UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA
FACULTAD DE DERECHO
DEPARTAMENTO DE DERECHO CONSTITUCIONAL

TESIS DOCTORAL

LAS TRANSFERENCIAS INTERNACIONALES DE DATOS EN LA NORMATIVA ESPAÑOLA Y COMUNITARIA

Autor: Vicente Guasch Portas
Licenciado en Derecho

2013

UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA
FACULTAD DE DERECHO
DEPARTAMENTO DE DERECHO CONSTITUCIONAL

TESIS DOCTORAL

LAS TRANSFERENCIAS INTERNACIONALES DE DATOS EN LA NORMATIVA ESPAÑOLA Y COMUNITARIA

Autor: Vicente Guasch Portas
Licenciado en Derecho

Director de la Tesis: Doctor Lucrecio Rebollo Delgado

Agradecimientos:

Mi agradecimiento y aprecio al Doctor Lucrecio Rebollo Delgado por compartir su saber y orientarme en este trabajo. Gracias a su apoyo se ha hecho posible esta tesis.

ÍNDICE

ABREVIATURAS Y SIGLAS

ADAMS	Anti-Doping Administration and Management System
AEPD	Agencia Española de Protección de Datos
AMA	Agencia Mundial Antidopaje
API	Información anticipada sobre pasajeros
Art.	Artículo/s
BOE	Boletín Oficial del Estado
BCR	Reglas o Normas Corporativas Vinculantes
CE	Comunidad Europea
CNIL	Comisión Nacional de Informática y Libertades (Francia)
Convenio 108	Convenio nº 108 del Consejo de Europa, de 28 de enero de 1981, para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal
Directiva	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 Éstos
DOCE	Diario Oficial de las Comunidades Europeas
DOUE	Diario Oficial de la Unión Europea
EEE	Espacio Económico Europeo
Grupo de Trabajo	Grupo de Trabajo sobre Protección de Datos del artículo 29 de la Directiva 95/46/CE
ICO	Oficina del Comisionado de Información (Reino Unido)
Instrucción 1/2000	Instrucción 1/2000, de 1 de diciembre, de la Agencia de Protección de Datos, relativa a las normas por las que se rigen los movimientos internacionales de datos (BOE de 16-12-2000)
LOPD	Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal

LORTAD	Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal
LRJAP	Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común
OAD	Organizaciones Antidopaje
OCDE	Organización para la Cooperación y el Desarrollo Económico
ONAD	Organizaciones Nacionales Antidopaje
ONU	Organización de las Naciones Unidas
PIPEDA	Personal Information and Electronic Documents Act (Canadá)
PNR	Registros de nombres de los pasajeros
RD	Real Decreto
RGPD	Registro General de Protección de Datos
RLOPD	Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal
SOX	Ley Sarbanes-Oxley (EE.UU.)
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TFUE	Tratado de Funcionamiento de la Unión Europea
TUE	Tratado de la Unión Europea
UE	Unión Europea

CAPÍTULO I

CONTEXTO JURÍDICO NACIONAL Y EUROPEO SOBRE PROTECCIÓN DE DATOS

1. CUESTIONES PREVIAS

La protección de datos de carácter personal es un campo del derecho de nacimiento muy reciente. Ha sido en los últimos años cuando ha aparecido la necesidad de proteger jurídicamente a las personas en lo que respecta al tratamiento de sus datos personales.

En nuestro país se recoge esta preocupación en el artículo 18.4 de la Constitución Española de 1978: "La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

El desarrollo del artículo 18.4 de la Constitución se efectuó a través de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD). Esta ley estuvo vigente hasta el 14 de enero de 2000, fecha en la que entró en vigor su sucesora: la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD).

La LORTAD se inspiró en dos fuentes principales:

- El Convenio nº 108 del Consejo de Europa, de 28 de enero de 1981, para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal.
- El Proyecto 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 y a la Libre Circulación de estos Datos (que años después acabaría convirtiéndose en la Directiva 95/46/CE).

La LOPD es fruto de la obligada transposición de la Directiva 95/46/CE, si bien en su redacción conserva intacto mucho del contenido de la LORTAD.

Si nos centramos en la primera de las dos normas foráneas antes mencionadas, el Convenio nº 108 del Consejo de Europa, fue firmado por España el 28 de enero de 1982 y ratificado mediante Instrumento de 27 de enero de 1984.

La segunda de las normas, la Directiva 95/46/CE, al igual que todas las de su tipo, en principio no tienen efecto directo. Son los países de la UE quienes deben desarrollar normativa interna que las transponga. En España, como hemos indicado anteriormente, se efectuó dicha transposición por medio de la LOPD (y como veremos en su momento, de forma poco afortunada en alguno de sus puntos).

Además de las normas jurídicas antes expuestas, es necesario mencionar que la protección de datos personales ha logrado el estatus de derecho fundamental en la Unión Europea a través de la Carta de los Derechos Fundamentales de la Unión Europea[1]. Su artículo 8 tiene el siguiente contenido:

"1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.
2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación.
3. El respeto de estas normas estará sujeto al control de una autoridad independiente".

[1] DOUE C 83 de 30 de marzo de 2010.

Una regulación similar la encontramos en el artículo 16 del Tratado de Funcionamiento de la Unión Europea.

2. PRINCIPIOS DE PROTECCIÓN DE DATOS

El régimen de protección de datos implantado por el Convenio 108 se basa, de acuerdo a Ruiz Miguel[2], en los siguientes principios:

- Principio de consentimiento. Derecho a cancelar aquellas informaciones que el interesado no desea que sigan figurando en un fichero.
- Principio de información. Derecho a conocer los datos del interesado que obran en el fichero.
- Principio de control. De este principio se desglosan los derechos a la rectificación de datos erróneos y a la cancelación de los poseídos irregularmente y a disponer de un recurso para hacer efectivas las pretensiones del interesado.
- Principio de calidad y lealtad. Los datos serán exactos y actualizados. Se obtendrán y tratarán lealmente y de forma proporcionada a la finalidad para la que se recogieron.
- Principio de seguridad y confidencialidad en el tratamiento de los datos.

La Directiva 95/46/CE (y la LOPD como norma de transposición) ha precisado y ampliado los citados principios. El principio de consentimiento pasa a operar también en el momento inicial, de forma que el tratamiento de datos sólo puede iniciarse si el interesado otorga su consentimiento. El principio de información también exigirá que el

[2] RUIZ MIGUEL, C: "El derecho a la protección de los datos personales en la Carta de Derechos Fundamentales de la Unión Europea: análisis crítico". Revista de Derecho Comunitario Europeo. Año 7. Núm. 14. Enero-Abril 2003. Pág. 33.

responsable del tratamiento informe al interesado sobre los datos que posea acerca de él. El principio de control se ve mejorado al facilitar la posibilidad de tener un recurso y configurar el derecho de oposición incluso como un derecho gratuito, además de establecer un organismo independiente con poderes inspectores y sancionadores. El principio de calidad y lealtad, así como el de seguridad y confidencialidad, se detallan en mayor medida.

3. EL MOVIMIENTO INTERNACIONAL DE DATOS

La estructura jurídica implantada en la Unión Europea puede llevar a unos resultados satisfactorios en el mercado interior en materia de protección de datos. Sin embargo todo el sistema puede carecer de eficacia si no se establecen mecanismos que contemplen el movimiento internacional de datos con terceros países. La normativa de la UE en el campo de la protección de datos es la más exigente del planeta. En cambio hay países con una regulación poco exigente, o incluso sin regulación de ningún tipo. Estas diferencias pueden conducir a que la protección conseguida en el seno de la Unión se pierda en el momento en que los datos puedan ser localizados en naciones con un nivel inferior o completamente nulo de protección.

La solución no puede venir del bloqueo radical de los datos personales hacia el exterior. Cualquier economía moderna tiene la necesidad de poder transmitir datos personales hacia el exterior. No hacerlo así supone la asfixia de muchos sectores económicos, que si no pueden desarrollarse en el interior de la Unión buscarán otras ubicaciones más favorables en el mundo, con lo que ello representa de menor riqueza y empleo.

Por las razones mencionadas la Directiva 95/46/CE y las leyes de transposición de los países de la UE han tenido que afrontar el movimiento internacional de datos hacia países terceros. Como bien señala el artículo 25.1 de la Directiva, únicamente podrá efectuarse una transferencia internacional de datos cuando "el país tercero de que se trate garantice un nivel de protección adecuado". Esta prohibición es mucho más dura de lo que podría parecer, ya que el grupo de países que han conseguido un nivel de protección reconocido como adecuado, es muy reducido: Suiza, Estados Unidos (principios de puerto seguro), Canadá (en cuanto a su *Personal Information and Electronic Documents Act*), Argentina, Guernesey, Isla de Man, Jersey, Islas Feroe, Andorra, Israel, Uruguay y Nueva Zelanda. Tampoco se espera que esta lista tenga mucho crecimiento en el medio plazo.

Si nos quedásemos solamente con el contenido del artículo 25.1, el movimiento de datos hacia el exterior de la Unión sería extremadamente limitado. La mayor parte de los países, entre los que se encuentran las nuevas potencias emergentes como China, India, Brasil o Rusia, quedan fuera de la relación antes citada de países. Pero el artículo 26 de la Directiva abre la puerta a una serie de excepciones que permitirán la transferencia de datos personales a países que no garanticen un nivel de protección adecuado. El primer conjunto de excepciones lo encontramos en el artículo 26.1 de la Directiva. Sin pretender ser exhaustivos ni profundizar en este punto en dichas excepciones, se podrá efectuar una transferencia siempre y cuando se cuente con el consentimiento inequívoco del interesado o cuando en su interés sea necesaria la transferencia para la celebración o ejecución de un contrato o para la salvaguarda de un interés público importante o para la salvaguardia del interés vital del interesado.

En el artículo 26.2 se aporta una nueva vía para poder efectuar una transferencia internacional de datos personales a un país que no garantice un nivel de protección adecuado: cuando el responsable del tratamiento ofrezca garantías suficientes respecto de la protección de la vida privada, de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los respectivos derechos. En particular estas garantías podrán derivarse de cláusulas contractuales apropiadas. Como se verá en el momento oportuno, existe otra figura no recogida en el texto de la Directiva de la que se espera un desarrollo importante en el futuro. Son las reglas o normas corporativas vinculantes. Esta figura ya se recoge extensamente en la propuesta de nuevo Reglamento de la UE relativo a la protección de datos[3]. Pero además de las cláusulas contractuales y de las normas corporativas vinculantes, incluso en la propuesta de Reglamento (considerando 83) no se cierran las puertas a "otras medidas adecuadas y proporcionadas que se justifiquen a la luz de todas las circunstancias que rodean la operación de transferencia de datos o las operaciones de transferencia de conjuntos de datos y siempre que las autorice una autoridad de control".

No podemos dejar sin comentar la ruptura de los esquemas tradicionales que ha supuesto la expansión de Internet. La Directiva 95/46/CE y las normas nacionales de transposición han regulado sobre una concepción de la informática que no es la actual. Internet ha hecho aparecer nuevos tratamientos de datos que antes no existían: redes sociales, buscadores, *Cloud Computing*. En el caso de los servicios de *Cloud*

[3] *Propuesta de 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 (Reglamento general de protección de datos)*. Bruselas, 25.1.2012 COM (2012) 11 final.

Computing, los beneficios que comportan a los usuarios pueden ser muy grandes, pero los problemas en el ámbito de la protección de datos personales también son de gran magnitud. Los servicios de *Cloud Computing* generalmente son deslocalizados. Además los datos se pueden mover de una punta a la otra del globo terráqueo con gran frecuencia, habitualmente a países que no proporcionan un nivel adecuado de protección. La LOPD (al igual que la Directiva 95/46/CE) califica estas transmisiones de datos a países terceros como transferencias internacionales de datos, y por lo tanto sería necesaria la autorización del Director de la AEPD. No contar con esta autorización (cosa harto frecuente en la práctica) supone una infracción calificada como muy grave, sancionada con multa de 300.001 a 600.000 euros.

4. NORMATIVA BÁSICA

La protección de datos de carácter personal es un campo del derecho de nacimiento muy reciente. Su desarrollo ha estado muy ligado a la evolución de la informática. La posibilidad de almacenar cantidades masivas de datos y de gestionarlos de forma automatizada ha obligado a que surgiese un nuevo derecho para la protección de los datos de carácter personal. Y ello además en un periodo de tiempo muy breve.

Si hacemos una breve historia de la evolución de esta normativa podríamos centrarnos en las normas europeas y españolas fundamentales en esta materia. En el plano del Consejo de Europa destaca el Convenio 108 y en la UE la Directiva 95/46/CE. En el campo español destacan la LORTAD (Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal), la LOPD (Ley Orgánica de Protección de Datos de Carácter Personal) y el RLOPD (Reglamento de desarrollo de la LOPD).

4.1. EL CONVENIO 108 (CONSEJO DE EUROPA)

Como bien señala Rebollo Delgado, "la inquietud de las organizaciones supranacionales por el respeto a los derechos de la personalidad, así como por las disfunciones sociales que los nuevos medios tecnológicos pueden producir, tuvo su plasmación en el Convenio nº 108 del Consejo de Europa"[4].

El Convenio nº 108, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, fue firmado por España el 28 de enero de 1982, y ratificado el 27 de enero de 1984. De acuerdo a lo dispuesto en el artículo 22.2 del Convenio, éste entró en vigor de forma general y para España el 1 de octubre de 1985[5].

Un aspecto que se ha criticado del Convenio es que no puede ser objeto de aplicación directa. Tal como se establece en su artículo 4.1, "cada Parte tomará, en su derecho interno, las medidas necesarias para que sean efectivos los principios básicos para la protección de datos enunciados en el presente capítulo". Si dicha regulación en la normativa interna no se lleva a efecto nadie podrá reclamar un derecho en base al propio texto del Convenio. Así lo entiende el Tribunal Constitucional en su Sentencia de 20 de julio de 1993[6].

[4] REBOLLO DELGADO, L: *Vida Privada y Protección de Datos en la Unión Europea*. Dykinson. Madrid 2008, p. 106.

[5] Véase en el BOE de 15 de noviembre de 1985 el texto completo del Convenio nº 108, así como el Instrumento de Ratificación por parte de España.

[6] Sentencia publicada en el BOE de 18 de agosto de 1993.

Como señala el Considerando segundo del Convenio, “es deseable ampliar la protección de los derechos y de las libertades fundamentales de cada uno, concretamente el derecho al respeto de la vida privada, teniendo en cuenta la intensificación de la circulación a través de las fronteras de los datos de carácter personal que son objeto de tratamientos automatizados”.

Y en su artículo 1 se indica que el fin del Convenio “es garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona («protección de datos»)”.

El Convenio se aplica a los ficheros y a los tratamientos automatizados de datos de carácter personal en los sectores público y privado. Cada Parte se compromete a tomar en su derecho interno las medidas necesarias para que sean efectivos los principios básicos para la protección de datos enunciados en el Capítulo II del Convenio.

El artículo 5, sobre calidad de los datos, exige que los datos de carácter personal que sean objeto de un tratamiento automatizado:

“a) se obtendrán y tratarán leal y legítimamente;

b) se registrarán para finalidades determinadas y legítimas, y no se utilizarán de una forma incompatible con dichas finalidades;

c) serán adecuados, pertinentes y no excesivos en relación con las finalidades para las cuales se hayan registrado;

d) serán exactos y si fuera necesario puestos al día;

e) se conservarán bajo una forma que permita la identificación de las personas concernidas durante un período de tiempo que no exceda del necesario para las finalidades para las cuales se hayan registrado".

El artículo 6 tiene en consideración que hay categorías particulares de datos. Este tipo de datos (los que revelen el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud o a la vida sexual, o referentes a condenas penales), no podrán tratarse automáticamente a menos que el derecho interno prevea garantías apropiadas.

El artículo 7 obliga a tomar "medidas de seguridad apropiadas para la protección de datos de carácter personal registrados en ficheros automatizados contra la destrucción accidental o no autorizada, o la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizados".

En el artículo 8 se establece que cualquier persona concernida deberá poder:

"a) conocer la existencia de un fichero automatizado de datos de carácter personal, sus finalidades principales, así como la identidad y la residencia habitual o el establecimiento principal de la autoridad controladora del fichero;
b) obtener a intervalos razonables y sin demora o gastos excesivos la confirmación de la existencia o no en el fichero automatizado de datos de carácter personal que conciernan a dicha persona, así como la comunicación de dichos datos en forma inteligible;
c) obtener, llegado el caso, la rectificación de dichos datos o el borrado de los mismos, cuando se hayan tratado con infracción de las disposiciones del derecho

interno que hagan efectivos los principios básicos enunciados en los artículos 5 y 6 del presente Convenio;

d) disponer de un recurso si no se ha atendido a una petición de confirmación o, si así fuere el caso, de comunicación, de ratificación o de borrado, a que se refieren los párrafos b) y c) del presente artículo".

En el artículo 10 las Partes se comprometen a establecer sanciones y recursos convenientes contra las infracciones de las disposiciones de derecho interno que hagan efectivos los principios básicos para la protección de datos.

Y en el artículo 11 se da libertad a las Partes para conceder a las personas concernidas una protección más amplia que la prevista en el Convenio.

