Revista de Estudios Europeos
n. 69, enero-junio, 2017, 17-36
ISSN: 2530-9854. http://www.ree-uva.es/

LA PROTECCIÓN DE DATOS PERSONALES EN EL ESPACIO DE LIBERTAD, SEGURIDAD Y JUSTICIA. ESPECIAL CONSIDERACIÓN A LAS TRANSFERENCIAS DE DATOS A TERCEROS PAÍSES Y ORGANIZACIONES INTERNACIONALES SEGÚN LA DIRECTIVA 2016/680.

THE PROTECTION OF PERSONAL DATA IN THE AREA OF FREEDOM, SECURITY AND JUSTICE.SPECIAL CONSIDERATION OF DATA TRANSFERS TO THIRD COUNTRIES AND INTERNATIONAL ORGANIZATIONS ACCORDING TO DIRECTIVE 2016/680.

Mª Belén SÁNCHEZ DOMINGO[1]
Universidad Rey Juan Carlos

Resumen: La necesidad de intercambio de datos personales para combatir la lucha contra el crimen organizado exige una mayor cooperación por parte de las autoridades judiciales y policiales de los Estados miembros de la Unión. En materia de protección de datos personales, la Unión considera necesario contar con un régimen específico en materia de protección y tratamiento de datos equivalente en todos los Estados miembros para lograr que la cooperación judicial y policial sea eficaz. A ello responde la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales[2], y a la libre circulación de dichos datos[3], de reciente aprobación. Este nuevo instrumento jurídico incluye normas comunes para el intercambio de información entre los Estados miembros UE y terceros países y organizaciones internacionales, tratando de facilitar la cooperación transfronteriza de las autoridades competentes en el ejercicio de funciones de investigación y prevención, con la finalidad de combatir más eficazmente el crimen y el terrorismo en toda Europa, estableciendo los requisitos necesarios para que la transferencia de datos a terceros países u organizaciones internacionales pueda realizarse respetando, a su vez, los principios reguladores que regulan dicha transmisión.

Summary: The necessity of interchange of personal data to fight against the war organized crime requires greater cooperation on the part of the judicial and police authorities of the Member States of the Union. Regarding the protection of personal data, the Union considers necessary to have a specific system for the protection and processing of equivalent data in all Member States to ensure that judicial and police cooperation is effective. To this responds the Directive 2016/680 of the European Parliament and of the Council relative to the protection of individuals with regard to the processing of personal data by competent authorities for the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, and to the free movement of such data, which was recently approved. This new legal instrument includes common rules for the exchange of information between EU Member States and third countries and international organizations, seeking to facilitate cross-border cooperation of the competent authorities in the exercise of research and prevention functions in order to combat more crime and terrorism throughout Europe by establishing the necessary requirements for the transfer of data to third countries or international organizations can be carried out while respecting the regulatory principles governing such transmission.

Palabras clave: Tratado de Lisboa, Derechos Fundamentales, protección de datos, autodeterminación informativa, intimidad, transferencia de datos.

Key words: Treated about Lisbon, Fundamental Laws, protection data of information, informative self-determination, intimacy, transfer of information.

---

1 Profesora Contratada Doctora en Derecho Penal. Acreditada a Profesora Titular de Derecho Penal. URJC.
El presente trabajo se enmarca dentro del proyecto de investigación: «Un paso más en la consolidación del espacio judicial europeo y su aplicación práctica en España: visión desde el proceso civil y penal", (DER2015-71418-P), financiado por el Ministerio de Economía y Competitividad para el trienio 2016-2018, de que formo parte como investigadora.

2 DO L 119/89 de 4 de Mayo de 2016.

3 Y que sustituye a la DM 2008/977/JAI del Consejo, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal (DO L 350 de 30.12.2008)

El Tratado de Lisboa y la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo. 3.4. Transferencias de datos a terceros países y organizaciones internacionales. 4. Reflexión final.

1. Introducción.

En la sociedad tecnológica de hoy en día, las tecnologías de la información y la comunicación incrementan la velocidad de tratamiento de la información, así como la capacidad de almacenamiento y la de transmisión de datos. En este contexto, la amenaza que las nuevas tecnologías constituyen para los ciudadanos y los derechos que le son inmanentes exige respuestas que hagan frente a estos desafíos. A nadie sorprende que la sociedad actual, en su constante evolución haya aceptado, en cierta forma, una flexibilidad referida a ciertas informaciones cuya finalidad no es otra que la de conocer aspectos referentes a la vida privada de la persona[4].

El impacto que el uso de la informática pueda tener a través de las TiC's, influye en el contenido de ciertos derechos fundamentales[5]. Así, en este contexto, precisamente el derecho a la protección de datos personales y la vida privada de la persona -intimidad-, son derechos que están sometidos a crecientes desafíos que hoy en día plantean las tecnologías de las comunicaciones globales. Actualmente, las redes informáticas son la principal vía de difusión de datos personales. Por ello, el imparable desarrollo social y, en concreto, el avance de la sociedad de la información conlleva la exigencia de respuestas jurídicas precisas, adaptadas a los nuevos fenómenos sociales que ocasiona el uso de las tecnologías de la información y de la comunicación[6].

Para hacer frente a estos nuevos desafíos, está plenamente justificado que la Unión Europea adopte medidas destinadas a obstaculizar este tipo de comportamientos, medidas que comportan la elaboración de instrumentos jurídicos que comprometan el establecimiento de garantías firmes y equivalentes en todos los Estados miembros[7] garantizando, a su vez, el pleno respeto del derecho fundamental a la protección de datos personales[8]. Asimismo, se exige una mayor cooperación por parte de las autoridades judiciales y policiales en la aplicación y cumplimiento de las leyes sobre protección de datos personales. Fueron los atentados terroristas de 2001 los que pusieron de manifiesto la necesidad de intercambiar -en el marco de la cooperación judicial y policial en la lucha contra el terrorismo-, ciertas informaciones relativas a datos personales de determinados individuos. Posteriormente, los

4 Sobre las nuevas tecnologías y protección de datos existe una dilatada literatura, así, entre otros, nos remitimos: Bru Cuadrada, E. (2007): "La protección de datos en España y en la Unión Europea. Especial referencia a los mecanismos jurídicos de reacción frente a la vulneración del derecho a la intimidad", Revista de Internet, Derecho y Política, nº 5, pp. 1 y ss.; Galán Muñoz, A. (2004): "¿Nuevos riesgos, viejas respuestas? Estudio sobre la protección de los datos de carácter personal ante las nuevas tecnologías de la información y la comunicación", Revista General de Derecho penal, 19, 2013, pp. 1 y ss.; Libro Colectivo: Derecho a la intimidad y nuevas tecnologías, Gómez Martínez, C., (Dir.), CGPJ, Centro de Documentación Judicial; Martínez Martínez, R. (2004): Una aproximación crítica a la autodeterminación informativa, Thomson-Civitas, pp. 23-57; Téllez Aguilera, A. (2001): Nuevas tecnologías. Intimidad y Protección de datos. Estudio sistemático de la Ley Orgánica 15/1999, Edisofer, S.L., pp. 21 y ss.; Por parte de la literatura italiana, también existe una espaciada bibliografía en relación a la riservatezza y nuevas tecnologías. Vid. entre otros, Fabio di Resta, (2000): Protezione delle informazione, Privacy e sicurezza, G. Giappichelli Edotpre, Torino, pp. 3 y ss.; Mucciarelli, F. (2004): "Informatica e tutela penale della riservatezza", Il diritto penale dell'informatica nell' época di Internet, a cura di L. Picotti, Padova, pp. 173-181.

5 Vid. Frigols i Brines, E. (2010): "La protección constitucional de los datos de las comunicaciones y del derecho a la intimidad a la luz del uso de las nuevas tecnologías", *La protección jurídica de la intimidad*, Boix Reig, J. (Dir.)/Jareño Real, A. (Coord.), Iustel, pp. 37 y ss.; López Ortega, J.J. (2004): "Intimidad informática y Derecho Penal. (La protección penal de la intimidad frente a las nuevas tecnologías de la información y comunicación)", *Derecho a la intimidad y nuevas tecnologías*, Cuadernos de Derecho Judicial, IX, pp. 109-142 (esp. pp. 109-115); Morant Vidal, J. (2003): *Protección penal de la intimidad frente a las nuevas tecnologías (estudio de los artículos 197 a 201 del Código Penal)*, Tirant Lo Blanch; En la literatura italiana, vid. Gordini, G., (2006): "Societá dell?informazione e diritti Constituzionali", *La Societá dell'informazione: libertá, pluralismo, risorce*, A cura di G. Gindi, Torino, pp. 67 y ss.

6 Sobre las relaciones entre informática y delitos informáticos, Vid. Picotti, L. (2004): "Sistematica dei reati informática, tecniche di formulazione legislativa e beni giuridice tutelati, *Il diritto penale dell'informaticaa nell'epoca di Internet,* a cura di L. Picotti, Padova, pp. 21-94; De la Cuesta Arzamendi, J.L. (Dir.). De la Mata Barranco, N., (Coord.), (2010): *Derecho Penal informático*, Ed. Aranzadi; Fernández Teruelo, J.G. (2007): *El Cibercrimen. Los delitos cometidos a través de internet*, Dykinson,

7 Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, "Un enfoque global sobre la protección de los datos personales en la Unión Europea", COM (2010) 609 final, Bruselas 4.11.2012.

8 También denominado derecho de autodeterminación informativa. Para una exposición más amplia sobre el derecho a la autodeterminación informativa en nuestra doctrina, vid. Guichot, E. (2005): *Datos personales y Administración Pública*, Thomson-Civitas, pp. 61 y ss.; Murillo De La Cueva, P.L. (2007): "Perspectivas del derecho a la autodeterminación informativa", *Revista de Internet, Derecho y Política*, nº 5, pp. 18-32 (esp. pp. 19-22); Murillo De La Cueva, P.L./Piñar Mañas, J.L. (2009): *El derecho a la autodeterminación informativa*, Fundación Coloquio Jurídico Europeo, Madrid; Martínez Martínez, R. (2004): *Una aproximación crítica…*, op. cit. pp. 323 y ss;

atentados terroristas de Bruselas de 22 de marzo de 2016 así como el de Niza de 14 de julio de 2016, han obligado a la UE a adoptar medidas legislativas que conduzcan a una actuación eficaz en el intercambio de información entre las distintas autoridades nacionales e internacionales y conseguir, a su vez, una mejora en la operatividad de las bases de datos y los sistemas de información[9]. A ello responde la Directiva del 27 de Abril, de 2016 del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos. La Directiva en cuestión procede, por una parte, a proteger los derechos y libertades fundamentales, en particular el derecho a la protección de los datos personales y, por otra parte, a garantizar un alto nivel de seguridad pública, asegurando el intercambio de datos personales entre las autoridades competentes dentro de la Unión.

El objetivo que se pretende con este trabajo es analizar el régimen legal de las transmisiones de datos personales a terceros países o instituciones internacionales. Dado que el marco normativo actual aplicable a la protección de datos personales es el resultado de un proceso evolutivo llevado a cabo por el Consejo de Europea y la Unión Europea, se ha considerado de interés en el desarrollo del trabajo aludir a la evolución normativa desarrollada por la Unión Europea en el establecimiento de un marco jurídico de protección eficaz de datos personales respetuosa a la vez con la libre circulación de dichos datos, por lo cual se analizarán los distintos instrumentos elaborados en el ámbito de la Unión Europea, aludiendo de manera específica a las disposiciones relacionadas con dicho régimen así como a los principios básicos inspiradores de las transferencias de datos.

En el desarrollo de esta exposición, se aludirá a las condiciones específicas exigibles para que la transferencia internacional de datos personales en materia de prevención y sanción penal se realice con el máximo respeto al conjunto de garantías que deben ser observadas en el tratamiento de datos personales, con mención expresa al requisito imprescindible para realizar el intercambio de datos personales del "nivel adecuado de protección". Es preceptivo proceder a realizar una interpretación de dicho requisito determinando los parámetros concretos exigibles que permitan la transmisión de los datos personales.

