferencia internacional de datos entre las administraciones fiscales o aduaneras o entre los servicios competentes en materia de seguridad social. También es posible exportar datos personales cuando el responsable del tratamiento en la Comunidad ofrezca garantías suficientes respecto de la protección de la vida privada, de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los respectivos derechos. Estas garantías podrán derivarse, en particular, de cláusulas contractuales apropiadas incluidas en los acuerdos de transferencia de datos. A este respecto la Comisión ha aprobado en 2001 y 2002 sendas Decisiones sobre las cláusulas contractuales tipo para la transferencia de datos personales a un país tercero. Estas cláusulas tipo constituyen un medio que permite la exportación de datos a países que no ofrecen el nivel de protección adecuado. Han de ser incorporadas en el contrato de transferencia de datos negociado entre el responsable exportador comunitario y el importador del país tercero. Las mismas reconocen una serie de derechos a las personas interesadas cuyos datos son exportados para garantizar el respeto de sus derechos en especial cuando el incumplimiento de tales cláusulas tipo conlleva un perjuicio para estas personas.

En el contexto de transferencias de datos internacionales, la Comisión ve positivamente el uso relativamente nuevo de códigos de conducta a los fines de transferir datos personales entre las diferentes filiales de una determinada empresa multinacional. Dichos códigos, al igual que las cláusulas contractuales, deberán reconocer una serie de derechos a las personas interesadas cuyos datos son exportados para garantizar el respeto de sus derechos.

La Unión Europea trata de llevar a cabo una política consistente en “exportar” nuestro sistema a fin de aproximar en la medida de lo posible los ordenamientos de nuestros mayores socios comerciales y conseguir un nivel de protección

adecuado en el tratamiento de los datos personales. La Comisión reconoce el papel fundamental que ejerce la Agencia Española de Protección de datos de cara a ayudar a los países de Latinoamérica a dotarse de legislaciones de protección de datos que sigan el modelo Europeo.

V. LA PROTECCION DE DATOS EN LOS AMBITOS DEL ESPACIO SCHENGEN Y DE LA COOPERACION JUDICIAL PENAL Y POLICIAL EN EL SENO DE LA UNION

Como he indicado anteriormente el régimen de protección de datos establecido por la Directiva 95/46/CE no se aplica a las materias que forman parte del llamado “tercer pilar” de la Unión Europea, esto es las cuestiones relativas a la política de seguridad y a la cooperación en los ámbitos judicial penal y policial. Se trata de algo comprensible en la medida que estas políticas no se hallan aún “comunitarizadas”, esto es sometidas a las disposiciones del Tratado de la Comunidad Europea de 1957 que prevé la creación de un mercado interior fundamentado en la libre circulación de bienes, personas y capitales. Los aspectos relativos a las cuestiones de política de seguridad y a la cooperación en los ámbitos judicial penal y policial se hallan sometidas al Tratado de la Unión Europea, en vigor desde 1993. Este Tratado incorpora una serie de políticas nuevas al ámbito de la construcción europea con el objeto de proceder a una mejor cooperación entre las autoridades nacionales y crear un espacio de libertad, seguridad y justicia.

A esto hay que añadir la situación vigente dentro del llamado espacio "Schengen" para la realización de la libre circulación de personas dentro del territorio de los Estados que forman parte de este “espacio”.

La protección de datos en estos ámbitos se lleva a cabo de acuerdo con disposiciones diferentes, lo que nos sitúa ante reglamentaciones específicas adoptadas al momento de desarrollar estas políticas. Esto ha dado lugar a una dispersión de normas y principios en esta materia, lo que no contribuye necesariamente a la claridad jurídica ni a su conocimiento.

a) El espacio Schengen

La política de realización de un espacio en el que sea efectiva la libre circulación de las personas se ha desarrollado a partir de los llamados Acuerdos de Schengen de 1985 y 1990. Estos acuerdos se desarrollaron fuera del marco comunitario y dentro de las primeras políticas de cooperación judicial y policial. Posteriormente, con el Tratado de Ámsterdam en 1997, que modifica los Tratados de la CE y de la Unión Europea, el conjunto de actos adoptados dentro de este marco se integró en 1 de Mayo de 1999 dentro del acervo comunitario para constituir Derecho comunitario en el sentido estricto del término.