Para concluir, mencionar que el Capítulo III regula los Flujos Transfronterizos de Datos. Este apartado lo estudiaremos con detenimiento más adelante.

4.2. LA DIRECTIVA 95/46/CE (UNIÓN EUROPEA)

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.

La Directiva 95/46/CE se aplica a los datos tratados por medios automatizados así como a los datos contenidos en un fichero no automatizado. Así en su Considerando 15 entiende que también quedan amparados por la Directiva los datos que se encuentran contenidos o se destinan a encontrarse contenidos en un archivo estructurado según criterios específicos relativos a las personas, a fin de que se pueda acceder fácilmente a los datos de carácter personal de que se trata.

De acuerdo al artículo 3.2 las disposiciones de la Directiva no se aplicarán al tratamiento de datos personales efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas. Tampoco se aplicarán al ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho de la Unión, tales como la seguridad pública, la defensa o la seguridad del Estado.

La Directiva tiene como objetivo proteger los derechos y las libertades de las personas en lo que respecta al tratamiento de datos personales, estableciendo principios de orientación para determinar la licitud de dicho tratamiento. Dichos principios se refieren a:

- **La calidad de los datos**: los datos personales serán tratados de manera leal y lícita, y recogidos con fines determinados, explícitos y legítimos. Además, serán exactos y, cuando sea necesario, actualizados.
- **La legitimación del tratamiento**: el tratamiento de datos personales sólo podrá efectuarse si el interesado ha dado su consentimiento de forma inequívoca o si el tratamiento es necesario para:
    - la ejecución de un contrato en el que el interesado sea parte, o
    - el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento, o
    - proteger el interés vital del interesado, o
    - el cumplimiento de una misión de interés público, o
    - la satisfacción del interés legítimo perseguido por el responsable del tratamiento.

- **Las categorías especiales de tratamiento**: deberá prohibirse el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas y la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud (concepto de compleja delimitación, ya que existen datos como los genéticos, que tienen una difícil clasificación[7]) o a la sexualidad. Esta disposición va acompañada de reservas que se aplicarán, por ejemplo, en caso de que el tratamiento sea necesario para salvaguardar el interés vital del interesado o para la prevención o el diagnóstico médico.
- **La información a los afectados por dicho tratamiento**: el responsable del tratamiento deberá facilitar cierta cantidad de información (identidad del responsable del tratamiento, fines del tratamiento, destinatarios de los datos, etc.) a la persona de quien se recaben los datos que le conciernan.
- **El derecho de acceso del interesado a los datos**: todos los interesados deberán tener el derecho de obtener del responsable del tratamiento:
    - la confirmación de la existencia o inexistencia del tratamiento de datos que le conciernen y la comunicación de los datos objeto de los tratamientos;
    - la rectificación, la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la presente Directiva, en particular a causa del carácter incompleto o inexacto de los datos, así como la notificación a los terceros a quienes se hayan comunicado los datos de dichas modificaciones.

[7] GÓMEZ SÁNCHEZ, Y: "Los datos genéticos en el Tratado de Prüm". Revista de Derecho Constitucional Europeo nº 7, 2007, pág. 137-165.

- **Las excepciones y limitaciones**: se podrá limitar el alcance de los principios relativos a la calidad de los datos, la información del interesado, el derecho de acceso y la publicidad de los tratamientos con objeto de salvaguardar, entre otras cosas, la seguridad del Estado, la defensa, la seguridad pública, la represión de infracciones penales, un interés económico y financiero importante de un Estado miembro o de la UE o la protección del interesado.
- **El derecho del interesado a oponerse al tratamiento**: el interesado deberá tener derecho a oponerse, por razones legítimas, a que los datos que le conciernen sean objeto de tratamiento. También deberá tener la posibilidad de oponerse, previa petición y sin gastos, al tratamiento de los datos respecto de los cuales se prevea un tratamiento destinado a la prospección. Por último, deberá ser informado antes de que los datos se comuniquen a terceros a efectos de prospección y tendrá derecho a oponerse a dicha comunicación.
- **La confidencialidad y la seguridad del tratamiento**: las personas que actúen bajo la autoridad del responsable o del encargado del tratamiento, incluido este último, sólo podrán tratar datos personales a los que tengan acceso, cuando se lo encargue el responsable del tratamiento. Por otra parte, el responsable del tratamiento deberá aplicar las medidas adecuadas para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental, la alteración, la difusión o el acceso no autorizados.
- **La notificación del tratamiento a la autoridad de control**: el responsable del tratamiento efectuará una notificación a la autoridad de control nacional con anterioridad a la realización de un tratamiento. La autoridad de control realizará comprobaciones previas sobre los posibles riesgos para los derechos y

libertades de los interesados una vez que haya recibido la notificación. Deberá procederse a la publicidad de los tratamientos y las autoridades de control llevarán un registro de los tratamientos notificados.

En el artículo 22 se prevé que las legislaciones nacionales deben prever un **recurso judicial** para los casos en los que el responsable del tratamiento de datos no respete los derechos de los interesados. Los daños que pueden sufrir las personas a raíz de un tratamiento ilícito han de ser reparados por el responsable del tratamiento de datos.

El Capítulo IV regula las transferencias de datos a países terceros. Veremos posteriormente con mucho detalle cuando se autorizarán o no dichas transferencias.

En el artículo 28 se dispone que los Estados miembros dispondrán que una o más **autoridades públicas** se encarguen de vigilar la aplicación en su territorio de las disposiciones adoptadas por ellos en aplicación de la Directiva.

En el artículo 29 se crea el **Grupo de protección de las personas** en lo que respecta al tratamiento de datos personales, que tendrá carácter consultivo e independiente. El Grupo estará compuesto por un representante de la autoridad o de las autoridades de control designadas por cada Estado miembro, por un representante de la autoridad o autoridades creadas por las instituciones y organismos de la UE, y por un representante de la Comisión.

4.3. LA LORTAD

La LORTAD (Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal) ha estado vigente hasta el

14 de enero de 2000. A la fecha de publicación de esta norma, el Convenio nº 108 ya llevaba más de siete años en vigor, por lo que sin duda alguna fue una de sus fuentes de inspiración. Otra de las guías de referencia fueron los trabajos preparatorios del Proyecto 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 y a la Libre Circulación de estos Datos. La última de las fuentes es la Constitución Española.

En la Exposición de Motivos se señala que el "progresivo desarrollo de las técnicas de recolección y almacenamiento de datos y de acceso a los mismos ha expuesto a la privacidad, en efecto, a una amenaza potencial antes desconocida". Y destaca que se habla de la privacidad y no de la intimidad. La primera es más amplia que la segunda, pues en tanto la intimidad protege la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona, la privacidad constituye un conjunto más amplio de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, dibujan un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado. Y añade que "si la intimidad, en sentido estricto, está suficientemente protegida por las previsiones de los tres primeros párrafos del artículo 18 de la Constitución y por las leyes que los desarrollan, la privacidad puede resultar menoscabada por la utilización de las tecnologías informáticas de tan reciente desarrollo". Por dichos motivos la LORTAD, "en desarrollo de lo previsto en el apartado 4 del artículo 18 de la Constitución, tiene por objeto limitar el uso de la informática y otras técnicas y medios de tratamiento automatizado de los datos de carácter personal para garantizar el honor, la intimidad personal y familiar de las personas físicas y el pleno ejercicio de sus derechos".

En el artículo 2 de la LORTAD se regula su ámbito de aplicación: “los datos de carácter personal que figuren en ficheros automatizados de los sectores público y privado y a toda modalidad de uso posterior, incluso no automatizado, de datos de carácter personal registrados en soporte físico susceptible de tratamiento automatizado”. Sin embargo la ley no será de aplicación:

- A los ficheros automatizados de titularidad pública cuyo objeto, legalmente establecido, sea el almacenamiento de datos para su publicidad con carácter general.
- A los ficheros mantenidos por personas físicas con fines exclusivamente personales.
- A los ficheros de información tecnológica o comercial que reproduzcan datos ya publicados en boletines, diarios o repertorios oficiales.
- A los ficheros de informática jurídica accesibles al público en la medida en que se limiten a reproducir disposiciones o resoluciones judiciales publicadas en periódicos o repertorios oficiales.
- A los ficheros mantenidos por los partidos políticos, sindicatos e Iglesias, confesiones y comunidades religiosas en cuanto los datos se refieran a sus asociados o miembros y ex miembros, sin perjuicio de la cesión de los datos que queda sometida a lo dispuesto en el artículo 11 de esta Ley, salvo que resultara de aplicación el artículo 7 por tratarse de los datos personales en él contenidos.

El título II de la LORTAD (artículos 4 a 11) enumera los principios fundamentales de la protección de datos:

- *Calidad de los datos* (art. 4). Sólo se podrán recoger datos de carácter personal para su tratamiento automatizado, así como someterlos a dicho tratamiento, cuando tales datos sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades legítimas para las que se hayan obtenido. No podrán usarse para finalidades distintas de aquellas para las que hubieran sido recogidos. Serán exactos y puestos al día. Y serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados y registrados.

- *Derecho de información en la recogida de datos* (art. 5). Los afectados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

a. De la existencia de un fichero automatizado de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.
b. Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.
c. De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
d. De la posibilidad de ejercitar los derechos de acceso, rectificación y cancelación.
e. De la identidad y dirección del responsable del fichero.

- *Consentimiento del afectado* (art. 6). El tratamiento automatizado de los datos de carácter personal requerirá el consentimiento del afectado, salvo que la Ley disponga otra cosa.

- *Datos especialmente protegidos* (art. 7). Sólo con consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento automatizado los datos de carácter personal que revelen la ideología, religión y creencias. Los que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados automatizadamente y cedidos cuando por razones de interés general así lo disponga una Ley o el afectado consienta expresamente.

- *Seguridad de los datos* (art. 9). El responsable del fichero deberá adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

- *Deber de secreto* (art. 10). El responsable del fichero automatizado y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos.

- *Cesión de datos* (art. 11). Los datos de carácter personal objeto del tratamiento automatizado sólo podrán ser cedidos para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del afectado. El consentimiento exigido en el apartado anterior no será preciso:

a. Cuando una Ley prevea otra cosa.
b. Cuando se trate de datos recogidos de fuentes accesibles al público.

c. Cuando el establecimiento del fichero automatizado responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho fichero con ficheros de terceros.
d. Cuando la cesión que deba efectuarse tenga por destinatario el Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales, en el ejercicio de las funciones que tienen atribuidas.
e. Cuando la cesión se produzca entre las Administraciones Públicas en ciertos supuestos previstos en la ley.
f. Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero automatizado o para realizar estudios epidemiológicos.

El título III de la LORTAD (artículos 12 a 17) enumera los derechos de las personas con relación a sus datos tratados automatizadamente:

- *Impugnación de valoraciones basadas exclusivamente en datos automatizados* (art. 12). El afectado podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento cuyo único fundamento sea un tratamiento automatizado de datos de carácter personal.

- *Derecho de información* (art. 13). Cualquier persona podrá conocer la existencia de ficheros automatizados de datos de carácter personal, sus finalidades y la identidad del responsable del fichero.

- *Derecho de acceso* (art. 14). El afectado tendrá derecho a solicitar y obtener información de sus datos de carácter personal incluidos en los ficheros automatizados.

- *Derecho de rectificación y cancelación* (art. 15). El responsable del fichero tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del afectado.

- *Tutela de los derechos y derecho de indemnización* (art. 17). Las actuaciones contrarias a lo dispuesto en la Ley pueden ser objeto de reclamación por los afectados ante la Agencia de Protección de Datos. Quienes por dichas actuaciones sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados.

En el Título VI se crea la Agencia de Protección de Datos y se regulan sus funciones. Entre ellas podemos destacar las siguientes:

- 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 y cancelación de datos.
- Emitir las autorizaciones previstas en la Ley o en sus disposiciones reglamentarias.
- Dictar, en su caso y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos automatizados a los principios de la Ley.
- Atender las peticiones y reclamaciones formuladas por las personas afectadas.

- Proporcionar información a las personas acerca de sus derechos en materia de tratamiento automatizado de los datos de carácter personal.
- Ordenar la cesación de los tratamientos de datos de carácter personal y la cancelación de los ficheros, cuando no se ajusten a las disposiciones de la Ley.
- Ejercer la potestad sancionadora en los términos previstos por la Ley.

En el Título V se regula el Movimiento Internacional de Datos. Se prohíben las transferencias con destino a países que no proporcionen un nivel de protección equiparable, salvo que se obtenga autorización previa del Director de la Agencia de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas. Se contemplan algunas excepciones en las que esa prohibición no será aplicable:

- Cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de Tratados o Convenios en los que sea parte España.
- Cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional.
- Cuando la misma tenga por objeto el intercambio de datos de carácter médico o la investigación epidemiológica.
- Cuando se refiera a transferencias dinerarias conforme a su legislación específica.

4.4. LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL (LOPD)

Tras la aprobación de la Directiva 95/46/CE todos los países de la Unión Europea se vieron en la obligación de transponerla a su derecho interno. La Directiva tenía diferencias importantes con la LORTAD, optando el legislador no por efectuar

modificaciones sobre dicha norma sino por la elaboración de una norma nueva: la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

La LOPD coincide en buena parte de su contenido con el de la LORTAD. De las diferencias que encontramos entre ambas normas podríamos destacar:

- La LORTAD regulaba el tratamiento automatizado de datos, mientras que la LOPD extiende su campo a todo tipo de ficheros (ya estén en formato papel o en cualquier otro soporte). En el caso de ficheros no automatizados, la Disposición Adicional Primera de la LOPD exige su adecuación a las exigencias legales en el plazo de doce años a contar desde el 24 de octubre de 1995.

- Surge la figura del *encargado del tratamiento*, definido en el artículo 3 de la LOPD como "la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento".

- Uno de los supuestos de excepción al principio del consentimiento[8] para el tratamiento de los datos se da cuando los datos figuren en fuentes accesibles al público. En la LORTAD las fuentes accesibles al público no estaban definidas como una lista cerrada. En la LOPD (art. 3) las fuentes accesibles al público únicamente son: el censo promocional, los repertorios telefónicos, las listas de personas pertenecientes a grupos de profesionales, los diarios y boletines oficiales y los medios de comunicación.

[8] REBOLLO DELGADO, L y SERRANO PÉREZ, Mª. M: *Introducción a la protección de datos.* Dykinson. Madrid 2008, p. 124.

- En la nueva Ley los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades *incompatibles* con aquellas para las que los datos hubieran sido recogidos (art. 4.2). La LORTAD hablaba en cambio de finalidades *distintas*.

- La LOPD añade en la relación de los denominados "datos especialmente protegidos" los datos relativos a la afiliación sindical (art. 7). La nueva regulación no puede considerarse plenamente afortunada. Así, en opinión de Gómez Sánchez, la correcta definición y regulación de los datos genéticos precisa de una reforma de la LOPD "en la que se incluya un título específico dedicado a las diferentes categorías de datos sensibles"[9].

- Como novedad, se regula en el artículo 12 de la LOPD el *acceso a los datos por cuenta de terceros*. No se considera comunicación de datos el acceso de un tercero a los mismos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento.

- La LOPD regula los *tratamientos con fines de publicidad y de prospección comercial* (art. 30), para quienes se dediquen a la recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial y otras actividades análogas.

- Se regula el *censo promocional* (art. 31), formado con los datos de nombre, apellidos y domicilio que constan en el censo electoral.

[9] GÓMEZ SÁNCHEZ, Y: "La protección de los datos genéticos: el derecho a la autodeterminación informativa". Revista DS: Derecho y Salud, vol. 16 de 2008, pág. 67.

- Se permite la creación de *Órganos* por parte de las Comunidades Autónomas (art. 41) que asumirán algunas de las funciones de la Agencia Española de Protección de Datos. Estos Órganos tendrán la consideración de autoridades de control y se les garantizará plena independencia.

- El Movimiento Internacional de Datos[10], regulado en los artículos 33 y 34 de la LOPD, sufre cambios muy relevantes, que serán comentados extensamente en los capítulos posteriores.

4.5. EL REGLAMENTO DE DESARROLLO DE LA LOPD

En la Disposición Final Primera de la LOPD se habilitaba al Gobierno para aprobar, o modificar, las disposiciones reglamentarias necesarias para la aplicación y desarrollo de la Ley. Por otra parte, tal como indica la Disposición Transitoria Tercera, hasta tanto se lleven a efectos las previsiones de la Disposición Final Primera, continuarán en vigor, con su propio rango, las normas reglamentarias existentes y, en especial, los Reales Decretos 428/1993, de 26 de marzo**;** 1332/1994, de 20 de junio, y 994/1999, de 11 de junio, en cuanto no se opongan a la LOPD.

La habilitación para el desarrollo reglamentario se tradujo, tras años de espera, en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

Entre las novedades más relevantes del RLOPD podemos destacar las siguientes:

[10] REBOLLO DELGADO, L: *Derechos fundamentales y protección de datos*. Dykinson. Madrid 2004, p. 157.

- Se incluye en su ámbito de aplicación a los ficheros y tratamientos de datos no automatizados, fijándose criterios específicos sobre medidas de seguridad de los mismos.