En el marco de la cooperación judicial y policial, el intercambio de datos personales se considera necesario para hacer frente al fenómeno de la criminalidad organizada y conseguir una mayor eficacia en su lucha, pero sin que en ningún caso pueda suponer una restricción de los derechos y libertades del titular de los datos. Las injerencias en el derecho fundamental a la protección de datos personales son legítimas siempre que estén permitidas por ley y se respete el núcleo del derecho fundamental a la protección de datos personales. La utilización e intercambio de datos personales por parte de las autoridades competentes en el marco de una investigación criminal o por razones de prevención y seguridad pública, los requisitos bajo los cuales se permite dicha transferencia puede ocasionar una disminución de los niveles de protección del derecho a la protección de datos personales con la consiguiente merma de las garantías que conforman el núcleo de dicho derecho. Son supuestos en los que se puede llegar a producir una colisión de derechos en la cesión de datos de carácter personal protegido como derecho fundamental, lo que requiere una ponderación de los bienes jurídicos enfrentados con el objetivo de lograr el necesario equilibrio entre la protección del derecho fundamental a la protección de datos y el refuerzo de la seguridad, esto es, el mantenimiento del equilibrio entre el binomio libertad-seguridad. Por ello, es necesario abordar el contenido de las disposiciones relativas al tratamiento de datos personales con expresa alusión a los principios que regulan dicho tratamiento así como a las restricciones y limitaciones previstas, especificando si de la actual regulación se desprende una interpretación restrictiva o demasiado amplia en lo que respecta al intercambio de datos personales entre las autoridades competentes llegando a lesionar el derecho fundamental a la protección de datos personales.

El trabajo se ha estructurado en tres apartados. Así, en primer lugar, en el apartado II se acomete el análisis de los instrumentos elaborados por el Consejo de Europa y la Unión Europea en materia de protección de datos personales, mientras que, en el apartado III, se procederá al análisis de los instrumentos elaborados por la Unión Europea en el marco de la cooperación judicial y penal, señalando los aspectos principales del marco de aplicación y contenido de la Decisión Marco

9 Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo y al Consejo, Aplicación de la Agenda Europea de Seguridad para luchar contra el terrorismo y allanar el camino hacia una Unión de la Seguridad genuina y efectiva, Bruselas, 24-4-2016, COM (2016) 230 final. En el documento, entre las propuestas realizadas para hacer frente a la lucha contra el terrorismo, se afirma que la elaboración de "unas normas comunes sobre protección de datos permitirán ahora a las autoridades policiales y judiciales cooperar más eficazmente entre sí, así como fomentar la confianza y garantizar la seguridad jurídica", reseñando además el acuerdo marco internacional («Acuerdo marco sobre la protección de datos») con el fin de garantizar un elevado nivel de protección de los datos personales que se transfieren entre la UE y los EE.UU para la prevención, detección, investigación y enjuiciamiento de delitos, incluido el terrorismo.

2008/977/JAI del Consejo, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal y elaborada en el antiguo tercer pilar de la Unión Europea. A su vez, en dicho apartado será objeto de reflexión la norma europea ya aludida, esto es, la Directiva del 27 de Abril, relativa a la protección de las personas físicas en relación al tratamiento de datos personales por parte de las autoridades competentes, instrumento que establece un nuevo marco jurídico en lo que respecta a la protección de datos personales en el ámbito de la cooperación policial y judicial en materias penales. Se finaliza -apartado IV- con unas reflexiones que reflejen los pros y contras de la actual regulación en materia de intercambio de datos personales con posibles soluciones al respecto.

2. Desarrollo normativo de la protección de datos en el ámbito del Consejo de Europa y Unión Europea.

Ya se ha expuesto con anterioridad que la importante actividad normativa desplegada tanto en el Consejo de Europa como la UE en el marco de protección de datos personales, se refleja en los distintos instrumentos elaborados al respecto. Conviene aclarar, por una parte, que dicha actividad, en un primer momento, no se realiza en el marco de configuración del espacio de libertad, seguridad y justicia, esto es, en el ámbito de la cooperación judicial penal. Además, en lo que hemos designado como primera etapa de elaboración de instrumentos jurídicos relativos al tratamiento de datos personales en la Unión Europea, se alude al derecho a la intimidad o vida privada y no a la protección de datos personales como derecho autónomo, subrayando que la labor realizada por el Consejo de Europa en lo que a protección de datos personales se refiere es llevada a cabo desde el prisma de la protección de los Derechos humanos. Ello se deduce del propio articulado del Convenio al afirmar en su artículo 1 que "la protección de datos personales es una manifestación del respeto a los derechos humanos", reiterado a su vez en el Preámbulo, al precisar que trata de conciliar "los valores fundamentales del respeto a la vida privada y de la libre circulación de la información entre los pueblos"[10].

En este contexto y conforme se ha expuesto en el apartado introductorio, en el presente apartado serán objeto de reflexión dos instrumentos normativos relativos al tratamiento de datos personales correspondientes a lo que hemos denominado como primera etapa: el Convenio 108 sobre protección de datos personales y la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, elaborada en el llamado "Primer Pilar" acorde a la antigua estructura del Tratado de la Unión.

Ambos instrumentos tienen como finalidad garantizar la protección de la vida privada de toda persona y la no injerencia arbitraria en su vida privada[11] y facilitar la libre circulación de datos entre los Estados, elaborando ambos instrumentos una serie de disposiciones que tratan de conciliar ambos valores, protegiendo los derechos de las personas respecto al tratamiento automatizado de datos personales, recogiendo ambos instrumentos los principios básicos de tratamiento de datos personales así como los criterios que han de regular los flujos transfronterizos, aspectos que se expondrán en las líneas siguientes.

2.1. Convenio 108 del Consejo de Europa.

El instrumento más relevante en materia de protección de las personas en relación al tratamiento automatizado de datos personales[12] es el Convenio 108 del Consejo de Europa[13]. Se trata de

10 Igualmente, el Consejo de Europa ha elaborado diversas normas con el fin de desarrollar dicho Convenio, entre otras, citamos la Recomendación Nº R (87)15, del Comité de Ministros del Consejo de Europa a los Estados miembros por la que se regula el uso de datos personales en el ámbito policial, de 17 de septiembre de 1987, que limita su ámbito de aplicación a los datos personales tratados automatizadamente. En dicha Recomendación, además de una específica referencia al artículo 8 CEDH, se afirma en su Preámbulo que, considerando las disposiciones del Convenio 108 "y en particular las derogaciones permitidas por el artículo 9", se recomienda a los Estados miembros asegurar la publicidad de lo dispuesto en los mismos y en particular los derechos que su aplicación confiere al individuo. En todo caso, son numerosas las referencias que la Recomendación hace para que se recojan en una "legislación nacional específica", las excepciones a los derechos que se recomiendan en la misma. Asimismo, dicha Recomendación requiere el establecimiento de autoridades independientes que velen por la efectividad y adecuada aplicación en lo relativo a la protección de datos personales, acorde al artículo 1, al establecer que cada Estado miembro deberá tener una autoridad independiente que deberá asumir el cumplimiento de los principios contenidos en la Recomendación.

11 Para un estudio más detallado acerca de los primeros gérmenes legislativos en lo que respecta a la protección de datos personales, vid. Davara Rodriguez, M.A. (1998): *La protección de datos en Europa: principios, derechos y procedimiento*, Universidad Pontificia de Comillas, pp. 29 y ss.; Téllez Aguilera, A. (2002): *La protección de datos en la Unión Europea. Diligencias normativas y anhelos unificadores*, Edisofer S.L. pp. 26 y ss.

12 El Convenio estuvo precedido por varias Recomendaciones y dos Resoluciones del Consejo de Ministros referidas a la protección de datos en los sectores privado y público respectivamente. En lo que respecta a la Recomendación 509/1968 del

un texto jurídico vinculante con carácter universal en el ámbito de la protección de datos[14] que tiene en su haber la importante influencia ejercida en los restantes instrumentos elaborados en el ámbito de la Unión Europea. Su finalidad es la de garantizar, a cualquier persona física, unos patrones mínimos de protección en relación al tratamiento automatizado de datos personales, tal y como lo expone el artículo 1 "… el respecto de sus derechos y libertades fundamentales, concretamente el derecho a la vida privada, con respeto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona"[15].

El Convenio pretende armonizar las legislaciones de los Estados miembros en materia de protección de datos, de forma que el Convenio invita a aquellos Estados no miembros del Consejo de Europa a que se adhieran al mismo, siendo facultad del Comité de Ministros el hacer partícipes a todos aquellos Estados que lo deseen (artículo 23.1). A mayor abundamiento y por lo que al Convenio se refiere, la Comisión ha reconocido de forma clara que la aproximación en materia de protección de datos personales en los Estados miembros es necesaria porque "contribuirá de forma importante al establecimiento efectivo de los derechos del ciudadano en el ámbito europeo" [16], considerando al Convenio como el instrumento adecuado para incluir en el ámbito europeo un nivel uniforme en materia de protección de datos.

En efecto, ha de recordarse que el Convenio, en materia de protección de datos y teniendo como objetivo ya señalado el de aproximación en materia de protección de datos personales, procede (artículo 2) a incluir una serie de definiciones sobre lo que se debe de entender por "datos de carácter

---

Consejo de Europa sobre "Los Derechos Humanos y los nuevos logros científicos y técnicos", vid. Arenas Ramiro, M. (2006): *El Derecho Fundamental a la protección de datos personales en Europa*, Tirant Lo Blanch, pp. 151-152 y Téllez Aguilera, A. (2002): *La protección de datos en la Unión…,* op. cit. pp. 91-92. Igualmente, es obligatorio mencionar, en este contexto, la Recomendación Núm. R (85) 20, de 25 de octubre de 1985, sobre protección de datos personales utilizados para fines de marketing directo; Recomendación Núm. R (86) 1, de 23 de enero de 1986 sobre protección de datos personales en la seguridad social; Recomendación Núm. R (89), 2, de 18 de enero de 1989, sobre protección de datos personales utilizados a efectos de empleo; Recomendación n.º (99) 5 del Consejo de Europa, de 23 de febrero de 1999, sobre la protección de la vida privada en Internet. La importancia de estas Resoluciones radica en que se consagra por primera vez principios esenciales sobre la protección de datos que aún hoy se encuentran vigentes.

Por su parte, la Resolución (73) 22, de 26 de septiembre de 1973 del Comité de Ministros del Consejo de Europa, relativa a la protección de la vida privada de las personas físicas respecto de los bancos de datos electrónicos en el sector privado, completada posteriormente con la Resolución (74) 29, de 20 de septiembre del Comité de Ministros del Consejo de Europa, relativa a la protección de la vida privada de las personas físicas respecto a los bancos de datos electrónicos en el sector público. Ambas Resoluciones que recogían principios básicos que luego serían reproducidos en el Convenio. En relación al contenido de ambas resoluciones, vid., Davara Rodriguez, M.A. (1998): *La protección de datos en Europa*…, op. cit. pp. 29 y ss.; Garzón Clariana, G. (1981): "La protección de los datos personales y la función normativa del Consejo de Europa", *Revista de Instituciones Europeas*, V. 8, nº 1, Enero-Abril, pp. 9-25, (esp. pp. 13-14); Martínez Martínez, R. (2002): *Una aproximación crítica* …, op. cit. pp. 160-162.

Es preceptivo señalar asimismo que la Organización para la Cooperación y Desarrollo de Europa (OCDE) mostró su interés en el tema de desarrollo automático de datos constituyendo en 1978 un grupo de expertos para analizar el tema y cuyo resultado fue la elaboración de los siguientes instrumentos: Recomendación de 23 de septiembre de 1980 sobre circulación internacional de datos personales para la protección de la intimidad; Recomendación de 27 de noviembre de 1992 relativa a la seguridad de los sistemas de información; la Declaración de 11 de abril de 1985 sobre "flujos transfronterizos de datos" y la Declaración de 9 de octubre de 1988, sobre "Protección de la intimidad en las redes globales": Para más detalles, vid.: Gutiérrez Castillo, V. L. (2005): "Aproximación a la protección jurídica internacional del Derecho de acceso y protección de datos en Europa", *Derecho y Conocimiento*, V. 3, pp. 5-6; Téllez Aguilera, A. (2002): *La protección de datos en la Unión*…, op. cit. pp. 37-39.

13 De 28 de enero de 1981, firmado por España el 28 de enero de 1982 y ratificado el 27 de enero de 1984, BOE de 15 de Noviembre de 1985.

14 Acerca del contenido del Convenio nos remitimos, entre otros, Arenas Ramiro, M. (2006): *El Derecho Fundamental a la protección de datos*…, op. cit. pp. 153-157; Bru Cuadrado, E. (2007): La protección de datos en España y la Unión…, op. cit. pp. 82-83; Estadella Yuste, O. (1995): *La protección de la intimidad frente a la transmisión internacional de datos personales*, Centre d'Investigació de la Comunicació, Generalitat de Catalunya. Tecnos, pp. 64-68; Garzón Clariana, G. (1981): La protección de los datos…, op. cit. pp. 17 y ss.; Lazpita Gurtubay, M. (1994): "Análisis comparado de las legislaciones sobre protección de datos de los Estado miembros de la Comunidad Europea", *Informática y Derecho*, nº 6-7, pp. 397-420, (esp. pp. 409-416); Zaballos Pulido, E. (2013): *La protección de datos personales en España: evolución normativa y criterios de aplicación*, Memoria presentada para optar al Grado de Doctor, Universidad Complutense de Madrid, pp. 98 y ss.; En la literatura italiana, vid. Pardolesi, R. (2003): "Dalla riservatezza alla protezione dei dati personali: una storia di evoluzione e discontinuità", in *Diritto alla riservatezza e circolazione dei dati personale*. A cura di Roberto Pardolesi, G, Giuffre editore, Volume primo, pp. 33-34; Nino, M. (2012): *Terrorismo internazionale, privacy e protezione dei dati personali***,** Ed. Scientifica, Napoli, pp. 66-73.