Por lo que a la protección de datos se refiere, el Tratado de Schengen contiene una serie de disposiciones en sus Títulos IV y VI. La introducción de estas disposiciones era necesaria para tener en cuenta la creación del Sistema de Información Schengen (SIS) [Art. 92-119]. El SIS es un sistema de información conjunto compuesto de una sistema central y de secciones nacionales que los alimentan y mantienen actualizado. El SIS contiene datos personales relativos a determinadas categorías de personas, como por ejemplo personas bajo mandato de búsqueda para extradición, nacionales de países terceros con miras a rechazar su entrada en el espacio Schengen, o personas desaparecidas.

Los datos personales introducidos en el SIS sólo pueden ser utilizados para los fines especificados en el Tratado de Schengen y dentro del marco de la cooperación judicial y policial.

El Tratado de Schengen establece un sistema dual para el control del cumplimiento de las disposiciones en materia de protección de datos personales. Por un lado, las autoridades nacionales designadas por los Estados participantes, son responsables del control y del cumplimiento por las secciones nacionales del SIS de la normativa nacional aplicable al tratamiento de esos datos personales. Por otro lado, una autoridad conjunta de supervisión es responsable del control del soporte técnico establecido en Estrasburgo.

El derecho de acceso del interesado a los datos contenidos en SIS son ejercitados de conformidad con la normativa en vigor en el Estado ante la que se alega. No se facilitará información a la persona de que se trate si dicha información pudiera ser perjudicial para la ejecución de la tarea legal consignada

en la descripción o para la protección de los derechos y libertades de terceros. Asimismo, toda persona tiene derecho a exigir la rectificación o la supresión de aquellos datos erróneos. También se reconoce a toda persona el derecho a emprender acciones en el territorio de cada Estado parte del sistema ante el órgano jurisdiccional o la autoridad competente en virtud del Derecho nacional, en particular a efectos de rectificación, supresión, información o indemnización motivadas por una descripción que se refiera a ella.

El 31 de mayo de 2005 la Comisión acaba de presentar un paquete de medidas relativas al establecimiento de una segunda generación del sistema de Información de Schengen (SIS-II). Una vez adoptad por el Consejo y el Parlamento, este sistema reemplazará al sistema vigente. La propuesta de reglamento presentada trata de alinear el marco jurídico del SIS con el Derecho comunitario, esto es la Directiva 95/46. Se trata de un acto basado en el artículo 62(2) y 66 del Tratado CE, con lo que el sistema queda plenamente integrado en el acervo comunitario. Por lo que respecta a la protección de los datos personales registrados y objeto de tratamiento por SIS II, la propuesta de reglamento establece que el tratamiento de los datos personales se llevará a cabo de acuerdo con las disposiciones de la Directiva 95/46/CE. Igualmente los derechos de acceso, rectificación o supresión se ejercerán de acuerdo con las disposiciones de la Directiva 95/46/CE. De este modo, el régimen de la directiva pasa de modo claro e indubitable a regir las operaciones de tratamiento de datos personales a las cuales se aplica el Reglamento. Asimismo queda claro que las autoridades nacionales competentes para el control de la legalidad de las operaciones llevadas a cabo serán las autoridades de protección de datos creadas en virtud de la Directiva 95/46/CE, por lo que respecta a las cuestiones de las secciones nacionales, mientras que la Autoridad Europea de Protección de Datos será encargada de velar por las actividades de tratamiento de datos por la Comisión llevadas a cabo de acuerdo con el reglamento.

b) La protección de datos en el ámbito de la cooperación policial. El Convenio sobre EUROPOL

Este Convenio de 1995 se basa en el artículo 31 del Tratado de la Unión Europea y establece un mecanismo de intercambio de información y de análisis entre las autoridades de los Estados miembros por lo que respecta a una serie

de actividades y delitos relacionados con el tráfico de drogas, la inmigración ilegal, tráfico de vehículos y seres humanos, o falsificación de monedas y otros medios de pago.