- Se excluyen de su ámbito de aplicación los datos de personas jurídicas y los de personas físicas que presten sus servicios en ellas con sus datos profesionales de contacto, puesto, correo, teléfono y fax. Asimismo, los datos relativos a empresarios individuales, cuando hagan referencia a ellos en su calidad de comerciantes, industriales o navieros.

- Se regula un procedimiento para garantizar que cualquier persona, antes de consentir que sus datos sean recogidos y tratados, pueda tener un pleno conocimiento de la utilización que estos datos vayan a tener.

- Se exige al responsable del tratamiento que conceda al interesado un medio sencillo y gratuito para permitir el ejercicio de su derecho de acceso, rectificación, cancelación y oposición.

- Se amplían las medidas de seguridad para los tratamientos automatizados en diferentes aspectos: copia de seguridad, distribución de soportes, cambio de contraseñas, control de acceso, etc.

- Se prohíbe el tratamiento de datos de menores de catorce años sin el consentimiento de sus padres.

- Se introducen cambios importantes en el tratamiento de ficheros sobre solvencia patrimonial y crédito.

- El responsable del fichero o tratamiento elaborará un documento de seguridad que recogerá las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente que será de obligado cumplimiento para el personal con acceso a los sistemas de información.

- En el apartado de transferencias internacionales de datos se efectúan cambios importantes. Se verán en toda su extensión en los próximos capítulos.

5. PROPUESTAS DE REFORMA DE LA NORMATIVA DE PROTECCIÓN DE DATOS

La herramienta básica de la normativa vigente de la UE en materia de protección de datos es la Directiva 95/46/CE. Se adoptó en 1995 con un doble objetivo: defender el derecho fundamental a la protección de datos y garantizar la libre circulación de estos datos entre los Estados miembros.

En los años transcurridos desde la aprobación de la Directiva se ha producido una rápida evolución tecnológica. La recogida e intercambio de datos se ha incrementado enormemente y se utilizan en una escala sin precedentes, tanto a nivel de las empresas privadas como en las administraciones públicas.

Pese a que los objetivos y principios de la Directiva 95/46/CE siguen siendo válidos en la actualidad, se han presentado una serie de problemas que con la normativa actual no se pueden resolver. Entre ellos, la Comisión Europea destaca en su documento de 25 de enero de 2012, COM(2012) 11 final, “la fragmentación en cómo se aplica en la Unión la protección de datos de carácter personal, la inseguridad jurídica y la percepción generalizada de la opinión pública de que existen riesgos significativos,

especialmente por lo que se refiere a la actividad en línea". La Comisión opina que ha llegado el momento "de establecer un marco más sólido y coherente en materia de protección de datos en la UE, con una aplicación estricta que permita el desarrollo de la economía digital en el mercado interior, otorgue a los ciudadanos el control de sus propios datos y refuerce la seguridad jurídica y práctica de los operadores económicos y las autoridades públicas".

La Comisión Europea considera que un Reglamento es el instrumento jurídico más apropiado para definir el marco de la protección de datos personales en la Unión. La aplicabilidad directa de un Reglamento reducirá la fragmentación jurídica y ofrecerá una mayor seguridad jurídica merced a la introducción de un conjunto armonizado de normas básicas, la mejora de la protección de los derechos fundamentales de las personas y la contribución al funcionamiento del mercado interior. Tal como afirma Gómez Sánchez, el "*efecto directo* del Derecho comunitario afecta al Derecho originario -Tratados constitutivos y a sus sucesivas modificaciones- y a los Reglamentos de Derecho derivado. Caso distinto es el de las Directivas, también integrantes del Derecho derivado, pero que, como antes hemos señalado, precisan de la acción de los poderes públicos nacionales para completar su eficacia"[11].

Con arreglo al principio de subsidiariedad (artículo 5, apartado 3, del TUE), la Unión solo debe intervenir en caso de que los objetivos perseguidos no puedan ser alcanzados de manera suficiente por los Estados miembros por sí solos, sino que puedan alcanzarse mejor a escala de la Unión. Las razones expuestas anteriormente indican,

[11] GÓMEZ SÁNCHEZ, Y: *Derecho Constitucional Europeo: Derechos y Libertades*. Sanz y Torres. Madrid 2008, pág. 21.

según el criterio de la Comisión, la necesidad de adoptar iniciativas a escala de la UE por los siguientes argumentos:

– El derecho a la protección de datos de carácter personal, consagrado en el artículo 8 de la Carta de los Derechos Fundamentales, requiere el mismo nivel de protección de datos en toda la Unión. La ausencia de normas comunes de la UE provocaría el riesgo de que hubiera diferentes niveles de protección en los Estados miembros y restricciones en los flujos transfronterizos de datos personales entre los Estados miembros con distintas normas.

– Los datos personales se transfieren a través de las fronteras nacionales, tanto internas como externas, a ritmos cada vez más rápidos. Además, existen retos prácticos a la ejecución de la legislación de protección de datos y la necesidad de cooperación entre los Estados miembros y sus autoridades, que tiene que organizarse a escala de la UE para garantizar la unidad de aplicación del Derecho de la Unión. Por otra parte, la UE es la que está en mejores condiciones para garantizar de forma efectiva y coherente el mismo nivel de protección de los ciudadanos cuando sus datos personales se transfieren a terceros países.

– Por sí solos, los Estados miembros no pueden mitigar los problemas que se plantean en la situación actual, especialmente los debidos a la fragmentación de las legislaciones nacionales. Por tanto, existe una necesidad específica de establecer un marco armonizado y coherente que permita una adecuada transferencia de datos personales a través de las fronteras interiores de la UE, al tiempo que se garantiza una protección efectiva a todas las personas físicas en la UE.

– Las iniciativas legislativas de la UE propuestas serán más efectivas que acciones similares adoptadas a nivel de los Estados miembros debido a la naturaleza y magnitud de los problemas, que no se circunscriben al ámbito de uno o varios Estados miembros.

La nueva regulación propuesta por la Comisión Europea está basada en un Reglamento que sustituya a la Directiva 95/46/CE, en el que se fija el marco jurídico general de protección de datos de la UE[12].

Siguiendo el documento de 25 de enero de 2012 COM(2012) 9 final[13], se exponen los principales componentes de la reforma del marco jurídico para la protección de datos de la UE:

I. Control de los ciudadanos sobre sus datos personales

Para reforzar los derechos de los ciudadanos a la protección de sus datos, la Comisión propone nuevas normas que:

a) Aumentarán el control de los ciudadanos sobre sus datos:

[12] Junto al nuevo Reglamento, la Comisión propone una Directiva (que sustituye a la Decisión Marco 2008/977/JAI) que fija las normas sobre la protección de los datos personales tratados con fines de prevención, detección, investigación o persecución de delitos y para las actividades judiciales correspondientes.

[13] *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. La protección de la privacidad en un mundo interconectado. Un marco europeo de protección de datos para el siglo XXI*. Bruselas, 25.1.2012 COM(2012) 9 final.

- asegurando que, siempre que se requiera su consentimiento, este se otorgue de forma explícita, a saber, mediante una declaración o una actuación clara y afirmativa por parte del interesado, y libre;
- dotando a los usuarios de Internet de un derecho efectivo al olvido en el entorno en línea: el derecho a que se supriman sus datos si retiran su consentimiento y no existen otros motivos legítimos para conservarlos;
- garantizando un acceso fácil a los datos propios y un derecho de portabilidad de los datos: el derecho a obtener del responsable del tratamiento una copia de los datos conservados y la libertad de transferirlos de un proveedor de servicio a otros sin trabas;
- reforzando el derecho a la información de tal forma que los ciudadanos comprendan plenamente cómo se tratan sus datos personales, especialmente cuando esas actividades afecten a niños.

b) Mejorarán los medios que permiten a los ciudadanos ejercer sus derechos:

- reforzando la independencia y las competencias de las autoridades nacionales de protección de datos de forma que estén adecuadamente equipadas para dar curso eficazmente a las reclamaciones, estén facultadas para llevar a cabo investigaciones efectivas, adopten decisiones vinculantes e impongan sanciones efectivas y disuasorias;
- ensanchando las vías de recurso administrativo y judicial en caso de violación de los derechos de protección de datos. Concretamente, las asociaciones debidamente habilitadas podrán ejercitar acciones judiciales en nombre de los particulares.

c) Reforzarán la seguridad de los datos:

- fomentando el uso de tecnologías que protejan la privacidad (tecnologías que, al minimizar la conservación de datos personales, resguardan la privacidad de la información), configuraciones por defecto respetuosas de la privacidad y regímenes de certificación de la privacidad;
- imponiendo a los responsables del tratamiento de los datos una obligación general de notificar, sin demora indebida, toda violación de datos tanto a las autoridades competentes en materia de protección de datos (en un plazo de 24 horas siempre que sea posible) como a los afectados.

d) Acrecentará la responsabilidad de quienes tratan datos, concretamente:

- exigiendo a los responsables del tratamiento de los datos que nombren a un Delegado de Protección de Datos en las empresas con más de 250 empleados y en las empresas que efectúen operaciones de tratamiento de datos que entrañen cierto riesgo;
- introduciendo el principio de «privacidad desde el diseño» a fin de asegurar que las garantías de protección de los datos se incorporan ya en la fase de planificación de los procedimientos y sistemas;
- imponiendo a las organizaciones que lleven a cabo operaciones de tratamiento que entrañen cierto riesgo la obligación de llevar a cabo evaluaciones de impacto sobre la protección de los datos.

II. Normas de protección de datos adaptadas al mercado único digital

Con el fin de potenciar la dimensión de mercado único de la protección de datos, la Comisión propone:

- fijar las normas de protección de datos al nivel de la UE mediante un Reglamento directamente aplicable en todos los Estados miembros, lo que pondrá fin a la aplicación acumulativa y simultánea de distintas leyes nacionales de protección de datos;
- simplificar el entorno regulador mediante una drástica reducción de los trámites burocráticos y la eliminación de determinadas formalidades, como los requisitos generales de notificación; habida cuenta de su importancia para la competitividad de la economía europea, se otorgará especial atención a las necesidades específicas de las microempresas y de las pequeñas y medianas empresas;
- ampliar la independencia y las facultades de las autoridades nacionales de protección de datos, habilitándolas para llevar a cabo investigaciones, adoptar decisiones vinculantes e imponer sanciones efectivas y disuasorias, y obligar a los Estados miembros a que les faciliten los recursos suficientes para el desempeño de esas tareas;
- crear un sistema de *ventanilla única* para la protección de datos en la UE: los responsables del tratamiento de datos de la UE tendrán como único interlocutor a una autoridad nacional de protección de datos, a saber, la del Estado miembro donde esté radicado el establecimiento principal;
- crear las condiciones necesarias para una cooperación presta y eficaz entre autoridades nacionales de protección de datos, lo que incluirá la obligación para cualquiera de ellas de llevar a cabo investigaciones e inspecciones a petición de cualquier otra y el reconocimiento mutuo de sus decisiones;
- crear un mecanismo de coherencia al nivel de la UE para asegurar que las decisiones de las autoridades nacionales de protección de datos que tengan mayor

repercusión europea tengan plenamente en cuenta los puntos de vista de las demás autoridades de protección de datos interesadas y se ajusten plenamente al Derecho de la UE;

- elevar el rango del Grupo de trabajo del artículo 29, convirtiéndolo en un Consejo Europeo de Protección de Datos a fin de mejorar su contribución a la aplicación coherente de la legislación en materia de protección de datos y de sentar unas sólidas bases de cooperación entre las autoridades de protección de datos, incluido el Supervisor Europeo de Protección de Datos, y potenciar las sinergias y la eficacia disponiendo que este último asuma las tareas de la Secretaría del Consejo Europeo de Protección de Datos.

III. Protección de los datos en un contexto de globalización

Los retos que plantea la globalización requieren herramientas y mecanismos flexibles, especialmente para las empresas activas en todo el mundo, que garanticen al mismo tiempo la protección sin fisuras jurídicas de los datos personales. La Comisión propone las medidas siguientes:

- adopción de normas claras que determinen en qué supuestos se aplica el Derecho de la UE a los responsables del tratamiento de datos establecidos en terceros países y que, en particular, especifiquen que siempre que se ofrezcan bienes y servicios a ciudadanos de la UE, o cuando se proceda a algún control de su comportamiento, serán de aplicación las normas europeas;
- toda decisión de adecuación que la Comisión adopte se basará en criterios explícitos y claros;

- la circulación legítima de datos a terceros países se facilitará reforzando y simplificando las normas sobre transferencias internacionales de datos a los países no cubiertos por ninguna decisión de adecuación, y sobre todo racionalizando ciertas herramientas (como por ejemplo las normas corporativas vinculantes) y generalizando su uso, de forma que puedan aplicarse a los responsables del tratamiento de datos y dentro de los grupos de sociedades, lo que reflejará mejor el número de empresas que llevan a cabo actividades de tratamiento de datos, especialmente mediante computación en nube;
- apertura de un diálogo y, cuando así proceda, negociaciones con terceros países (especialmente los socios estratégicos de la UE y los países de la Política Europea de Vecindad) y con las organizaciones internacionales pertinentes (como el Consejo de Europa, la Organización para la Cooperación y el Desarrollo Económico, las Naciones Unidas) a fin de promover la adopción de unas normas de protección de datos exigentes e interoperables en todo el mundo.

Para concluir, la reforma de la protección de datos de la UE quiere configurar un marco más moderno, sólido, coherente y global. Se quiere beneficiar con ella en primer lugar a los particulares, ya que consolidará sus derechos a la protección de datos y aumentará su confianza en el entorno digital. En segundo lugar se beneficia a las empresas ya que la reforma simplificará el marco jurídico. Esta simplificación debería suponer un estímulo para el desarrollo de la economía digital dentro de la UE, con el aumento de la riqueza y de puestos de trabajo que éste conllevaría.

6. DEFINICIÓN DEL CONCEPTO DE TRANSFERENCIA EN EL ÁMBITO DE LA PROTECCIÓN DE DATOS

Una cuestión clave en el presente trabajo es la definición del concepto de transferencia internacional de datos personales. En busca de esa definición partiremos en primer lugar del estudio de la normativa española.

En la LORTAD no se encuentra gran ayuda para aclarar dicho concepto. En su Título V, sobre movimiento internacional de datos, no se aborda la cuestión. Y en el artículo 3, sobre definiciones, solamente se indica en su letra c) que el *tratamiento de datos* engloba entre otros conceptos a las cesiones de datos que resulten de transferencias.

No encontraremos mucha ayuda tampoco en la LOPD. En su artículo 3.c) se repite la misma definición de tratamiento de datos que nos ofrecía la LORTAD. Y en su Título V, sobre movimiento internacional de datos, tampoco se aborda la cuestión.

En la Instrucción 1/2000, relativa a las normas por las que se rigen los movimientos internacionales de datos, encontramos una primera definición en su Norma Primera, de la Sección Primera, del Título III: "se considera transferencia internacional de datos toda transmisión de los mismos fuera del territorio español. En particular, se consideran como tales las que constituyan una cesión o comunicación de datos y las que tengan por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero.
A los efectos de esta instrucción, se entiende por transmitente la persona física o jurídica, pública o privada, responsable del fichero o tratamiento de los datos de carácter personal que son objeto de transferencia internacional, y por destinatario la persona

física o jurídica, pública o privada, situada fuera del territorio español que recibe los datos transferidos".

A pesar de que esta definición supone una primera aproximación al concepto hemos de criticar su contenido. Si se hubiera efectuado una correcta transposición de la normativa comunitaria, no se hubiera calificado como transferencia internacional a toda transmisión de datos fuera del territorio español. De esta definición se hubieran tenido que excluir las transmisiones efectuadas a cualquier otro país perteneciente al Espacio Económico Europeo.

Sin embargo se entendía que las transferencias de datos a los países del EEE también debían catalogarse como transferencias internacionales, si bien, en base al artículo 34.k) de la LOPD estaban liberalizadas. Según este artículo, podrán realizarse transferencias cuando tengan como destino un Estado miembro de la Unión Europea (debemos entenderlo como un país del EEE), o un Estado respecto del cual la Comisión Europea, en el ejercicio de sus competencias, haya declarado que garantiza un nivel de protección adecuado.

Una definición mucho más acertada del concepto la encontramos en el RLOPD. En su artículo 5.1.s) se define a la transferencia internacional como el "Tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español".

En base a la nueva definición del RLOPD, la cesión de datos a otro país miembro del EEE no se considerará transferencia internacional. Será una simple cesión de datos.

Por lo tanto tampoco habrá que observar los requisitos exigibles a las transferencias internacionales.

Como también nos indica la definición del RLOPD, existirá transferencia internacional en cualquiera de los dos casos siguientes:

- Cuando constituya una cesión o comunicación de datos.
- Cuando tenga por objeto la realización de un tratamiento de datos por cuenta del responsable.

En ambos supuestos se produce una salida física de datos fuera del EEE. Pero en el caso de acceso a los datos por cuenta de un encargado del tratamiento no se produce una salida jurídica de los datos, ya que el responsable del tratamiento está establecido en el territorio español y la norma que continuará aplicándose será la española.