15 Tal y como reza a su vez el Preámbulo del Convenio.

16 Vid. al respecto la Recomendación de la Comisión de 29 de julio de 1981, relativa al Convenio del Consejo de Europa sobre protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (DOC nº L 246/31), aceptando que la aproximación en lo que respecta a la protección de datos en las distintas legislaciones de los Estados miembros "contribuiría a eliminar las reservas existentes con relación al tratamiento de datos…", considerando que las diferencias existentes en materia de datos en las legislaciones de los EEMM crean condiciones divergentes en el tratamiento de los mismos…… recomiende a aquellos Estados miembros a que firmen en presente Convenio.

personal"[17], "fichero automatizado"[18], "tratamiento automatizado"[19] y autoridad "controladora del fichero"[20], definiciones que serán reproducidas en los subsiguientes instrumentos normativos que en materia de protección de datos personales ha elaborado la UE, entre los que se encuentran los relativos a la cooperación judicial y penal como se verá en el apartado III. A su vez, el Convenio viene a señalar, de forma expresa en el artículo 3, su campo de aplicación, abordando a su vez la protección de datos personales a cualquier tratamiento automatizado de datos, ya sea público o privado, así como a las distintas clases de ficheros automáticos, extendiendo a su vez el campo de aplicación a los ficheros de datos de carácter personal que no sean objeto de tratamiento automático[21].

En cuanto a los aspectos principales relativos al contenido del Convenio, se reconoce la necesidad de establecer unos principios básicos para la protección de datos que regulen la calidad de los mismos. Así lo dispone expresamente el Convenio al exigir a cada una de las Partes la adopción, en su derecho interno, de las medidas necesarias que garanticen la efectividad de los principios enunciados. Tales son, en concreto: el principio de lealtad[22], principio de exactitud, principio finalista, principio de pertinencia, principio de utilización no abusiva (artículo 5), principios todos ellos que serán reproducidos en los distintos textos normativos elaborados por la UE en relación con la materia reafirmando así la importancia que asume el Convenio en lo que a protección de datos personales se refiere. Continúa el artículo 6 del Convenio enumerando unas categorías particulares de datos catalogados como sensibles que requieren una serie de derechos y garantías mínimas para su tratamiento, reafirmando el Convenio la relevancia que puede tener la información de estos datos; así, se establece el principio de prohibición de tratamiento automático de datos que revelen el origen racial, las opiniones políticas, las convicciones religiosas o de otro tipo, o datos relativos a la salud o vida sexual, a menos que el derecho interno prevea el establecimiento de garantías adecuadas para su tratamiento[23] así como una serie de derechos reconocidos a los titulares de los datos, citando el derecho a la información, acceso, rectificación, borrado así como el derecho a recurrir (artículos 6, 7).

El Convenio enumera en su artículo 8 los derechos de los titulares de los datos bajo la rúbrica "Garantías complementarias para la persona concernida", derechos concretos que permiten al titular del derecho a la protección de los datos controlar cualquier uso o utilización que sus datos personales. Recordemos que los derechos a los que se refiere el Convenio son el derecho a conocer la existencia de ficheros automatizados así como el derecho que tiene a que se le comuniquen los datos que aparecen contenidos en mismos, derecho a rectificarlos o cancelarlos, disponiendo como medida importante el derecho del sujeto afectado a recurrir si no se ha atendido su petición de confirmación, ratificación o borrado[24], derechos cuya observancia es necesaria para no lesionar el derecho fundamental a la protección de datos personales.

Por último, y por lo que a transferencia de datos se refiere, el Convenio en su artículo 12 establece que una parte no podrá, con el único fin de proteger la vida privada, prohibir o someter a autorización especial los flujos transfronterizos de datos de carácter personal destinados al territorio

17 Artículo 1 a) "Datos de carácter personal" significa cualquier información relativa a una persona física identificada o identificable.

18 Artículo 1 b) "fichero automatizado" significa cualquier conjunto de informaciones que sea objeto de un tratamiento automatizado.

19 Artículo 1 c) "tratamiento automatizado" se entiende las operaciones que a continuación se indican efectuadas en su totalidad o en parte con ayuda de procedimientos automatizados: Registro de datos, aplicación a estos datos de operaciones lógicas aritméticas, su modificación, borrado, extracción o difusión.

20 Artículo 1 d) autoridad "controladora del fichero" significa la persona física o jurídica, la autoridad pública, el servicio o cualquier otro organismo que sea competente con arreglo a la ley nacional para decidir cuál será la finalidad del fichero automatizado, cuáles categorías de datos de carácter personal deberán registrarse y cuáles operaciones se les aplicarán.

21 En relación a las personas jurídicas, las disposiciones del Convenio sólo se refieren a los datos de carácter personal y los derechos otorgados a los afectados se refieren a personas físicas, pero no a personas jurídicas: vid. Estadella Yuste, O. (1995): *La protección de la intimidad…,* op. cit. pp. 67-68.
Por su parte, el artículo 3.2, c), determina que lo que se debe hacer constar en el momento de la firma o al depositar su instrumento de ratificación, aceptación, aprobación o adhesión, son las categorías de ficheros automáticos a los que se debe aplicar el Convenio. Para más detalles, vid. Guichot, E. (2005): *Datos personales y administración pública…,* op. cit. p. 29; Téllez Aguilera, A. (2002): *La protección de datos en la Unión*…, op. cit. pp. 26-58.

22 Específicamente, el Convenio en el artículo 5, a) determina, en relación a los datos de carácter personal, que "Se obtendrán y tratarán leal y legítimamente". En relación a ambos términos, Guichot, E. (2005) *Datos personales y administración pública…***,** op. cit. p. 30, precisa que aludir al concepto de tratamiento "legal y legítimo" es ajurídico, optando este autor por la categoría de legal o ilegal.

23 Datos que, en opinión de Garzon Clariana, G. (1981): La protección de los datos…, op. cit. p. 19, deben de ser amparados por una disciplina especial de protección cualificada.

24 Por su parte, el artículo 9 impone una excepción a los artículos 5, 6 y 8 siempre que dicha excepción constituya una medida necesaria en una sociedad democrática para: la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás: vid. Ruiz Miguel, C. (2003): «El derecho a la protección de datos personales en la Carta de Derechos Fundamentales de la Unión Europea», *Revista de Derecho Comunitario Europeo*, núm. 14, pp. 11-12.

de otra parte, intentado así conciliar el respeto a la vida privada y la libre circulación de datos personales entre los Estados parte, esto es, entre los Estados que han ratificado el Convenio. Ahora bien, este principio de prohibir o someter a autorización especial los flujos transfronterizos de los datos de carácter personal tiene unas excepciones delimitadas en el propio articulado del Convenio. La primera de ellas, cuando la legislación de un Estado parte prevea una reglamentación específica para determinadas categorías de datos personales -esto es, datos sensibles- o de ficheros automatizados de datos de carácter personales a menos que la reglamentación de la otra parte establezca una protección equivalente, esto es, deben existir en ambos Estados parte garantías equivalentes en lo que a protección de datos se refiere. La segunda se refiere a aquellos casos en los que la transmisión de datos se lleva a cabo a partir del territorio de un Estado hacia el territorio de otro Estado que no es parte del Convenio, utilizando como intermediario a otro Estado qué si es parte del Convenio, con la única finalidad de evitar que dichas transmisiones tengan como resultado burlar la legislación del país de procedencia de los datos. Por último, el artículo 2.2 del Protocolo Adicional al Convenio prevé la posibilidad de transferir datos personales a Estados que no son parte del Convenio y que no aseguren un adecuado nivel de protección cuando: a) si el derecho interno así lo establezca por causa de intereses concretos del afectado, o intereses legítimos, especialmente los de carácter público, o b) si se prevén las suficientes garantías, que pueden resultar de cláusulas contractuales por parte del responsable del tratamiento responsable de la transferencia y dichas garantías se consideran adecuadas por las autoridades competentes de conformidad con el derecho interno.

En relación a las excepciones al régimen general del tratamiento de datos personales, tal y como hemos expuesto en el apartado introductorio, el Convenio, en su artículo 9, establece la no injerencia en los derechos de los titulares y, en caso de producirse, la misma debe estar prevista por ley del Estado parte en cuestión, y siempre que "constituya una medida una medida necesaria en una sociedad democrática en los siguientes supuestos: a) para la protección de la seguridad del Estado, de la seguridad pública, para los intereses monetarios del Estado o para la represión de infracciones penales; b) para la protección de la persona concernida y de los derechos y libertades de terceros".

2.2. Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995.

Un paso más en el desarrollo de la actividad normativa por parte de la UE en materia de protección de datos lo constituye la Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995[25], relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos[26], Directiva que ha sido sustituida por el Reglamento 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016[27], relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

La base de dicha Directiva son los principios aportados por el Convenio anteriormente mencionado. Se trata del primer instrumento que obliga a los Estados miembros a garantizar la protección, a las personas físicas, de derechos como la intimidad y protección de datos, así como la libre circulación de tales datos. Al igual que el Convenio 108, instrumento del que parece que ha tomado modelo por la estructura idéntica que ofrecen ambos, la Directiva considera el derecho a la protección de datos personales en relación con el derecho al respeto de la vida privada, tal y como se afirma en el artículo 1.1 de la misma[28].

En efecto, entre los objetivos que se marca la Directiva y que ya han sido expuestos al inicio de este apartado, está el asegurar la libre circulación de datos personales entre los Estados miembros a la vez que proteger el derecho a la vida privada en lo que respecta al tratamiento de datos personales. Lo cual es expuesto de forma expresa en el artículo 1 y reiterado en el Considerando nº 2 de la Directiva. No obstante, dadas las diferencias existentes entre los niveles de protección de los derechos y libertades, en particular del derecho a la protección de datos personales en el seno de las legislaciones de los Estados miembros, opta la Directiva por una protección equivalente en todos los Esta-

25 DOCE nº l 181/31, de 23 de Noviembre de 1995.

26 Para un análisis más particularizado de los antecedentes, así como de su contenido, nos remitimos: Gutierrez Castillo, V.L. (2005): "Aproximación a la protección jurídica internacional del derecho de acceso y protección de datos en Europa", *Derecho y conocimiento: anuario jurídico sobre la sociedad de la información y del conocimiento*, nº 3, pp. 11 y ss.; Tellez Aguilera, A., (2002): *La protección de datos en la Unión…,* op. cit. pp. 67-70; Pariente De Prada, I. (2013): "La reforma de la protección de datos en el ámbito europeo", *El espacio de libertad, seguridad y justicia: Schengen y protección de datos*, Thomson-Aranzadi, pp. 121-146.

27 DO L 119/1 de 4 de Mayo de 2016.

28 Considerando 1 y 2 de la Directiva, así como en el artículo1: «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».

dos miembros para lo que resulta esencial la aproximación de las distintas legislaciones en lo que respecta a la protección de datos personales. La propia Directiva reconoce la disparidad existente entre las distintas disposiciones legales en relación a la protección de datos personales, pudiendo llegar a constituir un obstáculo para el ejercicio de actividades económicas como impedir la transmisión de datos de un Estado a otro[29].

En lo que respecta a su ámbito de aplicación, la Directiva se aplica a todas las actividades de tratamiento de datos personales en los Estados miembros en el ámbito del Derecho comunitario (1er. Pilar). Acorde al contenido del artículo 3.2, el instrumento en cuestión no se acomoda al tratamiento de datos personales destinado al ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario, entre las cuales cabe citar la seguridad pública, la defensa o la seguridad del Estado, esto es, se excluye expresamente, las actividades comprendidas en el Título VI TUE, cooperación judicial y policial en materia penal (3er. Pilar)[30].

La Directiva, a su vez, recoge una serie de principios relativos a la calidad de los datos (artículo 6)[31] coincidentes con los establecidos en el artículo 5 del Convenio de 1981 ya mencionado[32], articulando a su vez otros principios que tratan de legitimar el tratamiento de datos (artículo 7), dispensando igualmente a los denominados "datos sensibles" una tutela reforzada (artículo 8), en el sentido ya expresado en relación al Convenio.