Por lo que ahora nos interesa, el Convenio EUROPOL contiene sus propias disposiciones relativas al tratamiento de los datos personales. El sistema creado se inspira en el sistema del Tratado de Schengen. Los Estados miembros vienen obligados a designar una autoridad nacional de control cuya tarea consistirá en vigilar, de manera independiente y con arreglo a la legislación nacional, la licitud de la introducción y la consulta de datos y de la transmisión en cualquier forma de datos personales a Europol por parte del Estado miembro de que se trate, y en garantizar que no se vulneren los derechos de las personas. Asimismo se crea una autoridad común de control independiente cuyo cometido será vigilar la actividad de Europol, con arreglo a lo dispuesto en el presente Convenio, con el objeto de garantizar que el almacenamiento, el tratamiento y la utilización de los datos de que dispongan los servicios de Europol no vulneren los derechos de las personas.

En cuanto al régimen jurídico aplicable, puesto que la Directiva 95/46/CE no es de aplicación, el Convenio estipula que el tratamiento de datos personales se llevará de acuerdo con las disposiciones nacionales que los Estados miembros adopten, aunque en todo caso han de proporcionar al menos un nivel de protección de los datos semejante al previsto en el Convenio 108 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 encaminada a regular la utilización de datos de carácter personal en el sector de la policía.

c) La Cooperación judicial en el ámbito penal (EUROJUST)

Al igual que sucede con EUROPOL, la cooperación en el ámbito judicial es fruto del desarrollo de las políticas de colaboración adoptadas en el marco del tercer pilar de la Unión Europea. La Decisión del Consejo de 28 de febrero de 2002 crea Eurojust con el objeto de reforzar la lucha contra las formas graves de delincuencia.

Como en el caso de Europol, Eurojust permite el intercambio de informaciones entre las autoridades competentes de los Estados miembros con Eurojust.

Por lo que respecta al tratamiento de datos personales que pudieran recogerse, la Decisión de febrero de 2002 estipula que Eurojust adoptará las medidas necesarias para garantizar un nivel de protección de los datos personales equivalente al menos al que se deriva de la aplicación de los principios del Convenio 108 del Consejo de Europa de 28 de enero de 1981 y sus modificaciones posteriores que estén vigentes entre los Estados miembros. El derecho de acceso a los datos personales almacenados por Eurojust se ejercerá por la persona interesada en el Estado miembro que desee que consulta sin demora a Eurojust. Es el derecho de este Estado miembro el que regirá las condiciones y el procedimiento aplicable para el ejercicio de este derecho así como los derechos de rectificación y supresión de los datos personales. El reglamento interno adoptado el 24 de febrero de 2005 (DO C 68 de 19.3.2005) desarrolla la normativa relativa al tratamiento y a la protección de los datos personales de acuerdo con los principios del Convenio 108 del Consejo de Europa y de la Directiva 95/46/CE.

Eurojust dispone de un responsable de la protección de datos, miembro del personal designado específicamente para esta tarea. Este responsable "interno" supervisa las operaciones diarias de Eurojust, para garantizar la legalidad y el cumplimiento de la Decisión de 2002 y que las personas que solicitan información acerca de sus datos sean informadas de los derechos que les asisten.

Por último, Eurojust dispone también de una Autoridad Común de Control, independiente, encargada de velar por el cumplimiento de las disposiciones de la Decisión relativas al tratamiento de datos personales. Esta autoridad es competente para examinar los recursos presentados por las personas que no han quedado satisfechas con las respuestas o actuaciones de Eurojust en respuesta a las acciones entabladas con miras a ejercer su derecho de información o de rectificación o supresión.

La situación existente en los ámbitos de la cooperación penal y policial, reposa como hemos podido ver, en sistemas diferentes de los establecidos en el primer pilar de modo que no es posible hablar aún de un sistema armonizado de la

protección de los datos personales en el tercer pilar. La Comisión tiene la intención de presentar propuestas legislativas en la materia, que tengan en cuenta la naturaleza especialmente sensible de los temas abordados en estos sectores.

Aunque la Directiva no se aplica directamente a todas estas materias, sus principios sí son aplicados de manera indirecta, en la medida que las legislaciones nacionales de protección de datos aplican los principios de la Directiva y en que los mecanismos previstos en estos sectores reposan sobre el Convenio 108 del Consejo de Europa, Convenio que como vimos anteriormente inspira también la Directiva. Por lo tanto podríamos hablar de una aplicación indirecta por las autoridades nacionales.