El RLOPD también define en su artículo 5.j) y 5.ñ) a quienes intervienen en las transferencias internacionales, ya sea realizándolas o recibiendo los datos:

- Exportador de datos personales: la persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español que realice, conforme a lo dispuesto en el presente Reglamento, una transferencia de datos de carácter personal a un país tercero.
- Importador de datos personales: la persona física o jurídica, pública o privada, u órgano administrativo receptor de los datos en caso de transferencia internacional de los mismos a un tercer país, ya sea responsable del tratamiento, encargada del tratamiento o tercero.

Centrándonos ya en la normativa europea, la Directiva 95/46/CE no define que debe entenderse por transferencia internacional. En su artículo 2.b) solo indica que se entenderá como tratamiento de datos personales a la comunicación por transmisión, difusión o cualquiera otra forma que facilite el acceso a los datos. Los artículos 25 y 26 están dedicados a la *transferencia de datos personales a países terceros*, pero tampoco definen el concepto.

La propuesta de Reglamento general de protección de datos -COM(2012) 11 final, Bruselas, 25.1.2012- que previsiblemente se convertirá en la nueva normativa europea en materia de protección de datos, también omite definir el concepto de transferencia internacional. Su artículo 4, sobre definiciones, no hace mención alguna de este concepto. El Capítulo V, dedicado a la transferencia de datos personales a terceros países u organizaciones internacionales, pese a tener un contenido mucho más amplio que la Directiva 95/46/CE, tampoco las define. Que la nueva normativa siga sin definir este concepto es lamentable. Y así lo expone el Dictamen del Comité Económico y Social Europeo sobre la Propuesta de Reglamento[14], donde se reclama que lo que se entienda por transferencia de datos debería recogerse en el artículo 4 antes mencionado, donde se contienen las *Definiciones*.

[14] El Dictamen se encuentra publicado en el DOUE C 229 de 31 de julio de 2012.

CAPÍTULO II

TRANSFERENCIAS A ESTADOS QUE PROPORCIONEN UN NIVEL ADECUADO DE PROTECCIÓN

1. LA NECESIDAD DE UNA REGULACIÓN ESPECÍFICA

El gran avance de la tecnología[15], junto con el fenómeno de la globalización, ha llevado a un aumento muy importante de los flujos transfronterizos de datos.

El aumento de los flujos de datos se ha dado (tanto en su modalidad de cesión o comunicación de datos como en el caso de prestaciones de servicios), por una parte, a nivel del sector privado[16]. Las empresas multinacionales necesitan que la información pueda fluir entre sus diferentes sedes[17]. Pero también necesitan la contratación de servicios con empresas de otros países en donde los costes son más reducidos. Así, por ejemplo, a través de servicios de atención telefónica o de soporte técnico para sus bases

---

[15] A este respecto es muy interesante la lectura del documento de la Comisión IP/10/63 emitido en Bruselas el 28 de enero de 2010. En este documento, la Comisaria responsable de la Sociedad de la Información sostiene que la privacidad de los europeos será un gran desafío en la próxima década. También es muy relevante el documento IP/10/1462 emitido en Bruselas el 4 de noviembre de 2010. En él, la Vicepresidenta Viviane Reding, Comisaria de Justicia, Derechos fundamentales y Ciudadanía de la UE manifiesta la necesidad de actualizar las leyes de protección de datos para adaptarlas a los cambios que la globalización y las nuevas tecnologías han traído consigo.

[16] Tal como nos indica el *Informe sobre Protección de Datos a Nivel Internacional*, del Instituto Federal de Acceso a la Información Pública Gubernamental (México), de noviembre de 2004, en su página 195, una transferencia internacional de datos puede ser:

- Una comunicación a un tercero (entre dos responsables de sistemas de datos personales).
- Un encargo o prestación de servicios (entre un responsable del sistema de datos establecido en el territorio de alguno de los Estados miembros de la UE y un encargado del tratamiento establecido en un tercer país).

Documento disponible en la web **http://ieaip.org.mx/biblioteca_virtual/datos_personales/4.pdf**

[17] Como hace constar José Manuel de Frutos Gómez, Administrador Principal de la Dirección General de Justicia, Libertad y Seguridad (Comisión Europea), en la Presentación que efectuó en el VIII Encuentro Iberoamericano de Protección de Datos (Ciudad de México 29 y 30 de septiembre de 2010), "*tampoco es posible que, en aras del buen funcionamiento de este régimen, la Comunidad se aísle e impida toda relación con los países terceros*". Documento disponible en la dirección: **ieaip.org.mx/biblioteca_virtual/datos_personales/6.pdf**

de datos. Para poder contratar estos servicios, es necesario que los datos sean accesibles a los prestadores de los mismos.

Otro aspecto a considerar es el aumento de los flujos de datos entre administraciones públicas de países diversos. En este caso, los motivos de la transmisión de datos son diversos: seguridad pública, terrorismo, cooperación judicial, etc.

Las organizaciones internacionales han establecido límites a las transferencias internacionales para evitar la desprotección de los titulares de los datos. Se quiere evitar que la legislación interna de un país en materia de protección de datos pueda ser burlada mediante la transferencia a otro país en donde la legislación sea menos exigente, o incluso que no exista legislación alguna en este campo.

- Podemos citar, siguiendo un orden cronológico, las **Líneas Directrices de la OCDE sobre protección de la intimidad y los flujos transfronterizos de datos personales** de 23 de septiembre de 1980[18]. Ante la llegada de la tecnología de la información a diversos ámbitos de la vida económica y social, y dada la creciente importancia y poder del procesamiento informatizado de datos, la OCDE consideró imprescindible la elaboración de estas Líneas Directrices. Según las mismas, los Estados deben evitar, en general, restringir las transferencias internacionales de datos personales, excepto:

1) cuando los Estados receptores "no observen" el contenido de las Directrices;

[18] Véanse las “Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel”, de la OCDE, 1980 y el documento “Overview – OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data”, de la OCDE, 2002.

2) cuando la reexportación de datos personales eluda las disposiciones internas del Estado transmisor; ó

3) cuando ciertas categorías de datos personales reciban una protección especial en la legislación interna y tal *protección no sea equivalente* en otros Estados.

Las Directrices fueron adoptadas como una recomendación del Consejo de la OCDE apoyada en los tres principios que aglutinan a la organización: democracia pluralista, respeto de los derechos humanos y economías de mercado abiertas. Los principios establecidos en las Directrices se caracterizan por su claridad y flexibilidad de aplicación, y por su formulación, que es lo suficientemente general para permitir su adaptación a los cambios tecnológicos.

Tras las Líneas Directrices, el 11 de abril de 1985 los ministros de la OCDE adoptaron la *Declaración sobre flujos de datos transfronterizos*[19]. La Declaración aborda las cuestiones políticas que surgían del flujo de datos personales más allá de las fronteras nacionales como flujos de datos e información sobre actividades comerciales, flujos intraempresariales o de cualquier otro tipo. Los gobiernos representados en la OCDE reafirmaron su compromiso en la búsqueda de enfoques comunes ante las cuestiones de flujos de datos transfronterizos, y si fuera posible, desarrollar soluciones armonizadas.

Más reciente es la declaración ministerial sobre la protección de la privacidad de las redes globales, de 1998. En la conferencia ministerial de la OCDE "Un mundo sin fronteras: determinación del potencial del comercio electrónico", celebrada en 1998 en

[19] Véase en la web de la OCDE, en el apartado *Economie de l'Internet*, la sección de publicaciones y documentos de *Sécurité de l'information et protection de la vie privée*.

Otawa, los ministros reafirmaron su compromiso sobre la protección de la privacidad de las redes globales para garantizar el respeto de importantes derechos, generar confianza en las redes globales y evitar restricciones innecesarias en los flujos transfronterizos de datos personales.

- Conviene referenciar también la **Resolución 45/95 de la Asamblea General de la ONU**, de 14 de diciembre de 1990, sobre las directrices para la regulación de los archivos de datos personales informatizados. En el punto 9 de dicha resolución se establece que "cuando la legislación de dos o más países afectados por un flujo de datos a través de sus fronteras ofrezca *garantías comparables de protección* de la vida privada, la información debe poder circular tan libremente como en el interior de cada uno de los territorios respectivos. Cuando no haya garantías comparables, no se podrán imponer limitaciones injustificadas a dicha circulación, sino solamente en la medida en que así lo exija la protección de la vida privada". Como indica Jessica Matus[20], esto significa que "respecto de países que ofrecen salvaguardas o garantías similares o comparables, la regla es que exista libre circulación de los datos, constituyéndose en principio de las normas básicas de protección de datos. Respecto de países en que no existan estas salvaguardias recíprocas se limitarán las transmisiones en la medida que lo exija la protección de la intimidad". Dentro de las garantías mínimas que deben prever las legislaciones nacionales se encuentra la designación de una autoridad que será responsable de supervisar la observancia de los principios antes indicados. Esta autoridad deberá garantizar la imparcialidad y la independencia frente a terceros. Para el

[20] MATUS ARENAS, J: "Transferencias internacionales a países con niveles adecuados y no adecuados de protección. Aspectos prácticos". Ponencia para el Seminario Regional de Protección de Datos, Montevideo, Uruguay (uno a cuatro de junio de 2010), pág. 2.

caso de violación de las normas nacionales que lleven a la práctica los principios antes mencionados, de acuerdo al principio 8, de supervisión y sanciones, deberán regularse condenas penales u otras sanciones, junto con los recursos individuales adecuados.

En la Resolución 45/95 se pide a los gobiernos que tengan en cuenta sus principios rectores en sus leyes y reglamentos. De la misma forma, pide a las organizaciones gubernamentales, intergubernamentales y no gubernamentales que observen esos principios rectores al realizar las actividades propias de su competencia[21].

- El **Convenio 108 del Consejo de Europa**, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, de 28 de enero de 1981[22].

De acuerdo al artículo 12 del Convenio, que regula los flujos transfronterizos de datos de carácter personal y el derecho interno, una Parte no podrá, con el fin de proteger la vida privada, prohibir o someter a una autorización especial los flujos transfronterizos de datos de carácter personal con destino al territorio de otra Parte. Sin embargo, cualquier Parte tendrá la facultad de establecer una excepción a lo regulado anteriormente en los siguientes dos casos:

a) En la medida en que su legislación prevea una reglamentación específica para determinadas categorías de datos de carácter personal o de ficheros automatizados de datos de carácter personal, por razón de la naturaleza de dichos datos o ficheros, a menos que la reglamentación de la otra Parte establezca una protección equivalente.

[21] Véase en la web de la ONU, en el listado de las Resoluciones aprobadas por la Asamblea General durante su cuadragésimo quinto Período de Sesiones.

[22] Se puede acceder al contenido del Convenio 108 en la web de la Oficina de los Tratados del Consejo de Europa **http://conventions.coe.int/**

b) Cuando la transmisión se lleve a cabo a partir de su territorio hacia el territorio de un Estado no contratante por intermedio del territorio de otra Parte, con el fin de evitar que dichas transmisiones tengan como resultado burlar la legislación de la Parte a que se refiere el comienzo del presente párrafo.

Tal como nos indica Rebollo Delgado, con el contenido del Convenio, quedaba ya en 1981 establecido el marco genérico de protección de la persona, frente a las posibles intromisiones en su intimidad, o la lesión de derechos de la personalidad de forma más genérica, por parte de la informática[23].

A través de Protocolo Adicional al Convenio 108 (suscrito el 8 de noviembre de 2001)[24], se modifica la regulación de las transmisiones de datos a Estados que no sean parte. De acuerdo al artículo 2.1 de dicho protocolo adicional, "cada Parte preverá que la transferencia de datos personales a un destinatario sometido a la competencia de un Estado u organización que no es Parte del Convenio se lleve a cabo únicamente si dicho Estado u organización asegura un adecuado nivel de protección".

Además, según el artículo 1.1, cada Parte preverá que una o más Autoridades sean responsables de asegurar la conformidad de las medidas oportunas que den cumplimiento en el Derecho interno a los principios contenidos en los Capítulos II y III del Convenio y en el propio Protocolo.

- La **Directiva 95/46/CE**, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995. En el punto primero del artículo 25 de la Directiva se regula que "los Estados

[23] REBOLLO DELGADO, L: *Derechos Fundamentales y Protección de Datos*. Dykinson. Madrid 2004, p. 131.

[24] Se puede acceder al contenido del Protocolo Adicional al Convenio 108 en la web **http://conventions.coe.int/**

miembros dispondrán que la transferencia a un país tercero[25] de datos personales que sean objeto de tratamiento o destinados a ser objeto de tratamiento con posterioridad a su transferencia, únicamente pueda efectuarse cuando, sin perjuicio del cumplimiento de las disposiciones de Derecho nacional adoptadas con arreglo a las demás disposiciones de la presente Directiva[26], el país tercero de que se trate garantice un nivel de protección adecuado". La Directiva exige que todos los Estados miembros implementen un estándar de protección de datos a nivel de la Unión Europea. Tal como sostiene De Miguel Asensio, la Directiva 95/46/CE constituye un ejemplo de progreso en la uniformización jurídica, pues sus normas han tenido un notable impacto sobre las legislaciones de los Estados miembros, que en la mayor parte de los casos han tenido

[25] En el documento denominado *FREQUENTLY ASKED QUESTIONS RELATING TO TRANSFERS OF PERSONAL DATA FROM THE EU/EEA TO THIRD COUNTRIES*, elaborado por la Comisión Europea, nos indica que el término transferencia de datos personales está a menudo asociado al acto de enviar documentos, ya sea en formato papel o electrónicos, que contienen datos personales, a través de correo o por e-mail. Pero también se incluyen en esta definición todos los casos en los que un responsable de tratamiento toma acciones con el fin de que los datos personales se encuentren disponibles por otra parte situada en un país tercero.

Documento disponible en la web:

http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf

[26] Es muy interesante el comentario que se efectúa en el documento WP 38, adoptado el 26 de enero de 2001, del Grupo de Trabajo: "toda transferencia de la Comunidad a terceros países mediante cláusulas contractuales tipo que la Comisión considere que ofrece suficientes garantías es en sí una operación de tratamiento amparada por la legislación nacional que aplica la Directiva en los Estados miembros. La legalidad de dicha operación de tratamiento está sometida en su totalidad a las condiciones establecidas por la legislación nacional que aplica las disposiciones de la Directiva 95/46/CE. En caso de que una transferencia mediante las cláusulas contractuales tipo aprobadas por la Comisión no cumpla las condiciones fijadas en la legislación nacional con respecto a estos aspectos, la transferencia que se pretende hacer a terceros países no puede realizarse. Concretamente, si la revelación de datos a una tercera parte destinataria situada dentro del Estado miembro del responsable del tratamiento no fuera legal, la simple circunstancia de que el destinatario esté situado en un tercer país no cambia esta valoración jurídica".

que ser sustancialmente adaptadas[27]. Existe un cierto margen de maniobra a nivel nacional, pero la protección debe ser sustancialmente equivalente. Entonces el flujo de datos en el interior de la Unión Europea debe ser libre[28]. Aunque en la LOPD se hable solamente de los Estados miembros de la Unión Europea, debemos entender que la norma es aplicable a todos los países que forman el Espacio Económico Europeo, tal como ya indica el RLOPD en su artículo 5.1.s): "Transferencia internacional de datos: Tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo". Distinto es el régimen con los países terceros. En este caso se prohíbe la exportación de datos personales a cualquier país que no brinde un nivel adecuado de protección.

- Si nos centramos en la normativa española, podemos empezar con la mención del contenido del artículo 33.1 de la **Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal**:

"No podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un *nivel de protección equiparable* al que presta la presente Ley, salvo que, además de haberse observado lo

[27] DE MIGUEL ASENSIO, P: "La protección de datos personales a la luz de la reciente jurisprudencia del TJCE". Revista de la Facultad de Derecho de la Universidad de Granada, 3ª época, núm. 7, 2004, pág. 397-417.

[28] Tal como nos indica Jesús Rubí Navarrete, adjunto al Director de la AEPD, en su presentación sobre *Transferencia Internacional de Datos* (documento que se puede obtener en la web de la AEPD), para el Seminario de Cartagena de Indias del 14-16 de junio de 2011, podemos calificar como transferencia internacional de datos a toda comunicación de datos desde España a un país fuera del Espacio Económico Europeo. Pero no podemos calificar como transferencia internacional de datos a la comunicación de datos desde España a un país del Espacio Económico Europeo.

dispuesto en ésta, se obtenga autorización previa del Director de la Agencia Española de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas".

Podemos observar que la Directiva comunitaria y la norma española que la transpone no emplean el mismo término. Mientras la LOPD exige que el nivel de protección que se brinda en el país de destino sea equiparable al de la legislación española, la Directiva 95/46/CE habla de un nivel de protección adecuado. Y es evidente que la palabra *equiparable* es más restrictiva que el término *adecuado*.

El RLOPD se aleja del concepto "nivel de protección equiparable" de la LOPD y en sus artículos 67 y 68 hace referencia al "nivel adecuado de protección" acordado por la Agencia Española de Protección de Datos, o declarado por Decisión de la Comisión Europea.