Por su parte, el artículo 25 alude a los presupuestos y requisitos para que pueda realizarse una transferencia de datos personales a un tercer Estado[33], articulándose en el mismo una serie de garantías necesarias para realizar dicha transferencia. Dispone específicamente el precepto que la transferencia de datos personales objeto de tratamiento o destinados a ser objeto de tratamiento puedan efectuarse cuando "el país tercero de que se trate garantice un nivel de protección adecuado". Tal y como está redactado el precepto, el "nivel adecuado de protección" es el requisito necesario para que un país tercero pueda obtener la transferencia de datos de otro país de la Unión Europea. En relación a ello, debe tenerse en cuenta que la Directiva prevé el supuesto concreto de si el tercer país no garantiza el nivel adecuado de protección, el Estado miembro debe adoptar las medidas necesarias para que dicha transferencia de datos no se realice.

La Directiva, si bien no deja resuelta la cuestión de que se debe entender por "nivel adecuado de protección" dispone expresamente, en el nº 2 del artículo 25, una serie de parámetros indispensables para apreciar dicho carácter. Así, en particular, será la Comisión, según el artículo 25.4, el órgano encargado de evaluar la naturaleza de los datos, la finalidad y la duración del o de los tratamientos previstos en el país de origen y en el país de destino de los datos, las normas de Derecho, generales o sectoriales vigentes en el tercer país al que se transmiten dichos datos, así como las normas profesionales y las medidas de seguridad en vigor en ambos países. Además, y de conformidad con la interpretación que realiza el Tribunal de Justicia de la UE, el carácter adecuado del nivel de protección que ofrece un tercer país debe apreciarse a efectos de protección de la vida privada o de las libertades o de los derechos fundamentales de la persona, para lo cual se ha de tener en cuenta el artículo 8 de la Carta de los Derechos Fundamentales y el reconocimiento constitucional del derecho a la protección de datos personales o de la vida privada conforme a la legislación interna de cada uno de los países de la Unión Europea[34].

El problema que se plantea en relación al "nivel adecuado de protección" es precisar si el término "adecuado" debe corresponderse a un nivel de protección idéntico al otorgado a los derechos ya mencionados por el ordenamiento jurídico de la Unión en materia de protección de datos personales o

29 Tal y como lo reconoce la Directiva en su Considerando 8 al señalar: "… las grandes diferencias existentes en la actualidad entre las legislaciones nacionales aplicables en la materia y la necesidad de coordinar las legislaciones de los Estados miembros para que el flujo transfronterizo de datos personales sea regulado de forma coherente…".

30 Considerando 13 de la Directiva. En el mismo sentido se ha pronunciado el Tribunal de Justicia de la Unión Europea, en Sentencia 6.11.2003, Asunto C-101/01, Caso Lindqvist.

31 Requisitos de calidad, tal y como los define Pocar/Baruffi, (2014): *Commentario breve ai Trattati dell'Unione Europea*, Cedam, 2ª edizione, p. 190, precisando que deben ser obtenidos los datos de forma leal y lícitamente, para una finalidad determinada, explícita y legítima según la disposición de la propia Directiva.

32 Tal y como lo determina el Considerando 11 de la Directiva, textualmente: "Considerando que los principios de la protección de los derechos o libertades de las personas y, en particular, del respeto de la intimidad, contenidos en la presente Directiva, precisan y amplían los del Convenio de 28 de enero de 1981…".

33 El artículo 1.2 de la Directiva establece que "Los Estados miembros no podrán restringir ni prohibir la libre circulación de datos personales entre los Estados miembros por motivos relacionados con la protección garantizada en virtud del apartado 1".

34 Sentencia Tribunal de Justicia de 6 de Octubre de 2015, asunto C- 362/14, Asunto C-362/14, Maximilian Schrems, apartado 78, al declarar que si los derechos fundamentales pueden ser vulnerados en caso de transferencia de datos a un tercer país que no garantice un nivel de protección adecuado, "la facultad de apreciación de la Comisión sobre el carácter adecuado del nivel de protección garantizado por un tercer país queda reducida, por lo que se debe ejercer un control estricto de las exigencias derivadas del artículo 25 de la Directa 95/46, entendido a la luz de la Carta".

el otorgado por cada uno de los Estados miembros de la Unión en sus correspondientes ordenamientos jurídicos. La respuesta a esta cuestión nos la da el propio Tribunal de Justicia de la UE, al disponer como criterio a seguir en relación al término "adecuado", que él mismo debe interpretarse en el sentido de "que no cabe exigir que un tercer país garantice un nivel de protección idéntico al garantizado en el ordenamiento jurídico de la Unión"[35]. Según el Tribunal, ese nivel adecuado debe ser "sustancialmente equivalente" al garantizado en la Unión por la Directiva 95/46 entendida a la luz de la Carta"[36].

Para evaluar el nivel adecuado de protección en relación a la transferencia de datos personales a un tercer país, se debe tomar como referencia los criterios elaborados por el Grupo de Trabajo[37] constituido en relación a la aplicación de los artículos 25 y 26 de la Directiva. Conforme recoge el documento, es necesario considerar no sólo el contenido de las normas aplicables a los datos personales transferidos a un tercer país, sino también el sistema utilizado para asegurar la eficacia de dichas normas, siendo deseable poder lograr un "núcleo" de principios de "contenido" de protección de datos y de requisitos "de procedimiento/de aplicación", para lo que establece unas condiciones mínimas como punto de partida. Así, se deberá tener en cuenta, por una parte, el reconocimiento de una serie de principios básicos, principios que tal y como son enunciados por el Grupo de Trabajo en el correspondiente Documento, aparecen tanto en el Convenio como en la Directiva objeto de examen, refiriéndose al principio de proporcionalidad y calidad de los datos, de transparencia y de seguridad. A su vez, alude al reconocimiento de una serie de derechos al interesado: el derecho de acceso, rectificación y oposición. Por último, el establecimiento de restricciones en lo que respecta a la transmisión de datos personales a un tercer país. Para el Grupo de trabajo, otro punto interesante para evaluar el carácter adecuado es el mecanismo del procedimiento de aplicación, para lo cual se han de tener en cuenta tres objetivos: a) ofrecer un nivel satisfactorio de cumplimiento de las normas por parte de los responsables del tratamiento de datos personales, con la existencia de sanciones efectivas y disuasorias que ayuden a garantizar el cumplimiento de las normas; b) ofrecer asistencia a los interesados en el ejercicio de sus derechos; c) establecimiento de recursos para aquellos que se sientan perjudicados en el caso de no cumplimiento de las normas. Parámetros todos ellos expresados en la propia Directiva y que deben ser tenidos en cuenta por la propia Comisión tratando así de garantizar el nivel de protección equivalente a que alude el Tribunal de Justicia de la UE en lo que a transferencia de datos a un tercer país se refiere.

Los criterios expuestos por el grupo de trabajo vienen a determinar que el nivel adecuado de protección de datos responde a lo que podemos denominar como nivel mínimo de protección, con independencia de que algunos países reconozcan un nivel más elevado de protección en lo que se refiere a los datos personales[38]. Será la Comisión quien deberá autorizar la transferencia de datos a ese tercer país, aunque lo realice con un nivel menor de garantías relativas al núcleo esencial del contenido del derecho que las establecidas en la propia legislación interna del Estado miembro. No obstante, en este punto se deben valorar las consecuencias que tendría para el titular de los datos personales que se transfieren a ese tercer país, al ver memadas las garantías que rodean al contenido del derecho fundamental a la protección de datos personales, llegando incluso a poder lesionar el contenido de dicho derecho fundamental.

La Directiva prevé igualmente qué si el "nivel de protección adecuado" no está constatado, no se procederá a la transmisión de datos personales por parte de la Comisión encargada de evaluar el requisito de adecuación, esto es, siempre y cuando no se constate la capacidad o aptitud de tutela de tales datos por parte del ordenamiento del Estado destinatario de los datos. Si bien, en este supuesto concreto, la propia Directiva prevé en el artículo 25.6 el mecanismo de la negociación para tratar de resolver la situación de inadecuación, negociación que se iniciará en "el momento oportuno", y que irán destinadas a remediar la situación. No obstante, ni el precepto ni los Considerandos de la Directiva se ocupan de matizar las condiciones y formas en las que debe realizarse dichas negociaciones ni

35 Sentencia del Tribunal de Justicia (Gran Sala), de 6 de octubre de 2015, Asunto C-362/14, Maximilian Schrems,

36 Sentencia Tribunal de Justicia de 6 de Octubre de 2015, asunto C- 362/14, Asunto C-362/14, Maximilian Schrems, apartado 74, sentencia en la cual se declara inválida la Decisión 2000/520/CE de la Comisión, de 26 de junio de 2000, con arreglo a la Directiva 95/46/CE, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América (DOC L 215/17), al no garantizar Estados Unidos un nivel adecuado de los datos personales transferidos.

37 Vid. Documento de Trabajo "Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE", Aprobado por el Grupo de Trabajo el 24 de julio de 1998.

38 Lo cual reconoce el Grupo de Trabajo creado el 24 de julio de 1998, en el Documento de Trabajo "Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE", disponible en: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_es.pd.
En lo referente a la consecución de un núcleo de principios de contenido en relación a la protección de datos personales, es necesario destacar que en algunos supuestos, conforme a la legislación de los distintos países, será necesario ampliar y en otros supuestos incluso será necesario reducirla.

determina lo que debe considerarse por "momento oportuno", laguna importante a tener en cuenta y que deberá solucionarse mediante la aplicación de normas internacionales. Además, dichas negociaciones deben llevarse a cabo en sede diplomática mediante la adopción de un acuerdo internacional que será negociado entre la Comisión y las autoridades del tercer país al que se han transferido los datos, planteando la duda de hasta qué punto la Comisión puede obligar a ese tercer país a modificar e introducir nuevas garantías de protección de un derecho fundamental, máxime en un modelo de Estado de Derecho[39].

Es de destacar que la Directiva, en su artículo 26 y en su Considerando nº 58, establece la posibilidad de disponer de la transferencia de datos a un tercer país aún en el supuesto de que dicho país no garantice una tutela adecuada de protección de datos personales. Así, se establece como primera excepción el consentimiento del interesado a la transferencia prevista. Igualmente, cuando la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento de datos o una acción judicial (textualmente para la ejecución de medidas precontractuales tomadas a petición del interesado) o cuando sea necesario para la protección de un interés público importante (así, por ejemplo, en caso de transferencia internacional de datos entre las administraciones fiscales o aduaneras). También se procederá a realizar la transferencia en los casos en que sea necesaria para la salvaguardia del interés vital de interesado o cuando la transferencia se haga desde un registro previsto en la legislación con fines de consulta por el público o por personas con un interés legítimo. Por su parte, el artículo 26, nº 2 precisa qué si el responsable del tratamiento de datos ofrece garantías suficientes respecto a la protección de la vida privada y de los derechos y libertades fundamentales de las personas, los Estados miembros pueden autorizar la transferencia aún en el supuesto de que el tercer país no ofrezca garantías suficientes respecto a dichos derechos, derivándose dichas garantías de cláusulas contractuales apropiadas. En este supuesto los Estados miembros informarán a la Comisión y a los demás Estados miembros acerca de la autorización. Parece deducirse que se otorga a las cláusulas contractuales una tercera vía alternativa de protección a la intimidad en lo que respecta a la protección de datos personales sin restringir ni prohibir la libre circulación de datos personales entre los Estados miembros.

Por último, y para cerrar el marco normativo de la UE en esta materia se deben mencionar una serie de directivas cuya finalidad es la protección de datos personales[40] , así como el Reglamento del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000[41], relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos. El Reglamento, al igual que la Directiva, viene a establecer en su artículo 1 que su finalidad no es otra que la de garantizar la protección efectiva de los derechos y las libertades fundamentales de las personas físicas, en particular el derecho a la intimidad en lo que respecta a la protección de datos personales y, la no limitación de la libre circulación de dichos datos. Ambos instrumentos, Directiva y Reglamento, van a ser derogados respectivamente por el ya mencionado Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016[42], relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE. A su vez, en el marco de la cooperación judicial y penal se aprueba la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016, objeto de reflexión en las líneas siguientes.

---

39 Vid. al respecto Aparicio Salom, J. (2002): *Estudio sobre la Ley Orgánica de Protección de Datos de carácter Personal*, Thomson-Aranzadi, p. 217, quien, en relación al caso español conforme a la Ley de Protección de Datos Española (LOPD), afirma que incrementa la inseguridad el hecho de que no sea posible determinar con claridad "qué supone la exigencia de que se otorgue un nivel de protección equiparable que exige la LOPD, esto es, semejante pero no idéntico".