CONCLUSION

Desde sus primeros balbucesos normativos hasta hoy en día, la protección de datos personales ha ido progresando de manera paulatina hasta obtener el rango de derecho fundamental de la persona. Aunque sigue siendo un derecho desconocido para la mayoría de los ciudadanos. El régimen jurídico creado en la Unión Europea es un régimen progresista que concilia las exigencias propias de las actividades comerciales con las derivadas de la tutela efectiva de este derecho fundamental. Sistema que para atender a las evoluciones constantes de nuestra sociedad ha de ser interpretado y aplicado de manera dinámica y evolutiva. Sobre las autoridades nacionales de protección de datos reposa esta responsabilidad así como la de fomentar el conocimiento de este derecho y suscitar la toma de conciencia por los ciudadanos.

Una de las cuestiones fundamentales que tenemos que abordar en los próximos años es asegurar una mejor aplicación práctica en todos los Estados miembros y con base a principios y pautas comunes.

Otra cuestión a la que hay que prestar atención es la posible modificación de la Directiva vigente. El informe de la Comisión de 2003 señala algunos temas susceptibles de simplificación o modernización, que figuran en el Programa de Trabajo del Grupo del Artículo 29, como son la simplificación del régimen de notificación de ficheros a las autoridades nacionales, garantizar una aplicación más efectiva de la Directiva por las autoridades nacionales o profundizar en los temas relativos a la exportación de datos a países terceros. Aunque no parece que sea necesario proceder a una modificación legislativa, tampoco es preciso descartarla.

Por último no tendremos que descartar el desafío que plantea la integración de la protección de datos en toda la política de la Unión, en particular en las políticas de cooperación judicial penal y policial del llamado tercer pilar, que escapan al ámbito de aplicación de la Directiva para quedar sometidas a un régimen específico que se inspira directamente del Convenio 108 del Consejo de Europa. A medida que la cooperación judicial penal y policial se desarrollan y mantienen relaciones más estrechas con las políticas del llamado primer pilar de libre circulación de personas, se hace más evidente la necesidad de adoptar un régimen coherente para el conjunto de las políticas de la Unión. A este respecto

he de referirme a la *propuesta de Decisión Marco*, presentada por la Comisión el 5 de Octubre, relativa al *régimen aplicable a la protección de los datos personales en el marco de la cooperación policial y judicial en materia penal entre los Estados miembros (el llamado tercer pilar)*. Este instrumento una vez adoptado colmará el vacío legislativo existente a nivel de la Unión Europea. Su objetivo es la fijación de un régimen jurídico armonizado destinado a garantizar la protección de las personas físicas por lo que respecta al tratamiento de datos personales dentro de estos ámbitos de cooperación policial y judicial en materia penal, de manera que la transmisión de estos datos personales entre las autoridades de los Estados miembros no quede limitada o prohibida por consideraciones vinculadas a la protección de datos personales.

En este contexto debo también referirme a las disposiciones recientemente propuestas por la Comisión para facilitar la cooperación entre las autoridades nacionales en la lucha contra el terrorismo y la criminalidad organizada (*Propuesta de Directiva relativa a la conservación de datos tratados en relación con la prestación de servicios públicos de comunicación electrónica y la Propuesta de Decisión Marco relativa al intercambio de informaciones en virtud del principio de disponibilidad*). Estos instrumentos prevén acciones que en sí mismas conllevan una invasión de la esfera de la privacidad de los datos personales. Por ello es necesario que, en tanto que limitación de un derecho fundamental, los mismos respondan a los criterios de necesidad y proporcionalidad para salvaguardar un interés legítimo, como es la seguridad pública. Además han de fijar de manera estricta los objetivos, condiciones y modalidades en que tales intervenciones se van a llevar a cabo y han de establecer las garantías adecuadas para salvaguardar la tutela y protección de los derechos de los ciudadanos. Se trata en suma de responder a la siempre difícil y vieja cuestión de mantener el adecuado equilibrio entre la libertad y la seguridad.