Las circunstancias que deben tomarse en consideración a la hora de determinarse el carácter adecuado, o no, en el nivel de protección del país de destino de los datos, vienen recogidas en el artículo 33.2 de la LOPD:

"El carácter adecuado del nivel de protección que ofrece el país de destino se evaluará por la Agencia Española de Protección de Datos atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencias de datos. En particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de derecho, generales o sectoriales, vigentes en el país tercero de que se trate, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países".

El artículo 33.2 de la LOPD ha transcrito de forma casi literal el contenido del artículo 25.2 de la Directiva 95/46/CE.

Para finalizar este apartado, es interesante conocer quienes intervienen en una transferencia internacional de datos según el artículo 5 del RLOPD:

- Exportador de datos personales: la persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español que realice, conforme a lo dispuesto en el presente Reglamento, una transferencia de datos de carácter personal a un país tercero.
- Importador de datos personales: la persona física o jurídica, pública o privada, u órgano administrativo receptor de los datos en caso de transferencia internacional de los mismos a un tercer país, ya sea responsable del tratamiento, encargada del tratamiento o tercero.

2. EL DOCUMENTO DE TRABAJO WP 12

En este punto es imprescindible efectuar el análisis del Documento de Trabajo WP12 del Grupo de Trabajo (creado al amparo del artículo 29 de la Directiva 95/46/CE). Este Documento fue aprobado el 24 de julio de 1998, y lleva por título "Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE".

2.1. EVALUAR SI LA PROTECCIÓN ES ADECUADA

El capítulo uno del Documento WP 12 hace un análisis de lo que debe entenderse por "protección adecuada". Como indica Matus Arenas, "los perjuicios económicos que pueden derivarse de la limitación que establece el artículo 25 de la Directiva, tanto para

los países europeos como para los terceros, obliga a fijar o determinar con precisión qué es lo que efectivamente quiere exigir la Directiva con el requisito de *protección adecuada*, los criterios que de alguna manera otorguen objetividad al grado de adecuación, así como quién debe declararla o concederla"[29].

Como señala el documento WP12, el objetivo de la protección de datos no es otro que el de ofrecer protección a las personas cuyos datos son objeto de tratamiento. Este objetivo se logra combinando los derechos del interesado y las obligaciones de quienes tratan los datos o controlan dicho tratamiento. Estos derechos y estas obligaciones que vienen reconocidos en la Directiva 95/46/CE no han surgido de la nada. Se basan en aquellos dispuestos en el Convenio 108 del Consejo de Europa, que a la vez son concordantes con los incluidos en las directrices de la OCDE de 1980 o en las directrices de la ONU. Por todo ello, el Grupo de Trabajo opina que existe un alto consenso en relación con el contenido de las normas de protección de datos que va más allá de los límites de las fronteras de los países de la UE. Pero además de ser necesario que existan normas que protejan a las personas físicas, hay otro factor esencial: que estas normas se cumplan en la práctica[30]. Habrá que considerar entonces no sólo el

[29] MATUS ARENAS, J: "Transferencias internacionales a países con niveles adecuados y no adecuados de protección. Aspectos prácticos". Ponencia para el Seminario Regional de Protección de Datos, Montevideo, Uruguay (uno a cuatro de junio de 2010), pág. 4.

[30] Tal como nos dice el *Informe sobre Protección de Datos a Nivel Internacional*, del Instituto Federal de Acceso a la Información Pública Gubernamental (México), de noviembre de 2004, en su página 201, las sanciones constituyen un aspecto que debe estar presente en un sistema de protección de datos, como garantía para el derecho a la privacidad de los ciudadanos. La tipificación de conductas que supongan la comisión de una infracción, con su correspondiente sanción, es una garantía para los interesados cuyos datos son objeto de tratamiento.

Documento disponible en la web **http://ieaip.org.mx/biblioteca_virtual/datos_personales/4.pdf**

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. En los países europeos ha sido general la plasmación en su Derecho interno de las garantías necesarias en materia de protección de datos, lo que ha permitido sancionar los incumplimientos en esta materia, además de conceder a las personas físicas un derecho de reparación. Además las diferentes legislaciones europeas han incluido, en general, el establecimiento de autoridades de control con funciones de seguimiento e investigación de denuncias. Estos procedimientos han sido plasmados en la Directiva 95/46/CE.

Fuera de la Unión Europea es menos común encontrar medios tan sofisticados para asegurar el cumplimiento de las normas de protección de datos. Así, en el Convenio 108 se exige la incorporación de los principios de la protección de datos en su legislación, pero no se contemplan mecanismos tales como una autoridad de control. Menos aun en las directrices de la OCDE, que no prevén procedimientos para garantizar una protección efectiva de las personas físicas. En el caso de las directrices de la ONU ya se incluyen disposiciones de control y sanciones, lo que apunta a una progresiva sensibilización en cuanto a la necesidad de aplicar debidamente las normas de protección de datos.

Por todo ello, el Grupo de Trabajo llega a la conclusión de que, a la hora de analizar la protección adecuada, deberán tenerse en cuenta los dos elementos básicos: el contenido de las normas aplicables y los medios para asegurar su aplicación eficaz.

Partiendo del contenido de la Directiva 95/46/CE, y teniendo en cuenta las disposiciones de otros textos internacionales sobre la protección de datos, es posible lograr un *núcleo de principios de contenido y de requisitos de procedimiento y de aplicación*, cuyo cumplimiento pudiera considerarse un requisito mínimo para juzgar

adecuada la protección. Este núcleo mínimo no es aplicable de forma estricta en todos los casos. En ocasiones, el grado de riesgo de la transferencia exigirá la ampliación de ese núcleo mínimo. En otros casos, el riesgo será tan bajo que podría permitir la reducción de la lista. Sin embargo, en opinión del Grupo de Trabajo, la compilación de una lista básica de condiciones mínimas es un punto de partida útil para cualquier análisis.

Los principios de contenido sugeridos por el Grupo de Trabajo son los siguientes:

1) **Principio de limitación de objetivos.** Los datos deben tratarse con un objetivo específico y posteriormente utilizarse o transferirse únicamente en cuanto ello no sea incompatible con el objetivo de la transferencia. Las únicas excepciones a esta norma serían las necesarias en una sociedad democrática por alguna de las razones expuestas en el artículo 13 de la Directiva[31].

2) **Principio de proporcionalidad y de calidad de los datos.** Los datos deben ser exactos y, cuando sea necesario, estar actualizados. Los datos deben ser adecuados,

[31] Artículo 13 Excepciones y limitaciones

1. Los Estados miembros podrán adoptar medidas legales para limitar el alcance de las obligaciones y los derechos previstos en el apartado 1 del artículo 6, en el artículo 10, en el apartado 1 del artículo 11, y en los artículos 12 y 21 cuando tal limitación constituya una medida necesaria para la salvaguardia de:

a) la seguridad del Estado;

b) la defensa;

c) la seguridad pública;

d) la prevención, la investigación, la detección y la represión de infracciones penales o de las infracciones de la deontología en las profesiones reglamentadas;

e) un interés económico y financiero importante de un Estado miembro o de la Unión Europea, incluidos los asuntos monetarios, presupuestarios y fiscales;

f) una función de control, de inspección o reglamentaria relacionada, aunque sólo sea ocasionalmente, con el ejercicio de la autoridad pública en los casos a que hacen referencia las letras c), d) y e);

g) la protección del interesado o de los derechos y libertades de otras personas.

pertinentes y no excesivos con relación al objetivo para el que se transfieren o para el que se tratan posteriormente.

3) **Principio de transparencia.** Debe informarse a los interesados acerca del objetivo del tratamiento y de la identidad del responsable del tratamiento en el tercer país, y de cualquier otro elemento necesario para garantizar un trato leal. Las únicas excepciones permitidas deben corresponder a los artículos 13 y 11.2 de la Directiva.

Según el artículo 11.1, cuando los datos no hayan sido recabados del interesado, los Estados miembros dispondrán que el responsable del tratamiento o su representante deberán, desde el momento del registro de los datos o, en caso de que se piense comunicar datos a un tercero, a más tardar, en el momento de la primera comunicación de datos, comunicar al interesado por lo menos una información básica (identidad del responsable del tratamiento, fines del tratamiento, categorías de datos, destinatarios de los datos, etc.), salvo si el interesado ya hubiera sido informado de ello. Sin embargo el artículo 11.2 indica que dichas obligaciones no se aplicarán cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados o el registro o la comunicación a un tercero estén expresamente prescritos por ley.

4) **Principio de seguridad.** El responsable del tratamiento debe adoptar medidas técnicas y organizativas adecuadas a los riesgos que presenta el tratamiento. Toda persona que actúe bajo la autoridad del responsable del tratamiento, incluido el encargado del tratamiento, no debe tratar los datos salvo por instrucción del responsable del tratamiento.

5) **Derechos de acceso, rectificación y oposición.** El interesado debe tener derecho a obtener una copia de todos los datos a él relativos, y derecho a rectificar aquellos

datos que resulten ser inexactos. En determinadas situaciones, el interesado también debe poder oponerse al tratamiento de los datos a él relativos. Las únicas excepciones a estos derechos deben estar en línea con el artículo 13 de la Directiva.

6) Restricciones respecto a transferencias sucesivas a otros terceros países. Únicamente deben permitirse transferencias sucesivas de datos personales del tercer país de destino a otro tercer país en el caso de que este último país garantice asimismo un nivel de protección adecuado. Las únicas excepciones permitidas deben estar en línea con el artículo 26.1 de la Directiva. En este artículo se dispone que puede efectuarse una transferencia de datos personales a un país tercero que no garantice un nivel de protección adecuado cuando:

a) el interesado haya dado su consentimiento inequívocamente a la transferencia prevista, o

b) la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales tomadas a petición del interesado, o

c) la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar en interés del interesado, entre el responsable del tratamiento y un tercero, o

d) La transferencia sea necesaria o legalmente exigida para la salvaguardia de un interés público importante, o para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial, o

e) la transferencia sea necesaria para la salvaguardia del interés vital del interesado, o

f) la transferencia tenga lugar desde un registro público que, en virtud de disposiciones legales o reglamentarias, esté concebido para facilitar información al público y esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo, siempre que se cumplan, en cada caso particular, las condiciones que establece la ley para la consulta.

A continuación figuran ejemplos de principios adicionales que deben aplicarse a tipos específicos de tratamiento:

1) **Datos sensibles[32].** Cuando se trate de categorías de datos "sensibles" incluidas en el artículo 8 de la Directiva (origen racial o étnico, opiniones políticas, convicciones religiosas o filosóficas, pertenencia a sindicatos, así como datos relativos a salud o a sexualidad), deberán establecerse protecciones adicionales, tales como la exigencia de que el interesado otorgue su consentimiento explícito para el tratamiento.

2) **Mercadotecnia directa.** En el caso de que el objetivo de la transferencia de datos sea la mercadotecnia directa, el interesado deberá tener en cualquier momento la posibilidad de negarse a que sus datos sean utilizados con dicho propósito.

3) **Decisión individual automatizada.** Cuando el objetivo de la transferencia sea la adopción de una decisión automatizada en el sentido del artículo 15 de la Directiva[33], el

[32] REBOLLO DELGADO, L: *Derechos fundamentales y protección de datos*. Dykinson. Madrid 2004, p. 150.

[33] Artículo 15. Decisiones individuales automatizados

1. Los Estados miembros reconocerán a las personas el derecho a no verse sometidas a una decisión con efectos jurídicos sobre ellas o que les afecte de manera significativa, que se base únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, como su rendimiento laboral, crédito, fiabilidad, conducta, etc.

interesado deberá tener derecho a conocer la lógica aplicada a dicha decisión, y deberán adoptarse otras medidas para proteger el interés legítimo de la persona.

En cuanto a los mecanismos del procedimiento o de aplicación, el Grupo de Trabajo considera que existe un amplio consenso en Europa en que un sistema de "supervisión externa" en forma de autoridad independiente es una característica necesaria de un sistema de cumplimiento de la protección de datos. Sin embargo, en otras partes del mundo no se observa esa necesidad. Será necesario sentar las bases para evaluar el carácter adecuado de la protección ofrecida. Para ello es necesario distinguir los objetivos de un sistema normativo de protección de datos, y sobre esta base juzgar la variedad de diferentes mecanismos de procedimiento judiciales y no judiciales utilizados en terceros países.

El Grupo de Trabajo considera que los objetivos de un sistema de protección de datos son básicamente tres:

1) Ofrecer un **nivel satisfactorio de cumplimiento** de las normas. Ningún sistema puede garantizar el 100 % de cumplimiento, pero algunos son mejores que otros. Un buen sistema se caracteriza, en general, por el hecho de que los responsables del tratamiento conocen muy bien sus obligaciones y los interesados conocen muy bien sus

---

2. Los Estados miembros permitirán, sin perjuicio de lo dispuesto en los demás artículos de la presente Directiva, que una persona pueda verse sometida a una de las decisiones contempladas en el apartado 1 cuando dicha decisión:

a) se haya adoptado en el marco de la celebración o ejecución de un contrato, siempre que la petición de celebración o ejecución del contrato presentada por el interesado se haya satisfecho o que existan medidas apropiadas, como la posibilidad de defender su punto de vista, para la salvaguardia de su interés legítimo;

b) esté autorizada por una ley que establezca medidas que garanticen el interés legítimo del interesado.

derechos y medios para ejercerlos. La existencia de sanciones efectivas y disuasorias es importante a la hora de garantizar la observancia de las normas, al igual que lo son, como es natural, los sistemas de verificación directa por las autoridades, los auditores o los servicios de la Administración encargados específicamente de la protección de datos.

2) Ofrecer **apoyo y asistencia a los interesados** en el ejercicio de sus derechos. El interesado debe tener la posibilidad de hacer valer sus derechos con rapidez y eficacia, y sin costes excesivos. Para ello es necesario que haya algún tipo de mecanismo institucional que permita investigar las denuncias de forma independiente.

3) Ofrecer **vías adecuadas de recurso** a quienes resulten perjudicados en el caso de que no se observen las normas. Éste es un elemento clave que debe incluir un sistema que ofrezca la posibilidad de obtener una resolución judicial o arbitral y, en su caso, indemnizaciones y sanciones.

2.2. APLICACIÓN DEL ENFOQUE A LOS PAÍSES QUE HAN RATIFICADO EL CONVENIO 108 DEL CONSEJO DE EUROPA

En el capítulo dos del Documento de Trabajo WP12, se contempla la aplicación del enfoque que hemos estado analizando, a los países que han ratificado el Convenio 108 del Consejo de Europa[34]. Como bien indica el Documento, el Convenio 108 es un

[34] En la página web del Consejo de Europa, a fecha uno de enero de 2013, se informa de los 44 países que han ratificado el Convenio 108: Albania, Andorra, Armenia, Austria, Azerbaiján, Bélgica, Bosnia y Herzegovina, Bulgaria, Croacia, Chipre, República Checa, Dinamarca, Estonia, Finlandia, Francia, Georgia, Alemania, Grecia, Hungría, Islandia, Irlanda, Italia, Letonia, Liechtenstein, Lituania, Luxemburgo, Malta, Moldavia, Mónaco, Montenegro, Holanda, Noruega, Polonia, Portugal, Rumanía, Serbia, Eslovaquia, Eslovenia, España, Suecia, Suiza, La antigua República Yugoslava de Macedonia, Ucrania y Reino Unido. Firmaron el Convenio, pero no la han ratificado, Rusia y Turquía.

instrumento internacional con poder vinculante en el área de la protección de datos. Es un Convenio que puede ser ratificado, no sólo por los países pertenecientes al Consejo de Europa, sino también por Estados que no pertenezcan a él. Por estas razones, el Grupo de Trabajo considera interesante examinar si es posible considerar que los países que han ratificado el Convenio ofrecen un nivel adecuado de protección en el sentido del artículo 25 de la Directiva.

Para iniciar el análisis, se emplea el núcleo de principios de contenido y de requisitos de procedimiento o de aplicación señalados en el apartado anterior. En cuanto a los principios de contenido, el Convenio incluye las cinco primeras de las seis condiciones mínimas. También incluye el requisito de una protección adecuada para los datos sensibles (la cual será requisito de adecuación cuando se trate de tales datos).

El elemento ausente en el Convenio, desde el punto de vista del contenido de sus normas sustantivas, son las restricciones a las transferencias a países no signatarios del Convenio. Esto podría llevar a que un país signatario del Convenio 108 pudiera emplearse como instrumento en una transferencia de datos desde un país de la UE a otro tercer país con niveles de protección absolutamente insuficientes.

En cuanto a los mecanismos de procedimiento, el Convenio exige que sus principios se plasmen en legislaciones nacionales y que se establezcan sanciones y remedios apropiados en caso de violación de estos principios. Estas medidas deberían ser suficientes para garantizar un nivel razonable de cumplimiento de las normas y una reparación adecuada para los interesados en caso de incumplimiento de las mismas. Con ello se satisfacen los objetivos primero y tercero en cuanto a cumplimiento de la protección de datos. Sin embargo, el Convenio no obliga a las partes contratantes a establecer mecanismos institucionales que permitan la investigación independiente de

las quejas. No se garantiza, entonces, el apoyo y la asistencia prestados a las personas cuyos datos son objeto de tratamiento en el ejercicio de sus derechos (con lo cual no se cumple el objetivo segundo).