40 Igualmente hay que aludir a la Directiva 97/66/CE, del Parlamento europeo y del Consejo, de 15 de diciembre de 1997, sobre Protección de Datos y Telecomunicaciones, encargada de regular la protección de datos personales en el sector de las telecomunicaciones, que ha sido derogada por la Directiva 2002/58/CE, de 12 de Julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), que a su vez ha sido modificada por la Directiva 2006/24/CE, sobre Conservación de Datos de Tráfico en las Comunicaciones Electrónicas (DOUE nº L 105, de 13 de Abril de 2006), que no son sino aplicación de la Directiva 95/46/CE a estos ámbitos específicos. La Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, por la que se modifican la Directiva 2002/22/CE re4lativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (/CE) número 2006/2004 sobre cooperación en materia de protección de los consumidores.

41 DO L 8 de 12.1.2001, Reglamento (CE) nº 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos. Acerca del contenido de dicho Reglamento, vid. Arenas Ramiro, M. (2006): *El derecho fundamental a la protección de datos…,* op. cit. pp. 283-284;

42 DO L 119/1 de 4 de Mayo de 2016.

3. Desarrollo normativo de la protección de datos en el marco DEL ESPACIO DE LIBERTAD SEGURIDAD Y JUSTICIA.

3.1. La protección de datos personales en el marco de la cooperación judicial y penal.

La segunda fase de desarrollo normativo en lo que se refiere a la protección de datos personales en la Unión Europea se ha ido produciendo en la medida en que se reafirmaban los distintos componentes del ELSJ. La UE, en el desarrollo del objetivo de mantener y consolidar un espacio de libertad, seguridad y justicia donde se asume el objetivo de lucha contra la delincuencia organizada, admite la exigencia de mejora en la cooperación entre los servicios policiales, judiciales y aduaneros, tratando de encontrar el necesario equilibrio entre el respeto al derecho a la protección de datos personales, así como al derecho a la intimidad y la seguridad en el intercambio de la información.

Cabe recordar la importancia que han ido adquiriendo los derechos fundamentales en el espacio de libertad, seguridad y justicia, al quedar plenamente establecidos como un fundamento básico y una finalidad fundamental[43]. Ello se observa en las materias y las distintas actuaciones que ha llevado a cabo la Unión en el marco del espacio de libertad, seguridad y justicia.

Así, ya en el programa de la Haya (2005-2009) se contemplaba la elaboración, por parte del Consejo, de un Plan de acción[44] destacando como objetivos y prioridades del programa la inclusión de medidas destinadas a ofrecer una respuesta global que conllevase el desarrollo y puesta en práctica de un concepto estratégico en materia de lucha contra la delincuencia organizada en la UE[45]. A su vez, incluía como cometido la necesidad de encontrar un equilibrio adecuado entre protección de vida privada y seguridad en el intercambio de información entre autoridades policiales y judiciales, asegurando a su vez el respecto a los derechos mencionados[46].

Por su parte, el Programa de Estocolmo (2010-2014)[47], definía unas orientaciones estratégicas para la consecución del proyecto legislativo dentro del espacio de libertad, seguridad y justicia de acuerdo con el artículo 68 del TFUE. Entre sus objetivos destaca el de conferir a los ciudadanos de la UE los derechos y las libertades fundamentales consagrados en la Carta de los Derechos Fundamentales de la UE y en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales. Cabe recordar que el Plan de Acción[48] dispuesto en aplicación del programa de Estocolmo ya disponía como una de las acciones a concretar la de garantizar la aplicación coherente del derecho fundamental a la protección de datos, sabiendo que se respeta su intimidad, en especial en relación a la protección de datos de carácter personal.

Finalmente, en este contexto no debe olvidarse el reconocimiento que del derecho a la protección de datos personales realiza la CDFUE[49].Así, el artículo 8.1 afirma que "Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan". El reconocimiento de este derecho[50] se consolida como un Derecho fundamental autónomo y no como una nueva dimensión

43 Vid. Díaz Barrado, C.M. (2012): "La dispersión y sectorización de los derechos humanos en el seno de la Unión Europea", *Estudios de derecho internacional y de derecho europeo en homenaje al profesor Manuel Pérez González*, Coord. Aznar Gómez y otros, Vo. I, (Tomo I), Tirant Lo Blanch, pp. 1453-1474.

44 Comunicación de la Comisión al Consejo y al Parlamento Europeo, de 10 de mayo de 2005, «Programa de La Haya: Diez prioridades para los próximos cinco años. Una asociación para la renovación europea en el ámbito de la libertad, la seguridad y la justicia» COM (2005) 184 final. DO C 236 de 24.9.2005, en entre sus prioridades determinar que se encuentra el "luchar contra cualquier forma de discriminación y garantizar la protección de los datos personales".

45 Programa de la Haya: Consolidación de la Libertad, la Seguridad y la Justicia en la Unión Europea DOUE, nº C 53/01, de marzo de 2005

46 Precisaba dicho programa que "La incorporación de la Carta en el Tratado Constitucional y la adhesión al Convenio Europeo para la protección de los derechos humanos y de las libertades fundamentales impondrá a la Unión, con inclusión de sus instituciones, una obligación legal de garantizar -en todos sus ámbitos de actuación- no sólo el respecto sino también la promoción activa de los derechos fundamentales".

47 Programa de Estocolmo: Una Europa abierta y segura que sirva y proteja al ciudadano, DOUE nº C 115/1, de 4 de mayo de 2010.

48 Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones bajo el título "Garantizar el espacio de libertad, Seguridad y Justicia para los ciudadanos europeos", Bruselas, 20 de Abril de 2010, (COM 2010, 171 final), donde se reafirma la UE en Debemos reforzar la posición de la UE en cuanto a la protección de los datos personales en el contexto de todas las políticas de la UE, incluida la represión policial y la prevención de la delincuencia, así como en nuestras relaciones internacionales.

49 Carta de Derechos Fundamentales de la Unión Europea de 7 de Diciembre de 2000 (DO C 364), confirmada en Estrasburgo el 12 de diciembre de 2007 (DO C 303, de 14 de diciembre de 2007).

50 El Tratado Constitucional europeo, en su artículo II-68 recoge únicamente de la protección de datos de carácter personal; así, prevé que toda persona tiene derecho a la protección de datos de carácter personal que la afecten, y se le reconoce el derecho de acceder y de obtener la rectificación, datos que deben ser tratados de modo leal, en concreto para los fines determi-

de la privacidad, al reconocer dicho derecho al margen del derecho a la privacidad, artículo 7 de la Carta[51] y cuya observación queda sujeta al control de una autoridad independiente, novedad ésta importante al destacar que la ausencia de esta autoridad de control supondría una intromisión arbitraria en la esfera privada de la persona.

Siguiendo la estructura ya expuesta en el apartado introductorio del trabajo, en el presente apartado se analizan los dos instrumentos elaborados en el ámbito de la cooperación judicial y policial en relación al tratamiento de datos personales así como las disposiciones relativas a la transmisión de datos a terceros países u organizaciones internacionales.

3.2. Decisión Marco 2008/977/JAI del Consejo, de 27 de Noviembre de 2008.

El instrumento más relevante a nivel europeo en el marco de la cooperación judicial y policial en materia de protección de datos es la Decisión Marco 2008/977/JAI del Consejo, de 27 de Noviembre de 2008, relativa a la protección de datos de carácter personal tratados en el marco de la cooperación policial y judicial en materia penal[52]. El objetivo de la presente norma lo determina la propia Decisión Marco (en adelante, DM), en su considerando 42, el establecimiento de normas comunes para la protección de datos personales tratados en el marco de la cooperación judicial y policial[53].

La estructura que presenta la DM es similar a la de la Directiva ya analizada anteriormente, pero con una diferencia fundamental en lo que respecta a su ámbito de aplicación. En efecto, conforme a lo establecido en el Considerando (5) se precisa que la Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, no es aplicable "al tratamiento de datos personales efectuado en el ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario, como las contempladas en el título VI del Tratado de la Unión Europea y, en cualquier caso, al tratamiento de datos que tenga por objeto la seguridad pública, la defensa, la seguridad del Estado y las actividades del Estado en materia penal" [54]. El ámbito de aplicación de la DM queda limitada por tanto al tratamiento, con fines de prevención, investigación, detección o enjuiciamiento de delitos o ejecución de sanciones penales, de datos personales que se transmitan o se hayan transmitido o puestos a disposición entre Estados miembros[55] o a autoridades o sistemas de información[56], excluyendo los datos personales que un Estado miembro haya obtenido en el ámbito de aplicación de la DM y que tengan su origen en ese mismo Estado miembro (Considerandos 6 y 9)[57].

En su artículo 1, reafirmado asimismo en el Considerando 3 de la DM, viene a precisar que la legislación en el ámbito del título VI del Tratado de la UE debe "mejorar la cooperación policial y

---

nados, sobre la base de su consentimiento o en virtud de otro fundamento legítimo previsto por la ley. Dispone asimismo que el respeto de estas reglas estará sometida al control de una autoridad independiente.

51 Artículo 7: Respeto de la vida privada y familiar. "Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones". Véase como comentario del derecho y precepto: Gutiérrez Castillo, V.L. (2005): "Aproximación a la protección jurídica internacional …, op. cit. pp. 31-49; Martínez Martínez, R. (2007): "El derecho fundamental a la protección de datos: perspectivas", Revista de Internet, Derecho y Política, nº 5, pp. 47-61, (esp. p. 50 y 51).

52 DO L350/60 de 30 de diciembre de 2008.

53 Sobre la justificación de la Decisión Marco, vid. Cabezudo Bajo, Mª . J. (2008): "La protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal", *La Justicia y la Carta de Derechos Fundamentales de la Unión Europea*, De La Oliva Santos, A. (Dir.), Aguilera Morales, M./Cubillo López, I. (Coords.), Colex, pp. 327- 342 (esp. pp. 330-334).

54 Ver Informe de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las regiones, presentado de conformidad con el artículo 29, apartado 2, de la Decisión Marco del Consejo, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal: Bruselas, 25.1.2012. COM (2012) 12 final, SEC (2012) 75 final.

55 Ver "Informe de la Comisión al Parlamento Europeo, al Consejo, al Comité económico y social Europeo y al Comité de las regiones", presentado de conformidad con el artículo 29, apartado 2 de la Decisión Marco del Consejo, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal, COM (2012) 12 final, de 25.1.2012.

56 Considerando 7 y artículo 1. 2. a) b) y c) de la DM.

57 Lo que ha sido objeto de críticas por parte de la doctrina, vid. en este sentido, Nino, M, (2012): *Terrorismo Internazionale, Privacy e protezione dei dati personal…,* op. cit, 82, aludiendo a "datos domésticos". En la doctrina española, las críticas en relación a este punto, vid. Bayo Delgado, (2008): "La cooperación judicial internacional a la luz de la propuesta revisada de la Decisión Marco relativa a la protección de datos", *La protección de datos en la cooperación policial y judicial*, Aranzadi, pp. 28 y ss. Otras limitaciones, contempladas en el Considerando 39, al entender la presente norma no debe afectar al conjunto de disposiciones de protección de datos, al considerar que dichas disposiciones ya conforman un "conjunto completo y coherente de normas que abarcan todos los aspectos correspondientes de la protección de los datos". Así, cita a Europol, Eurojust, SIS, y SIA.

judicial en materia penal en lo que respecta a su eficacia y a su legitimidad y respeto de los derechos fundamentales, en particular el derecho a la intimidad y a la protección de datos personales"[58]. Para conseguir dicho objetivo, será necesario el establecimiento de normas comunes para la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal (Considerando 42)**[59]**.

En cuanto al contenido de la DM, es de obligada referencia aludir a los principios esenciales aplicables a la recogida y tratamiento de datos (artículo 3), similares a los establecidos en la Directiva 95/46 así como en el Convenio nº 108[60]. Se establece igualmente un tratamiento específico en relación a lo que se denomina "datos sensibles", en la misma línea que los dos instrumentos ya mencionados. El artículo 13 dispone la transferencia de datos personales a la autoridad competente de terceros países u a organismos internacionales de un determinado Estado estableciendo una serie de requisitos para la misma. No nos vamos a extender en el contenido de la DM por dos razones; en primer lugar, porque la misma ha sido objeto de críticas por su limitado ámbito de aplicación, así como por las diversas lagunas que presenta en relación a su contenido[61] y, además, porque la DM ha sido sustituía por Directiva 2016/680 (UE) del Parlamento Europeo y del Consejo objeto de reflexión en el epígrafe siguiente.

3.3. El Tratado de Lisboa y la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo.

El pasado 27 de Abril de 2016 fue publicada la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos[62] y por la que se deroga la Decisión Marco 2008/977/JAI.

La Directiva, junto al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016**,** relativo a la protección de las personas físicas en lo que respecta al tratamiento y libre circulación de datos personales, conforman lo que se denomina el nuevo marco europeo de protección de datos personales**.** En el propio preámbulo del TFUE define, en el artículo 67 los objetivos principales del espacio de libertad, seguridad y justicia, a cuya consecución pretende contribuir la Directiva en cuestión según dispone el Considerando (2) de la misma al garantizar un alto nivel de seguridad mediante la prevención de la delincuencia y la cooperación entre las autoridades judiciales y policiales.