El Grupo de Trabajo opina que el análisis efectuado parece indicar que es posible permitir la mayoría de las transferencias de datos personales a países que han ratificado el Convenio 108 a condición de que se cumplan dos condiciones:

- El país en cuestión también disponga de mecanismos adecuados para garantizar el cumplimiento, ayudar a las personas físicas y facilitar la reparación. El Grupo de Trabajo indica como ejemplo, una autoridad de control independiente dotada de las competencias apropiadas.
- El país en cuestión sea el destino final de la transferencia y no un país intermediario a través del cual transitan los datos, excepto cuando las transferencias sucesivas se dirigen de nuevo a la UE o a otro destino que ofrezca una protección adecuada.

Con posterioridad a la confección del Documento de Trabajo WP12, se ha elaborado un Protocolo Adicional del Convenio 108 (hecho en Estrasburgo el 8 de Noviembre de 2001)[35], en el que se han tenido en cuenta los dos puntos débiles mencionados anteriormente.

[35] En la página web del Consejo de Europa, a fecha uno de enero de 2013, se informa de los 33 países que han ratificado el Protocolo Adicional del Convenio 108: Albania, Andorra, Armenia, Austria, Bosnia y Herzegovina, Bulgaria, Croacia, Chipre, República Checa, Estonia, Finlandia, Francia, Alemania, Hungría, Irlanda, Letonia, Liechtenstein, Lituania, Luxemburgo, Moldavia, Mónaco, Montenegro, Holanda, Polonia, Portugal, Rumanía, Serbia, Eslovaquia, España, Suecia, Suiza, La antigua República Yugoslava de Macedonia y Ucrania. Firmaron el Convenio, pero no la han ratificado, Bélgica, Dinamarca, Grecia, Islandia, Italia, Noruega, Rusia, Turquía y Reino Unido.

En el primer artículo de dicho Protocolo se exige que todos los firmantes deberán tener una o más Autoridades que serán responsables de asegurar la conformidad de las medidas oportunas que den cumplimiento en el Derecho interno a los principios contenidos en el Convenio y en el propio Protocolo. Dichas Autoridades dispondrán de poderes de investigación y de intervención, así como del poder de iniciar procedimientos legales o de dirigirse a las autoridades judiciales correspondientes en relación con violaciones del derecho interno. Asimismo cada Autoridad de Control conocerá de las reclamaciones presentadas por parte de cualquier persona relativas a sus derechos y libertades fundamentales con respecto al tratamiento de datos personales y dentro de sus respectivas competencias.

Las Autoridades de Control ejercerán sus funciones con completa independencia, y cuando sus decisiones den lugar a reclamaciones, podrán ser recurridas judicialmente.

Las Autoridades de Control cooperarán mutuamente en la medida necesaria para el cumplimiento de sus obligaciones, y en particular a través del intercambio de cualquier información que resulte de utilidad.

El artículo 2 del Protocolo Adicional se ocupa de la transferencia de datos personales a destinatarios no sometidos a la competencia de las Partes del Convenio. Como regla general, solamente se podrá llevar a cabo dicha transferencia de datos si dicho Estado u organización asegura un adecuado nivel de protección.

Sin embargo, como excepción a la regla general, en el propio artículo 2 se prevé que las Partes puedan autorizar la transferencia de datos personales en los siguientes casos:

“a) Si el derecho interno así lo establece a 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, en particular, de cláusulas contractuales, por parte del responsable del tratamiento responsable de la transferencia y dichas garantías se estiman adecuadas por las autoridades competentes de conformidad con el derecho interno".

2.3. APLICACIÓN DEL ENFOQUE A LA AUTORREGULACIÓN INDUSTRIAL

En el capítulo tres del Documento de Trabajo WP 12 se analiza el carácter adecuado del nivel de protección que ofrece un país en base a la autorregulación industrial. El artículo 25.2 de la Directiva 95/46/CE establece que el nivel de protección que ofrece un país se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos. Se incluye en este conjunto de circunstancias no sólo a las normas de Derecho, sino también a "las normas profesionales y las medidas de seguridad en vigor en dichos países".

Tal como se nos indica en el Documento de Trabajo, lo que exige la Directiva es que se tengan en cuenta las normas no jurídicas que puedan existir en un país, siempre que estas normas *se cumplan*. Por ello considera importante la evaluación de la función de autorregulación industrial.

El Grupo de Trabajo inicia su estudio analizando lo que, a efectos del Documento de Trabajo analizado (WP 12), deberá entenderse por código de autorregulación: "cualquier conjunto de normas de protección de datos aplicable a una pluralidad de responsables del tratamiento que pertenezcan a la misma profesión o al mismo sector

industrial, cuyo contenido haya sido determinado fundamentalmente por los miembros del sector industrial o profesión en cuestión".

Un criterio esencial para juzgar el valor de un código es su fuerza ejecutiva, o lo que es lo mismo, la fuerza de la asociación en cuanto a su capacidad para imponer sanciones a sus miembros por incumplimiento del código, por ejemplo. Pero también tiene su relevancia la cuestión de si la asociación u organismo responsable del código representa a todos los operadores del sector o únicamente a un pequeño porcentaje de éstos. En el caso de un sector que esté fragmentado en múltiples asociaciones, cada una con su propio código de protección de datos, es inevitable que se provoque un panorama confuso y de opacidad para las personas cuyos datos son objeto de tratamiento. Pero también debemos tener en cuenta que, en aquellos sectores donde es práctica corriente transferir datos personales entre diferentes empresas del mismo sector, puede darse el caso de que la empresa que transmita los datos personales no esté sujeta al mismo código de protección de datos que la empresa receptora. Todo ello supone una fuente de inseguridad en cuanto a las normas que son aplicables.

A la hora de evaluar la autorregulación, al igual que para evaluar cualquier conjunto específico de normas sobre protección de datos, se deberá aplicar el enfoque general establecido en el capítulo uno del documento WP12. Deberá examinarse no sólo el contenido del instrumento sino también su eficacia para lograr:

- *Un buen nivel de cumplimiento general*

Un código profesional o industrial normalmente será desarrollado por un organismo representativo del sector industrial o profesión en cuestión, siendo de aplicación para los miembros de dicho organismo representativo. El nivel de cumplimiento del código

dependerá del grado de conocimiento de su existencia y de su contenido por parte de sus miembros, de las medidas que se adopten para garantizar la transparencia del código a los consumidores y de la naturaleza y la aplicación de las sanciones en caso de incumplimiento. La falta de sanciones realmente disuasorias y punitivas es una carencia importante en un código.

- *Apoyo y ayuda a las personas cuyos datos sean objeto de tratamiento*

Debe proporcionarse apoyo institucional a las personas que se enfrentan a un problema relativo a sus datos personales, para que puedan resolver sus dificultades. La imparcialidad del árbitro o juez es un punto clave. Para ello es imprescindible que dicho árbitro o juez sean independientes respecto al responsable del tratamiento. Pero de forma ideal, el árbitro debería ser también ajeno a la profesión o sector, para evitar la comunidad de intereses con el responsable del tratamiento. Si ello no fuera posible, se podría conseguir la neutralidad del órgano de decisión a través de la inclusión de representantes de los consumidores junto a los representantes del sector.

- *Una reparación adecuada*

Cuando se pruebe la infracción del código de autorregulación, deberá existir un recurso para el interesado que lleve a la solución del problema. Si además se ha producido un perjuicio para el interesado, debe contemplarse el pago de una compensación adecuada, que cubra tanto el daño físico y la pérdida financiera como cualquier daño psicológico o moral que se haya causado.

2.4. LA FUNCIÓN DE LAS DISPOSICIONES CONTRACTUALES

Este apartado del Documento WP 12 es materia del Capítulo siguiente de esta tesis doctoral (transferencias a estados que no proporcionen un nivel adecuado de

protección). Sin embargo creemos oportuno ubicarlo en el presente Capítulo para no dividir el estudio del Documento de Trabajo en dos capítulos distintos.

En el artículo 25.1 de la Directiva 95/46/CE se establece que sólo podrán efectuarse transferencias de datos personales a terceros países si el país considerado ofrece un nivel de protección adecuado. Sin embargo en el artículo 26.2 se establece una excepción al principio de protección adecuada: se permite la autorización a una transferencia o un conjunto de transferencias a un país que no garantice una protección adecuada cuando el responsable del tratamiento ofrezca garantías suficientes respecto de la protección de la vida privada, de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los respectivos derechos. Dichas garantías podrán derivarse, en particular, de cláusulas contractuales.

En el artículo 26.4 se faculta a la Comisión para declarar que determinadas cláusulas contractuales tipo ofrecen garantías suficientes a efectos de lo dispuesto en el artículo 26.2.

La utilización de contratos para regular las transferencias internacionales de datos personales no nace de la Directiva 95/46/CE. En Francia, por ejemplo, se vienen usando desde los años ochenta.

En el marco de las transferencias internacionales de datos, el contrato es un medio que permite al responsable del tratamiento ofrecer garantías adecuadas al transmitir datos fuera de la UE (lo que supone que quedan fuera del ámbito de aplicación del Derecho de la Unión), a un país en el que la protección de datos no sea suficiente.

Para que los contratos puedan cumplir su función, deben suplir la falta de protección adecuada con la inclusión de los elementos esenciales de la misma que no

existan en una situación determinada. Esos elementos esenciales, como ya vimos anteriormente, consisten en una serie de principios básicos para la protección de datos, junto con ciertas condiciones necesarias para asegurar su eficacia.

Dichos principios básicos son los siguientes:

- Principio de limitación de objetivos
- Principio de proporcionalidad y de calidad de los datos
- Principio de transparencia
- Principio de seguridad
- Derecho de acceso, rectificación y oposición
- Restricciones respecto a transferencias sucesivas a personas ajenas al contrato

Además en determinados casos deben aplicarse los principios complementarios relativos a los datos sensibles, a la mercadotecnia directa y a las decisiones automatizadas.

El contrato deberá contemplar de manera minuciosa la forma en que el receptor de los datos transferidos ha de aplicar los anteriores principios.

En cuanto a la efectividad de las normas sustantivas, vimos anteriormente tres criterios para evaluar la efectividad de un sistema de protección de datos. Estos criterios son la capacidad del sistema para:

- Ofrecer un nivel satisfactorio de cumplimiento de las normas
- Facilitar apoyo y asistencia a los interesados en el ejercicio de sus derechos
- Proporcionar vías adecuadas de recurso a quienes resulten perjudicados en el caso de que no se observen las normas.

Al evaluar la efectividad de una solución contractual deberemos examinar cada uno de estos aspectos detenidamente.

El elemento clave son las vías de recurso a disposición de los interesados. Sin embargo su aplicación práctica no es cosa fácil. Dependerá en buena parte de la legislación nacional elegida como aplicable al contrato. En general, dicha legislación debería ser la del Estado miembro en el que esté establecido el remitente. Sin embargo, incluso en este caso, encontramos un problema adicional: en algunos Estados miembros la normativa contractual no permite reconocer derechos a terceros.

La posición del interesado será todavía mucho mejor si las partes del contrato se comprometieran a someterse a un arbitraje vinculante en el supuesto de que dicho interesado impugnara su observancia de las disposiciones.

Otra posibilidad la encontramos en el caso de que el remitente de datos personales celebre un contrato independiente con el interesado. En este supuesto, el remitente se comprometería a responder de cualesquiera daños y perjuicios que se deriven del incumplimiento, por parte del receptor de los datos, de los principios básicos acordados para la protección de los datos. El interesado dispondría de esta forma de una vía de recurso frente al remitente por las faltas cometidas por el receptor. Por su parte, el remitente podría iniciar una acción contra el receptor por ruptura de contrato, con la finalidad de recuperar las posibles indemnizaciones que hubiera tenido que pagar al interesado.

En cuanto al apoyo y asistencia a los interesados, hemos de entender que las personas cuyos datos son transferidos a un país tercero tienen una gran dificultad para determinar la raíz de su problema concreto. A esas personas no les es posible juzgar si se han aplicado correctamente las normas sobre protección de datos o si tienen motivos para entablar una acción judicial. Por estas razones, la existencia de algún mecanismo

institucional que permita un examen independiente de las denuncias, es fundamental para una protección adecuada.

Pero las autoridades supervisoras en materia de protección de datos de un Estado miembro tienen poderes de control e investigación en el territorio del propio Estado. La transferencia de datos a un tercer Estado supondría la pérdida de tal garantía.

Una posibilidad sería exigir que en el contrato se confiriera a la autoridad supervisora del Estado del remitente, el derecho de inspeccionar el tratamiento realizado por el encargado de dicho tratamiento en el tercer país. Otra posibilidad es que el receptor de los datos en el país tercero se comprometa directamente con la autoridad supervisora del Estado miembro a autorizar el acceso de la misma cuando existan sospechas de que se han incumplido los principios de la protección de datos.

Cualquiera de las dos opciones es difícil de llevar a la práctica, ya que es complicado para la autoridad supervisora de un Estado asumir la responsabilidad de examinar e inspeccionar el tratamiento de los datos efectuado en un tercer país.

En cuanto al nivel satisfactorio de cumplimiento, es necesario poder confiar en que las partes del contrato se atienen realmente a sus cláusulas. Sin embargo en la solución contractual es difícil imponer sanciones por incumplimiento suficientemente importantes como para producir el efecto disuasorio imprescindible para crear un clima de confianza. Es posible que el receptor de la transferencia no esté sujeto a ninguna penalización si procesa los datos sin atenerse a lo dispuesto en el contrato. En este caso asumiría la responsabilidad el remitente de los datos, quien tendría entonces que entablar una acción legal independiente contra el receptor para resarcirse de sus posibles pérdidas. Es posible que esta falta de responsabilidad directa por el receptor pueda inducir al receptor a incumplir el contrato.

2.5. CUESTIONES DE PROCEDIMIENTO

En el artículo 25 de la Directiva se efectúa un planteamiento individualizado de las transferencias de datos: “El carácter adecuado del nivel de protección que ofrece un país tercero se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos; en particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, así como las normas profesionales y las medidas de seguridad en vigor en dichos países”.

Sin embargo, la gran cantidad de transferencias que se efectúan desde los países de la Unión Europea hacen imposible que cada una de ellas se examine en detalle. Es necesaria la aplicación de algún mecanismo que permita tomar decisiones que no impliquen una demora injustificada o el uso excesivo de recursos. Veamos tres soluciones alternativas:

- *Uso del artículo 25.6 de la Directiva*

De acuerdo al artículo 25.6 de la Directiva: La Comisión podrá hacer constar, de conformidad con el procedimiento previsto en el apartado 2 del artículo 31, que un país tercero garantiza un nivel de protección adecuado de conformidad con el apartado 2 del presente artículo, a la vista de su legislación interna o de sus compromisos internacionales, suscritos especialmente al término de las negociaciones mencionadas en el apartado 5, a efectos de protección de la vida privada o de las libertades o de los derechos fundamentales de las personas.

Los Estados miembros adoptarán las medidas necesarias para ajustarse a la decisión de la Comisión.

Tal como indica el artículo 25.6, las decisiones de la Comisión en este sentido pueden ser muy útiles. Sin perjuicio de los casos que pudieran presentar dificultades concretas, estas determinaciones pueden proporcionar cierta seguridad a los agentes económicos en cuanto a aquellos países que pueden considerarse garantes de un nivel adecuado de protección. Pero también puede tener una incidencia positiva en la mejora de los sistemas de protección de aquellos países terceros que quieran beneficiarse de dichas determinaciones por parte de la Comisión. Podemos mencionar otro aspecto muy positivo en el sentido de que, a través de las decisiones a nivel de la Unión Europea, se evita la publicación de listas "blancas" divergentes por parte de los gobiernos de los diferentes Estados miembros.

Este procedimiento tiene que enfrentarse a una serie de dificultades a tomar en consideración. La principal es que en muchos países no existe una protección uniforme en todos los sectores económicos. Así encontramos Estados en los que la ley protege los datos del sector público, pero no los del privado. O bien existen leyes específicas sólo para aspectos concretos. Incluso en países con estructura federal encontramos grandes divergencias entre la regulación de los distintos estados que forman la federación.

Todo ello nos lleva a la conclusión de que habrá pocos países que puedan ser considerados garantes de una protección adecuada.

A pesar de las dificultades mencionadas, el Grupo de Trabajo opina que el procedimiento del artículo 25.6 es una medida útil. Debería consistir en un proceso

continuo, no de una lista definitiva. Dicha lista debería ser ampliada y revisada constantemente de acuerdo con las nuevas situaciones que vayan surgiendo.

- *Análisis de riesgos de transferencias específicas*

La aplicación del artículo 25.6 puede ser muy útil en relación con un elevado número de transferencias. Pero en el caso de un tercer país que no sea objeto, total o parcialmente, de una determinación positiva, la autoridad de control deberá examinar cada caso concreto (ya sea mediante un análisis previo a la transferencia o a través de una revisión *ex post facto*). El enorme volumen de transferencias necesitará de un sistema que dé prioridad a determinadas categorías de transferencias porque suponen una amenaza especial para la vida privada. Sin embargo, el resultado final debe garantizar que sólo puedan realizarse transferencias cuando los terceros países aseguren un nivel de protección adecuado.

El Grupo de Trabajo considera que merecen especial atención las siguientes categorías de transferencias:

- las transferencias de ciertas categorías sensibles de datos definidas en el artículo 8 de la directiva;
- las transferencias que comportan el riesgo de pérdida financiera (por ejemplo, pagos con tarjeta de crédito a través de Internet);
- las transferencias que comportan un riesgo para la seguridad personal;
- las transferencias cuyo objetivo sea tomar una decisión que afecta significativamente a la persona (como, por ejemplo, decisiones de contratación o promoción, la concesión de créditos, etc.);

- las transferencias que comportan el riesgo de poner a la persona en una situación muy molesta o de empañar su reputación;
- las transferencias que pueden dar lugar a acciones específicas que constituyan una intrusión significativa en la vida privada de una persona, como las llamadas de teléfono no solicitadas;
- las transferencias repetitivas de volúmenes masivos de datos (por ejemplo, datos transaccionales tratados en redes de telecomunicaciones, Internet, etc.);
- las transferencias que incluyen la recopilación de datos mediante nuevas tecnologías que, por ejemplo, podrían realizarse de forma particularmente encubierta o clandestina (por ejemplo, "cookies" de Internet).

- *Cláusulas contractuales tipo*

El artículo 26.2 de la Directiva permite a los Estados miembros autorizar transferencias, incluso cuando el nivel de protección no sea adecuado, en virtud de disposiciones contractuales. De acuerdo al apartado 3 del mismo artículo, los Estados miembros informarán a la Comisión y a los demás Estados miembros acerca de las autorizaciones que concedan con arreglo al mencionado artículo 26.2[36]. La Comisión

[36] A este respecto es interesante la lectura de la nota de 21 de agosto de 2003 de la DG del Mercado Interior de la Comisión Europea *MARKT/E4/LCN/ck D(2003) 270*. Dicha nota se envió a todos los Estados miembros y a las autoridades responsables de la protección de datos de la UE. En el documento se muestra la preocupación de la Comisión por los indicios que sugieren claramente que "*se están realizando numerosas transferencias no autorizadas y quizá ilegales a destinos o destinatarios que no garantizan la protección adecuada*". La Comisión puso entre sus objetivos la mejora de la notificación de las autorizaciones concedidas con arreglo al apartado 2 del artículo 26 de la Directiva. La presente nota constituye la respuesta de los servicios de la Comisión a estas cuestiones y a algunas de las preguntas planteadas por varios Estados miembros y sus autoridades de control en materia de protección de datos sobre la mejor manera de informar a la Comisión Europea acerca de dichas autorizaciones.

puede mostrar su desacuerdo a las mismas y anular o confirmar la decisión de acuerdo a lo establecido en el artículo 31 de la Directiva.

Por otra parte, el artículo 26.4 de la Directiva autoriza a la Comisión a juzgar si ciertas cláusulas contractuales tipo ofrecen las garantías suficientes. Estas decisiones de la Comisión son vinculantes para los Estados miembros.

3. PAÍSES QUE OFRECEN UN NIVEL ADECUADO DE PROTECCIÓN SEGÚN LA COMISIÓN EUROPEA

Una vez analizado el documento WP 12 podemos pasar al estudio de aquellos países que tienen un nivel equiparable de protección. Sancho Villa la llama "política bilateral" en materia de transferencias de datos[37].

Tal como indica Guerrero Picó[38], "el peligro de fomentar siquiera indirectamente la existencia de paraísos de datos lleva a que las transferencias internacionales de datos personales sólo puedan efectuarse cuando se garantice un nivel de protección adecuado".

De acuerdo al artículo 33 de la LOPD no podrán realizarse transferencias de datos a terceros países que no proporcionen un nivel de protección equiparable, salvo que se obtenga autorización previa del Director de la Agencia Española de Protección de

[37] SANCHO VILLA, D: *Transferencia Internacional de Datos Personales*. Agencia Española de Protección de Datos, Madrid 2003, pág. 138.

[38] GUERRERO PICÓ, M. del C: "El Derecho Fundamental a la Protección de los Datos de Carácter Personal en la Constitución Europea". ReDCE, nº 4, julio-diciembre de 2005, pág. 307 y 308.

Datos[39]. El carácter adecuado del nivel de protección que ofrece el país de destino se evaluará por la Agencia Española de Protección de Datos.

En el artículo 34 se formulan una serie de excepciones a lo dispuesto en el artículo 33. Entre dichas excepciones nos interesa ahora la enumerada con la letra k: *Cuando la transferencia tenga como destino un Estado miembro de la Unión Europea, o un Estado respecto del cual la Comisión de las Comunidades Europeas, en el ejercicio de sus competencias, haya declarado que garantiza un nivel de protección adecuado*[40].

Como hace constar Cerda Silva[41], la Directiva 95/46/CE "no ha podido exigir un equivalente (i. e., exactamente el mismo) nivel de protección de terceros países, que no son miembros de la Unión Europea. Ésta les exige un nivel de protección menos fuerte: un nivel adecuado". Esto parece más realista como exigencia a terceros países, especialmente considerando que, de otro modo, la Directiva demandaría la adopción global del estándar de la Unión Europea.

De acuerdo al artículo 66.2.a) del RLOPD, no será necesaria la autorización del Director de la Agencia Española de Protección de Datos para aquellas transferencias en

[39] Incumplir esta disposición está castigado de forma muy dura en el artículo 44.4 de la LOPD. El importe de la multa será de 300.001 a 600.000 euros. Véase por ejemplo la resolución R/00189/2007 (procedimiento sancionador PS/00169/2006) de la AEPD (descargable en la web de la Agencia), donde se sanciona a una empresa que efectuaba transferencias internacionales de datos sin autorización del Director de la AEPD.

[40] Podemos clasificar a los países en tres categorías:

- Estados del Espacio Económico Europeo (países de la Unión Europea más Noruega, Islandia y Liechtenstein).
- Estados declarados con nivel adecuado de protección.
- Países terceros de los que no se ha declarado el nivel adecuado.

[41] CERDA SILVA, A: "El *Nivel Adecuado de Protección* para las Transferencias Internacionales de Datos Personales desde la Unión Europea". Revista de Derecho de la Pontificia Universidad Católica de Valparaíso, Chile, XXXVI (primer semestre de 2011), pág. 333 y 334.

las que el Estado en el que se encontrase el importador ofrezca un nivel adecuado de protección.

Hasta la promulgación del RLOPD tenían la consideración de países que ofrecen un nivel equiparable de protección todos los que forman parte del Espacio Económico Europeo (EEE)[42], es decir todos los países de la Unión Europea junto con Islandia, Liechtenstein y Noruega. El RLOPD entiende que las transferencias de datos a estos países no tienen la consideración de internacionales. Deben considerarse como simples cesiones o comunicaciones de datos[43]. Por lo tanto dejan de estar sujetas a las normas establecidas para las transferencias internacionales de datos, debiendo cumplir sencillamente con la regulación general de cualquier cesión o comunicación de datos.

Si los países del EEE quedan fuera de la regulación de las transferencias internacionales de datos, sólo vamos a encontrar dos vías para la determinación de los Estados que proporcionan un nivel adecuado de protección. La primera de dichas vías es la relación de países que se han beneficiado de una apreciación favorable por la Comisión Europea. La segunda vía es la posible apreciación favorable por parte de la AEPD.

[42] El Espacio Económico Europeo se constituyó por un acuerdo firmado el dos de mayo de 1992 (y que entró en vigor el uno de enero de 1994) entre los Estados miembros de la UE (compuesta en ese momento por doce naciones) y los seis países que formaban la Asociación Europea de Libre Comercio (AELC), excepto Suiza. Después de la entrada en la UE de tres estados de la AELC (Austria, Finlandia y Suecia a comienzos de 1995), Islandia, Noruega y Liechtenstein (que se unió a la AELC en mayo de 1995) pueden disfrutar de los beneficios del mercado único gracias al acuerdo de constitución del EEE.

[43] VERDAGUER LÓPEZ, J. y BERGAS JANÉ, M. A: *1000 Soluciones de Protección de Datos*. Editorial CISS. Valencia 2010, pág. 508.

En el artículo 34.k de la LOPD se dispone que no será necesaria la autorización del Director de la AEPD en el caso de transferencias internacionales de datos que tengan como destino un Estado respecto del cual la Comisión Europea, en el ejercicio de sus competencias, haya declarado que garantiza un nivel de protección adecuado. De igual forma se expresa el artículo 68 del RLOPD[44].

En el mismo sentido, de acuerdo con el artículo 25.6 de la Directiva 95/46/CE, la Comisión podrá hacer constar que un país tercero garantiza un nivel de protección adecuado, a la vista de su legislación interna o de sus compromisos internacionales, a efectos de protección de la vida privada o de las libertades o de los derechos fundamentales de las personas. Los Estados miembros adoptarán las medidas necesarias para ajustarse a la decisión de la Comisión.

La Directiva 95/46/CE reconoce que los flujos transfronterizos de datos son necesarios para el desarrollo del comercio internacional[45]. No se busca entonces una limitación indiscriminada de dichos flujos transfronterizos. Solo se impedirá la transferencia de datos a aquellos países que no garanticen un nivel de protección

[44] Artículo 68 del RLOPD: No será necesaria la autorización del Director de la Agencia Española de Protección de Datos para la realización de una transferencia internacional de datos que tuvieran por importador una persona o entidad, pública o privada, situada en el territorio de un Estado respecto del que se haya declarado por la Comisión Europea la existencia de un nivel adecuado de protección.

[45] Así queda de manifiesto en el considerando 56 de la Directiva: "que los flujos transfronterizos de datos personales son necesarios para el desarrollo del comercio internacional; que la protección de las personas garantizada en la Comunidad por la presente Directiva no se opone a la transferencia de datos personales a terceros países que garanticen un nivel de protección adecuado; que el carácter adecuado del nivel de protección ofrecido por un país tercero debe apreciarse teniendo en cuenta todas las circunstancias relacionadas con la transferencia o la categoría de transferencias".

adecuado[46]. Y ello lo podemos comprobar en el artículo 25.4 de la Directiva: cuando la Comisión compruebe que un tercer país no garantiza un nivel de protección adecuado, los Estados miembros adoptarán las medidas necesarias para impedir cualquier transferencia de datos personales al tercer país de que se trate.

La comprobación de que un tercer país garantiza un nivel de protección adecuado se llevará a cabo mediante el procedimiento establecido en el artículo 31.2 de la Directiva[47]. En la práctica este procedimiento supone: la propuesta de la Comisión, una opinión del Grupo del artículo 29 de la Directiva, una opinión del Comité del artículo 31 de la Directiva, un derecho de escrutinio de 30 días del Parlamento Europeo y la adopción de la decisión por el colegio de Comisarios.

[46] Tal como nos indica Jesús Rubí Navarrete, adjunto al Director de la AEPD, en su presentación sobre *Transferencia Internacional de Datos* (documento que se puede obtener en la web de la AEPD), para el Seminario de Cartagena de Indias del 14-16 de junio de 2011, se impedirá la transferencia de datos a aquellos países que no garantizan un nivel de protección adecuado siempre que no se cuente con alguna alternativa, como pueden ser las cláusulas contractuales tipo, BCR, Safe Harbor o alguna de las excepciones previstas en la LOPD y en la Directiva 95/46/CE.

[47] Artículo 31.2 de la Directiva: El representante de la Comisión presentará al Comité un proyecto de las medidas que se hayan de adoptar. El Comité emitirá su dictamen sobre dicho proyecto en un plazo que el presidente podrá determinar en función de la urgencia de la cuestión de que se trate.

El dictamen se emitirá según la mayoría prevista en el apartado 2 del artículo 148 del Tratado. Los votos de los representantes de los Estados miembros en el seno del Comité se ponderarán del modo establecido en el artículo anteriormente citado. El presidente no tomará parte en la votación.

La Comisión adoptará las medidas que serán de aplicación inmediata. Sin embargo, si dichas medidas no fueren conformes al dictamen del Comité, habrán de ser comunicadas sin demora por la Comisión al Consejo. En este caso:

la Comisión aplazará la aplicación de las medidas que ha decidido por un período de tres meses a partir de la fecha de dicha comunicación;

el Consejo, actuando por mayoría cualificada, podrá adoptar una decisión diferente dentro del plazo de tiempo mencionado en el primer guión.

Como afirma Argüello Téllez[48], es a través de esta herramienta que el "alcance de esta Directiva trasciende incluso las fronteras de sus Estados Miembros, a través de exigir a terceros países, la garantía de contar con un nivel adecuado de protección para que los datos personales provenientes de la Unión Europea puedan circular y ser tratados libremente dentro de sus fronteras". Pero es una realidad que esta *seguridad* queda prácticamente limitada a los países de la Unión y los pocos países a los que se ha reconocido un nivel de protección adecuado. "El resto de países pueden convertirse en un caldo de cultivo para la propagación de paraísos de datos".

Ser catalogado como país con nivel adecuado de protección no es sencillo. Normalmente exige que los países expidan regulaciones apropiadas y efectúen cambios institucionales. Adicionalmente, deben iniciar un trámite ante la Comisión Europea que según experiencias recientes, se demora un poco más de dos años[49]. Pese a ello hay países que están muy interesados en conseguir este estatus por la enorme rentabilidad económica que les puede representar: por ejemplo la India. En abril de 2012 este país ha pedido a la Unión Europea que levante las restricciones al flujo de procesos de deslocalización empresarial especializada y de alto valor añadido mediante su designación como país seguro en la protección de datos[50].

[48] ARGÜELLO TÉLLEZ, F: "La protección de datos personales en un mundo global". Conferencia que tuvo lugar el 16 de diciembre de 2004 en la sede de la Agencia Catalana de Protección de Datos. Accesible en la dirección electrónica **http://www.apd.cat/media/315.pdf**. En esta conferencia Argüello Téllez alaba el papel de España, a través de la AEPD, en la difusión del Derecho Fundamental a la protección de datos, a través de la creación de la Red Iberoamericana de Protección de Datos.

[49] REMOLINA ANGARITA, N. y otros: *Obligaciones y Contratos en el Derecho Contemporáneo*. Universidad de La Sabana. Bogotá 2010, pág. 386.

[50] Fuente: **www.indatimes.com** (16 de abril de 2012).

En sentido contrario, la Directiva 95/46/CE en su artículo 25.3 abre la posibilidad a que por parte de los Estados miembros y la Comisión se confeccionen *listas negras* de países que no garantizan un nivel de protección adecuado. Las consecuencias políticas que tendría la inclusión de países en estas listas ha impedido que se hayan puesto en práctica.

La Comisión ha reconocido el nivel adecuado de protección ofrecido por un grupo reducido de países:

- **Suiza**. Decisión 2000/518/CE, de 26 de julio de 2000, relativa al nivel de protección adecuado de los datos personales en Suiza (DOCE L 215 de 25 de agosto de 2000). El Grupo de Trabajo del artículo 29 de la Directiva emitió el Dictamen 5/99 -WP 22- de 7 de junio de 1999.

- **Estados Unidos**. Decisión 2000/520/CE, de 26 de julio de 2000, 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 (DOCE L 215 de 25 de agosto de 2000). El Grupo de Trabajo del artículo 29 de la Directiva emitió varios dictámenes:
    - Dictamen 1/99 -WP 15- de 26 de enero de 1999,
    - Dictamen 2/99 -WP 19- de 3 de mayo de 1999,
    - Dictamen 4/99 -WP 21- de 7 de junio de 1999,
    - Dictamen 7/99 -WP 27- de 3 de diciembre de 1999,
    - Dictamen 3/2000 -WP 31- de 16 de marzo de 2000 y
    - Dictamen 4/2000 -WP 32- de 16 de mayo de 2000.

- **Canadá**. Decisión 2002/2/CE, de 20 de diciembre de 2001, sobre la adecuación de la protección de los datos personales conferida por la ley canadiense *Personal Information and Electronic Documents Act* (DOCE L 2 de 4 de enero de 2002). El Grupo de Trabajo del artículo 29 de la Directiva emitió el Dictamen 2/2001 -WP 39- de 26 de enero de 2001.

- **Argentina**. Decisión 2003/490/CE, de 30 de junio de 2003, sobre la adecuación de la protección de datos personales en Argentina (DOUE L 168 de 5 de julio de 2003). El Grupo de Trabajo del artículo 29 de la Directiva emitió el Dictamen 4/2002 -WP 63- de 3 de octubre de 2002.

- **Guernesey**. Decisión 2003/821/CE, de 21 de noviembre de 2003, sobre la adecuación de la protección de datos en Guernesey (DOUE L 308 de 25 de noviembre de 2003). El Grupo de Trabajo del artículo 29 de la Directiva emitió el Dictamen 5/2003 -WP 79- de 13 de junio de 2003.

- **Isla de Man**. Decisión 2004/411/CE, de 28 de abril de 2004, relativa al carácter adecuado de la protección de los datos personales en la Isla de Man (DOUE L 151 de 30 de abril de 2004). El Grupo de Trabajo del artículo 29 de la Directiva emitió el Dictamen 6/2003 -WP 82- de 21 de noviembre de 2003.