La Directiva en cuestión viene a afirmar el cambio producido operado tras el Tratado de Lisboa con la introducción de la protección de datos personales en el ámbito de la cooperación judicial y policial. El marco legal básico de dicha Directiva es el artículo 83.2 TFUE, en la premisa del establecimiento, en materia de Derecho penal sustantivo, de normas mínimas que definan las infracciones penales y sanciones que resulte necesario establecer para desarrollar de forma efectiva las políticas de armonización propias de la Unión o las que se refieran a ámbitos criminales dotados de especial gravedad y dimensión transfronteriza, como el terrorismo, la criminalidad organizada, el tráfico de drogas, el blanqueo o la criminalidad informática (artículo 83.1 TFUE).

---

58 Considerando 3 de la DM.

59 Para un análisis más detallado sobre la DM nos remitimos a Etxebarria Juridi, J.F. (2009): "Principio de disponibilidad y protección de datos personales: a la búsqueda del necesario equilibrio en el espacio judicial penal europeo", Eguzkilore, nº 23, San Sebastián, Diciembre, pp. 351 – 366, (esp. p. 362), quien manifiesta la inexistencia de un régimen unificado en la materia.

60 En este punto, nos remitimos a la crítica que realiza NINO, M, (2012): *Terrorismo Internazionale, Privacy e protezione dei dati personale…*, op. cit. p. 88, quien considera una decisión no acertada aplicar los mismos principios y la misma modalidad de tratamiento de datos a categorías distintas, optando este autor por una protección más rígida de los datos a los que se refiere la DM que a los que prevé la Directiva.

61 Tal y como lo exponer el Documento de trabajo de los servicios de la Comisión. Resumen de la evaluación de impacto que acompaña al documento Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y Directiva del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y la libre circulación de dichos datos, Bruselas, 25-1-2012. SEC (2012) 73 final.

Para más detalles acerca del contenido de la Decisión Maro, así como a las críticas realizadas por la doctrina a su contenido, nos remitimos, por parte de la doctrina italiana, Nino, M, (2012): *Terrorismo Internazionale, Privacy e protezione dei dati personale…,* op. cit. pp. 86-92.

62 Acerca del antecedente de la Directiva, Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y la libre circulación de dichos datos, vid. COM (2012) 10 final, de 25.01.2012.

Parte la Directiva en reconocer en su primer Considerando que la protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental, tomando como referente de dicho reconocimiento el artículo 8, apartado de la Carta de los Derechos Fundamentales de la Unión Europea y el artículo 16, apartado 1, del TFUE, base legal de la Directiva[63].

La Directiva trata de establecer normas armonizadoras para la protección y la libre circulación de los datos personales tratados con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, apelando, conforme al Considerando (15), a la necesidad de garantizar el mismo nivel de protección de datos personales y evitar divergencias que puedan obstaculizar el intercambio de datos personales entre las autoridades judiciales y policiales, lo cual evidencia la necesidad de una aproximación de legislaciones internas de los Estados miembros. Todo ello sin impedir "a los Estados miembros que ofrezcan garantías mayores que las establecidas en la presente Directiva para la protección de los derechos y libertades del interesado" (Considerando 15 y artículo 1, 3)

Conforme a lo expuesto, la finalidad de la Directiva es, además de garantizar un alto nivel de protección de datos personales mediante el establecimiento de un marco sólido y coherente para la protección de datos personales en la Unión Europea[64], facilitar la libre circulación de datos personales entre las autoridades policiales y judiciales competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública, tal y como se indica en el artículo 1 y se reitera en el Considerando (4). Expresamente, establece la Directiva que, en el marco de una actuación policial consistente en la adopción de medidas coercitivas llevadas a cabo para reprimir una manifestación o disturbio, la misma será considerada como actuación de la policía llevada a cabo con la finalidad de detección o prevención frente a las amenazas para la seguridad pública (Considerando 12) pudiendo proceder en este supuesto a la libre circulación de datos personales entre las apropias autoridades policiales y judiciales en el marco de la investigación policial.

Por lo que respecta al ámbito de aplicación de la Directiva en cuestión, la misma se aplica al tratamiento de datos personales realizados por parte de las autoridades competentes, judiciales y policiales, para actividades de prevención, investigación, detección o enjuiciamiento de infracciones penales o ejecución de sanciones penales (artículo 2, 1). Si bien, con efecto extensivo, también será objeto de aplicación la presente Directiva, a diferencia del Convenio nº 108, al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero[65]. Por último, hemos de excluir de forma expresa del ámbito de aplicación de la presente norma al tratamiento de datos personales realizados en el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión y los tratamientos de datos personales por parte de las instituciones, órganos u organismos de la Unión[66].

En cuanto al contenido concreto de la Directiva, de la lectura de la misma se observa ciertas similitudes con la Directiva 95/46/CE, aunque en algunos aspectos se aprecia un desarrollo más exhaustivo. Por ello, considero de interés proceder a realizar una serie de consideraciones, de forma breve, dejando entrever además la influencia que en el contenido de la misma han tenido los instrumentos antes mencionados, el Convenio 108 del Consejo de Europa y la de la Directiva 95/46/CE.

Así, en primer lugar, los principios relativos al tratamiento de datos personales con fines de investigación, prevención o detección de infracciones penales, detallados en la Directiva en los artículos 4 y ss., vienen a ser coincidentes con los ya especificados tanto en el Convenio 108 como en la Directiva 95/46/CE y Decisión Marco ya expuestos, si bien con una redacción algo más precisa que la que presentaba los textos normativos mencionados.

A su vez, enumera una serie de definiciones coincidentes con las ya mencionadas en relación a la Directiva 95/ 46/CE, pero con algunas novedades entre las que destaca la previsión específica que se realiza a lo que se entiende por "autoridad competente" para la prevención, investigación, detec-

63 Acerca del artículo 16 del TFUE, vid. Pocar/Baruffi, (2014): *Commentario breve ai Trattati* …, op. cit. pp. 189-198.

64 El artículo 16, apartado 2 del TFUE, precepto que exige al Parlamento Europeo y al Consejo que establezcan normas sobre la protección de las personas físicas respecto del tratamiento de datos de carácter personal y sobre la libre circulación de los datos. En base a este artículo, vid. la Declaración nº 21 del Acta final de la Conferencia Intergubernamental acerca del Tratado de Lisboa, donde se reconoce igualmente dicha posibilidad en los ámbitos de la cooperación judicial en materia penal y de la cooperación policial que se basen en el artículo 16 del Tratado de Funcionamiento de la Unión Europea.

65 Viene a especificar en el Considerando (18) de la Directiva que la presente norma se debe aplicar al tratamiento manual -no automatizado- si los datos personales están contenidos o destinados a ser incluidos en un fichero, indicando de forma expresa que aquellos ficheros o conjuntos de ficheros que no estén estructurados con arreglo a criterios específicos, no podrán incluirse en el ámbito de aplicación de la presente Directiva. Entre los criterios específicos, se encuentran

66 En cuyo caso se aplicaría el Reglamento (CE) nº 45/2001 al ser de aplicación al tratamiento de datos de carácter personal por parte de las instituciones, órganos y organismos de la Unión (artículo 2.3).

ción o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluidas la protección y prevención frente a amenazas para la seguridad pública; o las definiciones que da la Directiva respecto a lo que se debe entender por datos genéticos, datos biométricos o datos relativos a la salud, datos todos ellos que vienen a unirse a lo que hemos denominado datos sensibles acorde al Convenio y a la Directiva 95//46/CE, regulados igualmente en la Directiva objeto de reflexión en su artículo 10 y para los que se establecen una serie de garantías específicas debido a su categoría especial.

4.4. Transferencias de datos a terceros países y organizaciones internacionales.

La Directiva, en el artículo 35 y ss., alude a las transferencias de datos personales a terceros países u organizaciones internacionales. La redacción de este precepto presenta algunas diferencias respecto al artículo 25 de la Directiva 95/46/CE, cuyo contenido ya se ha expuesto en las líneas precedentes[67] y del Reglamento 2016/679 que la sustituye[68]. Así, acorde a la Directiva en cuestión, la transferencia de datos personales solo podrá ser llevada a cabo por las "autoridades públicas competentes", y se realizarán solamente si resultan necesarias para la prevención, investigación, detección o enjuiciamiento de infracciones penales o ejecución de sanciones penales, inclusive en los supuestos de prevención y protección frente a las amenazas contra la seguridad pública. La Directiva exige como requisito para proceder a realizar la transferencia de datos personales que se trasmiten o proceden de otro Estado miembro, que dicho Estado miembro haya dado su autorización previa para la transferencia de conformidad con el Derecho nacional. Además, al igual que la Directiva 95/46/CE, dicha transferencia sólo podrá llevarse a cabo en los supuestos en los que la Comisión haya determinado que el tercer país u organización internacional a quienes se van a transferir los datos, garantizan un nivel "adecuado de protección" o hayan ofrecido garantías apropiadas de protección de datos personales. Acorde a la redacción de este precepto de la Directiva en cuestión, se plantea la misma incógnita ya expuesta en lo relativo a la Directiva 95/46/CE en el sentido de determinar cuando existe ese nivel adecuado de protección. En el Considerando (67) de la Directiva objeto de reflexión, se alude a los mismos criterios ya expuestos en relación al artículo 25 de la Directiva 95/46/CE que delimitaban el adjetivo "adecuado" para precisar dicho nivel, criterios que, como ya se ha dicho, fueron elaborados por el Grupo de trabajo creado en 1998 y que dio lugar al Documento de Trabajo relativo a las Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE Así, precisa la Directiva 2016/680 que en consonancia con los valores fundamentales en los que se basa la Unión, en especial la protección de los derechos humanos, la Comisión debe tener en cuenta si ese tercer país respeta al Estado de Derecho, el acceso a la justicia, las normas y principios internacionales en materia de derechos humanos, así como su Derecho tanto general como sectorial, el Derecho penal y el orden público. Incluye la Directiva en el artículo la necesidad de que la Comisión deba tener en cuenta el acceso de las autoridades públicas a los datos personales, así como la aplicación de dicha legislación, las normas de protección de los datos, las normas profesionales y las medidas de seguridad. Además, ese tercer país debe ofrecer garantías que aseguren un nivel de protección adecuado que sea esencialmente "equivalente al garantizado en el interior de la Unión".

En ausencia del nivel adecuado de protección, prevé la Directiva (artículo 37), la transferencia de datos personales en el supuesto concreto de que existan garantías adecuadas materializadas en un instrumento vinculante que aseguren la protección de datos personales. Entre dichos instrumentos menciona la Directiva, por ejemplo, acuerdos bilaterales jurídicamente vinculantes celebrados por los Estados miembros y aplicados en su ordenamiento jurídico y cuyo cumplimiento puede ser exigido por los interesados de dichos Estados o, como mecanismo alternativo, que el responsable del tratamiento haya evaluado todas las circunstancias que concurren en la transferencia de datos personales llegando a la conclusión de que existen garantías apropiadas con respecto a la protección de datos personales.

Aún en la hipótesis de no existir una autorización previa por parte de la Comisión para llevar a cabo la transferencia de datos a un tercer país o una organización internacional, bien por no existir un nivel adecuado de protección ni las garantías adecuadas mencionadas en la Directiva, expresamente se podrá llevar a cabo dicha transferencia (artículo 38) en los siguientes supuestos: a) para proteger los

67 Vid. supra pp. 11-14.

68 Diferencias que se deducen del propio Reglamento 2016/679, artículo 44, Principio General de las transferencias, al determinar: "Solo se realizarán transferencias de datos personales que sean objeto de tratamiento o vayan a serlo tras su transferencia a un tercer país u organización internacional si, a reserva de las demás disposiciones del presente Reglamento, el responsable y el encargado del tratamiento cumplen las condiciones establecidas en el presente capítulo, incluidas las relativas a las transferencias ulteriores de datos personales desde el tercer país u organización internacional a otro tercer país u otra organización internacional. Todas las disposiciones del presente capítulo se aplicarán a fin de asegurar que el nivel de protección de las personas físicas garantizado por el presente Reglamento no se vea menoscabado".

intereses vitales del interesado o de otra personal; b) para salvaguardar intereses legítimos del interesado cuando así lo disponga el Derecho del Estado miembro que transfiere los datos personales; c) cuando sea esencia para prevenir una amenaza inmediata y grave para la seguridad pública de un Estado miembro o de un tercer país; d) la transferencia sea necesaria en casos concretos a efectos de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales; e) la transferencia sea necesaria en casos individuales para el establecimiento, el ejercicio o la defensa de acciones legales en relación a la prevención, investigación, detección o enjuiciamiento de una infracción penal o la ejecución de una sanción específica. Excepciones que deben ser muy restrictivas, exclusivamente para los supuestos aludidos en el artículo citado.

No obstante, consideramos que en relación a la transferencia de datos personales a un tercer país u organización internacional, siguen persistiendo los mismos problemas de interpretación en relación a la decisión de adecuación y el nivel requerido de protección, no quedando resuelta la incógnita de qué sucederá en el supuesto de que un Estado miembro tenga un nivel superior de garantías relativas al contenido del derecho fundamental a la protección de datos de aquellos sujetos intervinientes en un proceso penal y cuyos datos se deben transferir, como, por ejemplo, datos relativos a víctimas, sospechosos y testigos, que el de la Unión, si queda lesionado el contenido del derecho a la protección de datos personales al rebajar el nivel de garantías en el supuesto de que se proceda a transferir los datos en el marco de una investigación judicial, así como los mecanismos legislativos que debe desarrollar la Comisión para que no se produzca dicha lesión.

Finalmente, hemos de realizar una referencia específica al artículo 41 y ss. de la Directiva en cuestión, donde se alude a la existencia de autoridades de control. Específicamente, el artículo 41 precisa la existencia de una o varias autoridades públicas (autoridades de control) independientes, con la única finalidad de supervisar "la aplicación de la presente Directiva, con el fin de proteger los derechos y las libertades fundamentales de las personas físicas en lo que respecta al tratamiento de datos personales…", lo que se reafirma a su vez en el Considerando (75). Autoridad de control que debe ser creada de conformidad con el Reglamento (UE) 2016/679.

La creación de una o varias autoridades de control en el cumplimiento de las normas de la Unión en materia de protección de datos ya venía prevista en el Convenio nº 108 (artículo 13.2) y en la Directiva 95/46/CE (artículo 28). La creación de esta figura tiene como finalidad el garantizar el cumplimiento de las disposiciones relativas al tratamiento de datos personales de las personas físicas por parte de los organismos e instituciones correspondientes, en aras de garantizar una protección efectiva a dicho derecho, llegando a constituir su creación un elemento esencial de la protección de las personas en lo que respecta al tratamiento de datos personales[69]. La autoridad de control debe disponer de amplios poderes para el ejercicio de sus funciones, siendo un requisito necesario para el ejercicio de las funciones que tiene asignadas la de ejercitar las mismas con total independencia en cada uno de los Estados miembros, garantía que tiene como finalidad la de asegurar un control eficaz e íntegro en el cumplimiento de la normativa de protección de las personas físicas frente al tratamiento de datos personales. El requisito de independencia de la autoridad de control viene reconocido igualmente en la Carta de Derechos Fundamentales de la Unión, al precisar en el artículo 8.3 que el respeto a las normas relativas a la protección de datos personales "quedará sujeto al control de una autoridad independiente".

La Directiva, en su artículo 41, asigna a la autoridad de control la función de supervisar la aplicación de la presente Directiva, atribuyendo a su vez, en el artículo 46, una serie de funciones como son la de informar a cualquier interesado en relación con el ejercicio de sus derechos, promover la sensibilización de los responsables y encargados del tratamiento de datos acerca de las obligaciones que les incumben, asesorar igualmente al Parlamento nacional, al Gobierno y a otras instituciones y organismos sobre las medidas legislativas y administrativas relativas a la protección de los derechos y libertades de las personas físicas con respecto al tratamiento de datos. Igualmente, se le asigna la función de cooperación con otras autoridades de control en el intercambio de información y de prestar asistencia mutua con el objetivo de velar por la coherencia en la aplicación de la Directiva.

Por último, en relación al contenido del artículo 46, es necesario aludir a la obligación impuesta a la autoridad de control de proporcionar a la persona interesada toda la información necesaria referente al curso de su reclamación que, en relación con el tratamiento de datos personales conozca la autoridad de control, así como de informar igualmente a la persona interesada sobre el curso y el resultado de la investigación así como de la necesidad de realizar nuevas investigación o una coordinación más estrecha con la autoridad de control, lo cual nos parece adecuada al suponer una garantía

69 Vid. Sentencia del Tribunal de Justicia de 6 de octubre de 2015, Asunto C- 362/14, caso Schrems, nos. 40, 41 y 42. Precisa el Tribunal qué para garantizar esa protección, las autoridades naciones de control han "de lograr un justo equilibrio entre el respecto del derecho fundamental a la vida privada y los intereses que exigen la libre circulación de datos personales".

que se otorga al titular de los datos objeto de tratamiento de estar informado en cualquier momento del curso de su solicitud.

La creación de esta autoridad de control contemplada ya en la Directiva 95/46/UE y en respuesta a lo establecido en su artículo 28 y consecuencia de la transposición a los distintos ordenamientos internos de los Estados miembros, se instituye en Italia la figura del "Garante per la protezione dei dati personale"[70]. El artículo 154 del Códice de la Privacy precisa las funciones a desarrollar, entre las que destaca la de controlar que el tratamiento de datos personales se haya efectuado con respeto lo establecido en la propia normativa y de conformidad a la notificación (artículos 37-38 códice de la privacy), así como en lo relativo al cese y a la conservación de los datos de tráfico, examinar todas las reclamaciones y señalizaciones así como resolver sobre los recursos presentados tanto por los propios interesados o por parte de las asociaciones que les representan; prescribir de oficio a los titulares del tratamiento de datos las medidas de seguridad necesarias con la finalidad de que el tratamiento se adapte a las disposiciones vigentes, así como manifestar sus opiniones en los casos previstos. El garante tiene la obligación de elaborar anualmente un informe sobre las actividades desarrolladas y su actuación acorde a lo determinado en el Códice de la Privacy, con la obligación de presentar dicho informe al Parlamento y al Gobierno[71].

Por lo que respecta al ordenamiento jurídico español y también como consecuencia de la transposición de la Directiva 95/46/UE, la autoridad independiente viene determinada en la Agencia de protección de datos. La LO 15/1999[72] regula el Derecho Fundamental a la protección de datos y dispone que será la Agencia Española de protección de datos la encargada de tutelar y garantizar dicho derecho. El Director de la Agencia de Protección de Datos dirige la Agencia y ostenta su representación, ejerciendo sus funciones con plena independencia y objetividad, destacando entre sus funciones la de velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos así como emitir cuantas autorizaciones previstas en la Ley y dictar las instrucciones precisas para adecuar los tratamientos a los principios de la presente Ley. Otras de las funciones que tiene encomendadas hace referencia a las peticiones y reclamaciones formuladas por las personas afectadas así como la obligación de informar a todas aquellas personas que reclamen información acerca de sus derechos en materia de tratamiento de los datos de carácter personal y la potestad sancionadora[73] que le faculta la ley conforme a los parámetros establecidos en el Título VII de la presente Ley[74].

En lo que respecta a las facultades asignadas a estas autoridades independientes de control, es de destacar la de transmisión de datos a terceros países, función que realmente no viene establecida en el artículo 28 pero que se deduce del propio artículo 28 de la Directiva y del Considerando 60, al precisar que las "transferencias de datos personales hacia terceros países solo podrán efectuarse si se respetan plenamente las disposiciones adoptadas por los Estados miembros en aplicación de la misma Directiva"[75].

Habrá que esperar a la transposición de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, si otorga a este organismo nuevas funciones que den cobertura al contenido de la propia Directiva de forma que garantice su aplicación o se procederá a la creación de otra autoridad de control, en respuesta a lo establecido en el artículo 41.3: "Los Estados miembros podrán disponer que una autoridad de control creada en virtud del Reglamento (UE) 2016/679 pueda ser la autoridad de control mencionada en la presente Directiva y asuma la responsabilidad de las funciones de la autoridad de control que vayan a crearse de conformidad con el apartado 1 del presente artículo". Como se sabe, la Directiva debe ser transpuesta a más tardar el 6 de mayo de 2018 y en lo que respecta al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a

70 Garante Europeo de la protección de datos (GEPD) en la literatura italiana, vid. Pocar/Baruffi, (2014): *Commentario breve ai Trattati…,* op. cit., p. 191.

71 Artículo 154 del Códice de la Privacy, antes del 30 de abril del año sucesivo al cual se refieren las actuaciones de la autoridad.

72 LO 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, (LOPD) (BOE núm. 298, de 14 de diciembre de 1999. Vid. Igualmente el Real Decreto 1720/2007, de 21 de diciembre de desarrollo de la Ley Orgánica de Protección de Datos. Se trata de un desarrollo de la Ley Orgánica 15/99 de Protección de Datos de 13 de diciembre;

73 Para más detalles acerca de la Ley de Protección de datos, nos remitimos, entre otros a: Aparicio Salom, J., (2002): *Estudio sobre la Ley Orgánica de Protección de Datos…*, op. cit; Lesmes Serrano, C., (Coord.), (2008): *La Ley de Protección de Datos. Análisis y Comentario de su Jurisprudencia.* Lex Nova,

74 Artículo 37 de la LO de Protección de datos.

75 Sentencia del Tribunal de Justicia de 6 de octubre de 2015, Asunto C- 362/14, caso Schrems, de tal forma que conforme al artículo 25, las autoridades de control independientes han de asumir el control del cumplimiento de las reglas de la Unión para la protección de las personas físicas frente a tratamiento de datos personales, asumen la competencia de determinar si una transferencia de datos personales a un tercer país respeta las exigencias determinadas por la Directiva.

la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), en el artículo 94 se precisa que la Directiva 95/46/CE queda derogada con efecto a partir del 25 de mayo de 2018.

4. Reflexión final.

A lo largo del presente trabajo, se han ido exponiendo los avances normativos que en materia de protección de datos personales ha ido realizando la Unión, dirigiendo sus esfuerzos en la obtención del establecimiento de un marco sólido y coherente, de contornos propios, en materia de protección de datos personales en el denominado espacio de libertad, seguridad y justicia. La utilización y distribución de datos personales para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, pueden incrementar la vulnerabilidad de los derechos de la persona, entre ellos el derecho a la protección de datos personales, lo que justifica la adopción de normas específicas encaminadas a regular los principios y derechos sobre protección de datos, y el papel de las autoridades de control, en el marco de la cooperación judicial y policial, así como en las investigaciones y los procesos penales nacionales. A ello responde la Directiva (UE) 2016/680, objeto de análisis en las presentes líneas, instrumento que va a contribuir sin duda alguna a sustentar el equilibrio entre la eficacia de las investigaciones y los procesos penales, por un lado, y los derechos de los sospechosos y acusados, incluido su derecho a la protección de datos, por otro.

No obstante, sin dejar de admitir que el tratamiento automatizado de datos personales ha sido en los últimos tiempos objeto de una especial atención, tanto por parte del Derecho internacional como comunitario e interno de los Estados miembros de la Unión como lo reflejan los distintos instrumentos elaborados al respecto, el resultado era insuficiente antes de la entrada en vigor del Tratado de Lisboa en lo que atañe a la protección de los derechos mencionados en el ámbito de las investigaciones policiales y los procesos penales, incluida la cooperación policial y judicial. En efecto, antes de la entrada en vigor del Tratado de Lisboa no había base jurídica para armonizar las legislaciones nacionales de los Estados miembros en lo que se refería al intercambio de información entre autoridades nacionales, tan sólo en el ámbito de la cooperación policial y judicial. Además, durante décadas la inercia del legislador europeo ha sido incluir normas específicas sobre tratamiento y protección de datos en cada instrumento jurídico por el que se creaba una base de datos particular, por lo que había una gran dispersión normativa, además de regular algunos aspectos (como la transferencia de datos a terceros países y organizaciones internacionales) de manera notablemente distinta en unos y otros instrumentos. Así, por ejemplo, SIS-II tiene sus propias normas sobre intercambio de información contenidas en el Reglamento (CE) n. 1987/2006 y la Decisión 2007/533/JAI, y el artículo 39 relativo a la transferencia de datos personales a terceras partes dispone que "Los datos tratados en el SIS II en virtud del presente Reglamento no se transferirán a terceros países ni a organizaciones internacionales, ni se pondrán a su disposición". Disposiciones que son distintas a las del sistema Prüm, en donde se establece en relación con el tratamiento de datos de carácter personal transmitidos o que se transmitan en virtud del presente Tratado, que cada Estado parte garantizará que su derecho interno ofrezca un nivel de protección de datos equivalente como mínimo al que resulta del Convenio del Consejo de Europa de 28 de enero de 1981 o, el sistema ECRIS, regulado por la Decisión 2009/315/JAI de 26 Febrero, relativa a la organización y al contenido del intercambio de información de los registros de antecedentes penales entre los Estados miembros y que regula únicamente el **in**tercambio de información de los registros de antecedentes penales entre los Estados miembros

Sólo a partir de la entrada en vigor del Tratado de Lisboa, y tomando como base jurídica el artículo 16 TFUE, ha sido posible adoptar un instrumento jurídico UE que dispone normas mínimas comunes sobre protección de datos en los ámbitos policial y judicial, tanto en lo que se refiere a los intercambios de información entre Estados Miembros (cooperación policial y judicial UE) como a nivel nacional (investigaciones policiales nacionales, proceso penal). Este nuevo instrumento jurídico (la Directiva 2017/680), incluye también normas comunes para el intercambio de información entre los Estados miembros UE y terceros países y organizaciones internacionales.

Si bien hemos de destacar que ha sido un proceso lento y gradual, el resultado ha sido satisfactorio con el establecimiento de un marco propio de protección de datos personales, requisito indispensable y necesario para poder intercambiar información entre los Estados miembros, y también con terceros países y organizaciones internacionales, en ámbitos tan decisivos como la lucha contra el terrorismo y la delincuencia organizada. Así, la nueva Directiva supone un avance muy importante en la consolidación del espacio de libertad, seguridad y justicia[76].

76 Objetivo pretendido por la propia Unión, tal y como dispone la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, bajo el título "Garantizar el espacio de libertad,

No obstante, la regulación de la transmisión de datos a un tercer país u organización internacional presenta algunas deficiencias en su contenido debido a la imprecisión de algunos términos como, por ejemplo, "amenaza", "gravedad" y "nivel adecuado". Habrá que esperar a la implementación de la Directiva en los Estados Miembros y su posterior aplicación por los órganos judiciales para conocer cómo dichos órganos interpretan los conceptos de "amenaza", "gravedad" y "nivel adecuado", entre otros. En esta labor interpretativa, y como criterio novedoso a tener en cuenta, los tribunales podrían tener en cuenta los dictámenes elaborados por las Autoridades de Control de Datos (artículo 35), y del Comité Europeo de Protección de Datos (artículo 51 en relación con el Reglamento 2016/679).

Hemos de precisar que, en nuestra opinión, la Directiva debe de otorgar un mayor protagonismo a las autoridades de control en la función de evaluación de los requisitos bajo los cuales se permite el intercambio de los datos personales a un tercer país u organización internacional. En esta función evaluadora consideramos esencial la implicación de la autoridad de control, especialmente en los supuestos de transferencias no basadas en una decisión de adecuación ni en la existencia de garantías adecuadas. Excepciones que, tal y como indica la Directiva en cuestión se deben interpretar de forma restrictiva, no obstante, consideramos que la intervención en estos supuestos de la autoridad de control conllevaría una consolidación de las garantías del derecho a la protección de datos personales.

Es verdad que en estos casos debe de informarse a las autoridades de control de las transferencias realizadas, pero esta comunicación es siempre posterior a la transmisión de los datos.

Así, el artículo 38.1 de la Directiva, tal y como ya se ha expuesto, dispone que, en ausencia de una decisión de adecuación o de garantías apropiadas pueden realizarse transferencias de datos a terceros países siempre que se cumplan determinados requisitos, expresamente previstos en el apartado (1), que habrán de interpretarse restrictivamente, y además, dichas transmisiones "deberán documentarse y la documentación se pondrá a disposición, previa solicitud, de la autoridad de control, con inclusión de la fecha y la hora de la transferencia, información sobre la autoridad competente destinataria, la justificación de la transferencia y los datos personales transferidos".

Y el artículo 39, 3 de la Directiva prevé que, en los casos de transmisión de datos personales a destinatarios específicos establecidos en terceros países, "la autoridad competente de la transferencia informará a la autoridad de control acerca de las transferencias efectuadas a tenor del presente artículo".

Como he señalado, en ambos casos la intervención de la autoridad de supervisión es posterior a la transmisión. Su participación en un momento anterior supondría una mayor garantía para los ciudadanos.

En estos supuestos, el papel de las autoridades de control permitiría, por ejemplo, evitar que si un Estado miembro tiene un nivel superior de garantías relativas al derecho fundamental a la protección de datos que el que determina la propia Unión en relación a lo que considera "nivel adecuado", esto es, nivel mínimo de protección, el Estado miembro pudiera transferir los datos de los sujetos que forman parte en una investigación criminal y cuyos datos van a ser transferidos, renunciando así a algunas de las garantías que el ordenamiento jurídico de su Estado reconoce en el ámbito de la investigación penal. En este contexto, el papel que puede desarrollar la autoridad de control en la función de evaluación del nivel de garantías me parece fundamental para afianzar los niveles de protección del derecho fundamental a la protección de los datos personales.

Notas bibliográficas.

Aparicio Salom, J. (2002): *Estudio sobre la Ley Orgánica de Protección de Datos de carácter Personal,* Ed. Aranzadi,

Arenas Ramiro, M. (2006): *El Derecho Fundamental a la protección de datos personales en Europa,* Tirant Lo Blanch, pp. 151-152.

Bayo Delgado, (2008): "La cooperación judicial internacional a la luz de la propuesta revisada de la Decisión Marco relativa a la protección de datos", *La protección de datos en la cooperación policial y judicial*, Aranzadi, pp. 28 y ss

Bru Cuadrada, E. (2007): "La protección de datos en España y en la Unión Europea. Especial referencia a los mecanismos jurídicos de reacción frente a la vulneración del derecho a la intimidad", *Revista de Internet, Derecho y Política*, nº 5, pp. 1 y ss.

seguridad y justicia para los ciudadanos europeos", presentada en Bruselas el 20 de Abril de 2010, COM (2010) 171 final, Plan de Acción por el que se aplica el Programa de Estocolmo, p. 3, donde se compromete la Unión a reforzar la posición de la UE en cuanto a la protección de los datos personales en el contexto de todas las políticas de la UE, incluida la represión policial y la prevención de la delincuencia, así como en materia de relaciones internacionales.

Cabezudo Bajo, Mª . J. (2008): "La protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal", *La Justicia y la Carta de Derechos Fundamentales de la Unión Europea,* de la Oliva Santos, A. (Dir.), Aguilera Morales, M./Cubillo López, I. (Coords.), Colex, pp. 327- 342.

Davara Rodríguez, M.A. (1998): *La protección de datos en Europa: principios, derechos y procedimiento*, Universidad Pontificia de Comillas, pp. 29 y ss.

De la Cuesta Arzamendi, J.L. (Dir.). De la Mata Barranco, N., (Coord.), (2010): *Derecho Penal informático,* Aranzadi.

Díaz Barrado, C.M. (2012): "La dispersión y sectorización de los derechos humanos en el seno de la Unión Europea", *Estudios de derecho internacional y de derecho europeo en homenaje al profesor Manuel Pérez González,* Coord. Aznar Gómez y otros, Vo. I, (Tomo I), Tirant Lo Blanch, pp. 1453-1474.

Estadella Yuste, O. (1995): *La protección de la intimidad frente a la transmisión internacional de datos personales,* Centre d'Investigació de la Comunicació, Generalitat de Catalunya, Tecnos, pp. 64-68.

Etxebarria Juridi, J.F. (2009): "Principio de disponibilidad y protección de datos personales: a la búsqueda del necesario equilibrio en el espacio judicial penal europeo", Eguzkilore, nº 23, San Sebastián, Diciembre, pp. 351 – 366

Fabio di Resta, (2000): *Protezione delle informazione, Privacy e sicurezza,* G. Giappichelli Edotpre, Torino, pp. 3 y ss.

Fernández Teruelo, J.G. (2007): *El Cibercrimen. Los delitos cometidos a través de internet,* Dykinson.

Frigols i Brines, E. (2010): "La protección constitucional de los datos de las comunicaciones y del derecho a la intimidad a la luz del uso de las nuevas tecnologías", *La protección jurídica de la intimidad*, Boix Reig, J, (Dir.)/Jareño Real, A. (Coord.), Iustel, pp. 37 y ss.

Galán Muñoz, A. "¿Nuevos riesgos, viejas respuestas? Estudio sobre la protección de los datos de carácter personal ante las nuevas tecnologías de la información y la comunicación", *Revista General de Derecho penal,* 19, 2013, pp. 1 y ss.

Galán Muñoz, A. (2004), Libro Colectivo: *Derecho a la intimidad y nuevas tecnologías*, Gómez Martínez, C., (Dir.), CGPJ, Centro de Documentación Judicial, 2004, pp. 1 y ss.

Garzón Clariana, G. (1981): "La protección de los datos personales y la función normativa del Consejo de Europa", *Revista de Instituciones Europeas,* V. 8, nº 1, Enero-Abril, pp. 9-25, (esp. pp. 13-14).

Gordini, G., (2006): "Societá dell?informazione e diritti Constituzionali", *La Societá dell'informazione: libertá, pluralismo, risorce*, A cura di G. Gindi, Torino, pp. 67 y ss.

Guichot, E. (2005): *Datos personales y Administración Pública,* Thomson-Civitas, pp. 61 y ss.

Gutiérrez Castillo, V.L. (2005): "Aproximación a la protección jurídica internacional del derecho de acceso y protección de datos en Europa", *Derecho y conocimiento: anuario jurídico sobre la sociedad de la información y del conocimiento,* nº 3, pp. 31-49.

Lazpita Gurtubay, M. (1994): "Análisis comparado de las legislaciones sobre protección de datos de los Estado miembros de la Comunidad Europea", *Informática y Derecho,* nº 6-7, pp. 397-420, (esp. pp. 409-416).

Lesmes Serrano, C., (Coord.), (2008): *La Ley de Protección de Datos. Análisis y Comentario de su Jurisprudencia.* Lex Nova.

López Ortega, J.J. (2004): "Intimidad informática y Derecho Penal. (La protección penal de la intimidad frente a las nuevas tecnologías de la información y comunicación)", *Derecho a la intimidad y nuevas tecnologías*, Cuadernos de Derecho Judicial, IX, pp. 109-142 (esp. pp. 109-115.

Martínez Martínez, R. (2004): *Una aproximación crítica a la autodeterminación informativa,* Thomson-Civitas, pp. 23-57.

Martínez Martínez, R. (2007): "El derecho fundamental a la protección de datos: perspectivas", Revista de Internet, Derecho y Política, nº 5, pp. 47-61.

Morant Vidal, J. (2003): *Protección penal de la intimidad frente a las nuevas tecnologías (estudio de los artículos 197 a 201 del Código Penal),* Tirant Lo Blanch.

Mucciarelli, F. (2004): "Informatica e tutela penale della riservatezza", *Il diritto penale dell'informatica nell' época di Internet,* a cura di L. Picotti, Padova, pp. 173-181.

Murillo de la Cueva, P.L. (2007): "Perspectivas del derecho a la autodeterminación informativa", *Revista de Internet, Derecho y Política,* nº 5, pp. 18-32 (esp. pp. 19-22).

Murillo de la Cueva, P.L./Piñar Mañas, J.L. (2009): *El derecho a la autodeterminación informativa,* Fundación Coloquio Jurídico Europeo, Madrid**.**

Nino, M. (2012): *Terrorismo internazionale, privacy e protezione dei dati personali***,** Ed. Scientifica, Napoli, pp. 66-73.

Pardolesi, R. (2003): "Dalla riservatezza alla protezione dei dati personali: una storia di evoluzione e discontinuità", in *Diritto alla riservatezza e circolazione dei dati personale*. A cura di Roberto Pardolesi, G, Giuffre editore, Volume primo, pp. 33-34.

Pariente De Prada, I. (2013): "La reforma de la protección de datos en el ámbito europeo", *El espacio de libertad, seguridad y justicia: Schengen y protección de datos,* Thomson- Aranzadi, pp. 121-146.

Picotti, L. (2004): "Sistematica dei reati informática, tecniche di formulazione legislativa e beni giuridice tutelati, *Il diritto penale dell'informaticaa nell'epoca di Internet,* a cura di L. Picotti, Padova, pp. 21-94.

Pocar/Baruffi, (2014): *Commentario breve ai Trattati dell'Unione Europea,* Cedam, 2ª edizione, pp. 189-198.

Ruiz Miguel, C. (2003): «El derecho a la protección de datos personales en la Carta de Derechos Fundamentales de la Unión Europea», *Revista de Derecho Comunitario Europeo,* núm. 14, pp. 11-12.

Téllez Aguilera, A. (2001): *Nuevas tecnologías. Intimidad y Protección de datos. Estudio sistemático de la Ley Orgánica 15/1999*, Edisofer, S.L., pp. 21 y ss.

Téllez Aguilera, A. (2002): *La protección de datos en la Unión Europea. Diligencias normativas y anhelos unificadores*, Edisofer S.L. pp. 26 y ss.

Zaballos Pulido, E. (2013): *La protección de datos personales en España: evolución normativa y criterios de aplicación*, Memoria presentada para optar al Grado de Doctor, Universidad Complutense de Madrid, pp. 98 y ss.