- **Jersey**. Decisión 2008/393/CE, de 8 de mayo de 2008, relativa a la protección adecuada de los datos personales en Jersey (DOUE L 138 de 28 de mayo de 2008). El Grupo de Trabajo del artículo 29 de la Directiva emitió el Dictamen 8/2007 -WP 141- de 9 de octubre de 2007.

- **Islas Feroe**. Decisión 2010/146/UE, de 5 de marzo de 2010, relativa a la protección adecuada dada en la Ley de las Islas Feroe sobre el tratamiento de datos personales (DOUE L 58 de 9 de marzo de 2010). El Grupo de Trabajo del artículo 29 de la Directiva emitió el Dictamen 9/2007 -WP 142- de 9 de octubre de 2007.

- **Andorra**. Decisión 2010/625/UE, de 19 de octubre de 2010, relativa a la adecuada protección de los datos personales en Andorra (DOUE L 277 de 21 de octubre de 2010). El Grupo de Trabajo del artículo 29 de la Directiva emitió el Dictamen 7/2009 -WP 166- de 1 de diciembre de 2009.

- **Israel**. Decisión 2011/61/UE, de 31 de enero de 2011, relativa a la protección adecuada de los datos personales por el Estado de Israel en lo que respecta al tratamiento automatizado de los datos personales (DOUE L 27 de 1 de febrero de 2011). El Grupo de Trabajo del artículo 29 de la Directiva emitió el Dictamen 6/2009 -WP 165- de 1 de diciembre de 2009.

- **Uruguay**. Decisión 2012/484/UE, de 21 de agosto de 2012, relativa a la protección adecuada de los datos personales por la República Oriental del Uruguay en lo que respecta al tratamiento automatizado de datos personales (DOUE L 227 de 23 de agosto de 2012). El Grupo de Trabajo emitió el Dictamen 6/2010 -WP 177- de 12 de octubre de 2010.

- **Nueva Zelanda**. Decisión adoptada por la Comisión Europea[51] el 19 de diciembre de 2012, pero todavía no publicada en el DOUE en la fecha de finalización de

[51] Véase comunicado de prensa, Bruselas 19 de diciembre de 2012, referencia IP/12/1403.

esta tesis doctoral. El Grupo de Trabajo emitió el Dictamen 11/2011 -WP 182- de 4 de abril de 2011.

Está pendiente de reconocimiento del nivel adecuado de protección por parte de la Comisión, pese al dictamen favorable del Grupo de Trabajo del artículo 29 de la Directiva:

- **Principado de Mónaco**. Dictamen 07/2012 -WP 198- de 19 de julio de 2012.

Caso especial es el de **Hungría**. El Grupo de Trabajo emitió el Dictamen 6/99 -WP 24- de 7 de septiembre de 1999 sobre el nivel de protección de datos personales en Hungría. En el Dictamen el Grupo recomendaba a la Comisión y al Comité establecido por el artículo 31 de la Directiva 95/46/CE constatar que Hungría garantizaba un nivel de protección adecuado según lo dispuesto en el apartado 6 del artículo 25 de la Directiva. La Comisión por su parte, adoptó la Decisión 2000/519/CE, de 26 de julio de 2000, relativa a la protección adecuada de los datos personales en Hungría (DOCE L 215 de 25 de agosto de 2000). De acuerdo al artículo 1 de la Decisión, a los efectos del apartado 2 del artículo 25 de la Directiva 95/46/CE, para todas las actividades por ella cubiertas, se consideraba que Hungría garantizaba un nivel adecuado de protección de los datos personales transferidos desde la Unión Europea.

Tras la adhesión de Hungría a la Unión Europea el uno de mayo de 2004 la Decisión dejó de tener sentido, ya que, de acuerdo al artículo 1 de la Directiva 95/46/CE, no se podrá restringir ni prohibir la libre circulación de datos personales entre los Estados miembros[52]. En la normativa interna tenemos idéntica regulación ya que el

[52] Artículo 1 de la Directiva 95/46/CE:

artículo 34 k) de la LOPD exceptúa del régimen general de autorización el supuesto en que la transferencia tenga como destino un Estado miembro de la Unión Europea.

Como nos indica Remolina Angarita[53], Colombia y otros países latinoamericanos también buscan que la Comisión Europea los catalogue como un lugar que garantiza un nivel adecuado de protección de datos personales. Ello conlleva muchos beneficios para el país pues el flujo internacional de datos es un factor cardinal para el desarrollo de varias actividades, entre ellas los llamados *call centers*[54].

Las Decisiones de la Comisión sobre el nivel adecuado de protección las podemos dividir en dos tipos distintos. En el caso más general (Suiza, Argentina, Guernsey, Isla de Man, Jersey, Islas Feroe, Andorra, Israel y Uruguay), la Comisión reconoce el nivel adecuado de protección de toda la normativa del país, lo que conlleva la liberalización de todas las transferencias de datos, sin limitaciones de ninguna clase.

Objeto de la Directiva

1. Los Estados miembros garantizarán, con arreglo a las disposiciones de la presente Directiva, la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales.

2. Los Estados miembros no podrán restringir ni prohibir la libre circulación de datos personales entre los Estados miembros por motivos relacionados con la protección garantizada en virtud del apartado 1.

[53] REMOLINA ANGARITA, N. y otros: *Obligaciones y Contratos en el Derecho Contemporáneo*. Biblioteca Jurídica Diké y Universidad de La Sabana. Bogotá 2010, pág. 380.

[54] Un *call center*, es un centro de atención de llamadas telefónicas. Dichos centros disponen de una serie de personas que se dedican a atender llamadas o a realizar llamadas o incluso a ambas tareas. El fin de estas llamadas puede tener diversos objetivos: departamentos de atención a clientes, atención a reclamaciones, asistencias y soportes técnicos, departamentos que hacen encuestas, empresas de telemarketing, etc.

En el caso de Estados Unidos y Canadá, las Decisiones de la Comisión reconocen su nivel de protección adecuada solamente de forma limitada. Mientras que la Decisión referente a Estados Unidos reconoce un nivel de protección adecuada sólo a los destinatarios acogidos al sistema de *puerto seguro*, la Decisión que afecta a Canadá reconoce un nivel de protección adecuada sólo a aquellos destinatarios a los que se aplica la *Personal Information and Electronic Documents Act*.

3.1. LAS TRANSFERENCIAS INTERNACIONALES DE DATOS A ESTADOS UNIDOS

En el momento en que entró en vigor en la Unión Europea la Directiva relativa a la protección de datos, surgió un problema muy importante con los Estados Unidos.

La Directiva sólo permite la transferencia de datos personales a aquellos países que ofrezcan un nivel adecuado de protección de la vida privada. Pero Estados Unidos no tiene una regulación completa de carácter general sobre la materia. Ello implica que no se puede considerar que Estados Unidos ofrezca un nivel adecuado de protección de la vida privada. Tal como indica Aced Félez, mientras que para la UE la protección de datos personales es un derecho fundamental de los ciudadanos, “en Estados Unidos la protección de datos se considera un elemento disponible por parte de los ciudadanos, regulado parcialmente en una multitud de normas específicas y sectoriales sin conexión entre ellas, poniéndose casi todo el énfasis en la autorregulación y sin que exista una autoridad o autoridades de control encargadas de garantizar eficazmente el

cumplimiento de las reglas y la aplicación de unos estándares universalmente aceptados"[55].

La Unión Europea y los Estados Unidos iniciaron en 1999 las negociaciones para encontrar un sistema que permitiese la declaración de adecuación del nivel de protección de datos personales en este último país.

El Departamento de Comercio de los Estados Unidos presentó una propuesta en la que se establecían los *Principios de Puerto Seguro*. En base a esta propuesta, los operadores que se adhiriesen a dichos *Principios* tendrían una presunción de adecuación a las exigencias de la Directiva 95/46/CE. Se obtendría así un mecanismo que permitiría la libre transferencia de datos personales a dichos operadores.

Los operadores deberían manifestar ante la Oficina Federal de Comercio, u otro organismo que ella hubiera designado, la adhesión a los Principios de Puerto Seguro y su compromiso de llevarlos a la práctica.

Los Principios de Puerto Seguro se publicaron por el Departamento de Comercio de Estados Unidos el 21 de julio de 2000[56]. Forman un conjunto de siete principios básicos:

- **Notificación**. Las entidades informarán a los particulares de los fines con los que recogen y utilizan información sobre ellos; la forma de contactar con ellas para cualquier pregunta o queja; los tipos de terceros a los cuales se revelará la información;

[55] ACED FÉLEZ, E: "Transferencias internacionales de datos personales entre Europa y USA". Ponencia del II Congreso Mundial de Derecho Informático. Madrid, 23 a 27 de septiembre de 2002. El documento se encuentra en la dirección electrónica:

http://www.ieid.org/congreso/ponencias/Aced,%20Emilio.pdf

[56] Se publicaron también en el DOCE L 215 de 25 de agosto de 2000, junto a la Decisión de la Comisión sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada.

las opciones y medios que la entidad ofrece a los particulares para limitar su uso y su divulgación. La notificación se hará en lenguaje claro y transparente la primera vez que se invite a los particulares a proporcionar a la entidad información personal o, posteriormente, tan pronto como sea posible, pero en cualquier caso antes de que la entidad use dicha información para un fin distinto de aquel con el que inicialmente la recogió o trató la entidad que la transfiere o la divulga por primera vez a un tercero[57].

- **Opción**. Las entidades ofrecerán a los particulares la posibilidad de decidir (ser excluido) si su información personal: a) puede divulgarse a un tercero[58] o bien b) puede usarse para un fin incompatible con el objetivo inicial con el que fue recogida o no haya sido autorizado posteriormente por el particular. Se deben proporcionar a los particulares mecanismos claros y transparentes, fácilmente disponibles y asequibles para ejercer su derecho de opción. Si se trata de información delicada, como datos sobre el estado de salud, el origen racial o étnico, las opiniones políticas, las creencias religiosas o filosóficas, la afiliación sindical o la vida sexual de la persona, la opción de participar será afirmativa o explícita (aceptación) si la información va a revelarse a un tercero o a utilizarse para un fin distinto del que inicialmente motivó la recogida de información o de una manera distinta a la autorizada con posterioridad por éste al optar por la «aceptación». En cualquier caso, una entidad debe tratar como delicada toda

[57] La notificación no es necesaria cuando la información se revela a un tercero que ejecute un cometido, como agente, en nombre y bajo instrucciones de la entidad. No obstante, en este caso sí se aplica el principio de transferencia ulterior.

[58] La opción, al igual que la notificación, no es necesaria cuando la información se revela a un tercero que ejecute un cometido, como agente, en nombre y bajo instrucciones de la entidad. No obstante, en este caso sí se aplica el principio de transferencia ulterior.

información recibida de un tercero cuando dicho tercero la identifique y la trate como información delicada.

- **Transferencia ulterior**. Para revelar información a terceros, las entidades deberán aplicar los principios de notificación y opción. Cuando una entidad desee transferir los datos a un tercero que actúe como agente, podrá hacerlo si previamente se asegura de que éste suscribe los principios, si es objeto de una resolución sobre su «adecuación» con arreglo a la Directiva u otra disposición o si firma con él un convenio por escrito para que ofrezca como mínimo el mismo nivel de protección de la vida privada que el requerido por dichos principios. Si la entidad cumple estos requisitos, no será responsable (a menos que la propia entidad acuerde lo contrario) del tratamiento realizado por el tercero a quien haya transferido este tipo de información y que vulnere las limitaciones o estipulaciones establecidas, a menos que la entidad sepa, o debiera saber, que el tercero realizaría dicho tratamiento y no haya adoptado medidas razonables para impedir o detener tal tratamiento.

- **Seguridad**. Las entidades que creen, mantengan, utilicen o difundan información personal tomarán precauciones razonables para evitar su pérdida, su mal uso y consulta no autorizada, su divulgación, su modificación y su destrucción.

- **Integridad de los datos**. De acuerdo con los principios, la información personal debe ser pertinente para los fines con los que se utiliza. Una entidad no podrá tratar la información personal de manera incompatible con los fines que motivaron su recogida o aprobó posteriormente el particular. En la medida necesaria para alcanzar dichos fines, las entidades adoptarán medidas razonables para que los datos tengan fiabilidad para el uso previsto y sean exactos, completos y actuales.

- **Acceso**. Los particulares deberán tener acceso a la información personal que las entidades tengan sobre ellos y poder corregir, modificar o suprimir dicha información si resultase inexacta, excepto en dos casos: cuando permitir el acceso suponga una carga o dispendio desproporcionado en relación con los riesgos que el asunto en cuestión conlleve para la vida privada de la persona; o cuando puedan vulnerarse los derechos de otras personas.

- **Aplicación**. Una protección eficaz de la vida privada debe incluir mecanismos para garantizar la conformidad con los principios, una vía de recurso para las personas a que se refieran los datos y se vean afectadas por el incumplimiento de dichos principios y sanciones contra la entidad incumplidora. Como mínimo, tales mecanismos deben incluir:

a) una vía de recurso independiente, asequible e inmediatamente disponible para investigar y resolver con arreglo a los principios las denuncias y litigios de los particulares y otorgar daños y perjuicios donde determinen la legislación aplicable o las iniciativas del sector privado;
b) procedimientos de seguimiento para comprobar que los certificados y declaraciones de las empresas sobre sus prácticas en materia de vida privada se ajustan a la verdad y que dichas prácticas se aplican en consecuencia; y
c) obligación de subsanar los problemas derivados del incumplimiento de los principios para las entidades que se hayan adherido a ellos y las sanciones correspondientes contra ellas, que serán lo suficientemente rigurosas para garantizar su cumplimiento.

La Unión Europea reconoce la competencia de los siguientes organismos públicos estadounidenses para investigar las quejas y solicitar medidas provisionales contra las prácticas desleales o fraudulentas, en caso de incumplimiento en la aplicación de los principios:

- Comisión Federal de Comercio (Federal Trade Commission, FTC) con arreglo a la competencia que le confiere el artículo 5 de la Ley de la Comisión Federal de Comercio,
- Departamento de Transporte con arreglo a la competencia que le confiere el artículo 41712 del título 49 del United States Code.

Como se había mencionado anteriormente, junto a los principios de puerto seguro, el Departamento de Comercio publicó las correspondientes preguntas más frecuentes, con el fin de aclarar el contenido de los principios. Dichas preguntas están referidas a los siguientes asuntos:

- Datos especialmente protegidos.
- Excepciones del periodismo.
- Responsabilidad subsidiaria.
- Bancos de inversiones y sociedades de auditoría.
- La función de las autoridades de protección de datos.
- Autocertificación.
- Verificación.
- Acceso.
- Recursos humanos.

- Contratos para la transferencia de datos de la Unión Europea a Estados Unidos exclusivamente para tratamiento.
- Resolución de litigios y ejecución.
- Opción – Momento de la exclusión.
- Información sobre viajes.
- Productos médicos y farmacéuticos.
- Información extraída de registros públicos e información de dominio público.

La Decisión 2000/520/CE de 26 de julio de 2000 de la Comisión considera que los principios de puerto seguro, aplicados de conformidad con la orientación que proporcionan las preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos, garantizan un nivel adecuado de protección de los datos personales transferidos desde la Unión Europea a entidades establecidas en Estados Unidos de América. Para garantizar que la Decisión se aplique correctamente, es necesario que las entidades que suscriban los principios y las preguntas más frecuentes, puedan ser reconocidas por los interesados. Para ello, el Departamento de Comercio de Estados Unidos o su representante debe comprometerse a mantener y poner a disposición del público una lista de las entidades[59] que autocertifiquen su adhesión a los principios y su aplicación de conformidad con las preguntas más frecuentes y que estén sujetos a la jurisdicción de cómo mínimo uno de los siguientes organismos públicos: la Comisión Federal de Comercio o el Departamento de Transporte de Estados Unidos de América.

[59] El Departamento de Comercio de Estados Unidos permite la consulta de las entidades que están adheridas a través de la siguiente página web: **https://safeharbor.export.gov/list.aspx**

Si tenemos en cuenta las normas internas españolas, en la Instrucción 1/2000[60], de uno de diciembre, de la Agencia de Protección de Datos, relativa a las normas por las que se rigen los movimientos internacionales de datos[61], encontramos las obligaciones de quien pretenda efectuar una transferencia de datos a los Estados Unidos en base a la Decisión de la Comisión. Tal como indica Davara Rodríguez, en la Instrucción 1/2000 se recoge la línea doctrinal de la Agencia Española de Protección de Datos en materia de transferencias a terceros países[62]. De acuerdo al punto 3 de la Norma cuarta, si la transferencia se funda en lo establecido en la Decisión 2000/520/CE de la Comisión, quien pretenda efectuar la transferencia deberá acreditar que el destinatario se encuentra entre las entidades que se han adherido a los principios de Puerto Seguro, así como que el mismo se encuentra sujeto a la jurisdicción de uno de los organismos públicos estadounidenses que figuran en el Anexo VII de la citada Decisión[63].

[60] La Sentencia de la Audiencia Nacional (Sala de lo Contencioso-Administrativo, Sección Primera), de 15 de marzo de 2002, en relación con la Instrucción 1/2000, anuló el apartado 2) de la Norma Tercera y la Norma Sexta de dicha Instrucción, si bien ambos únicamente en cuanto pretenden extender su aplicación a las transferencias internacionales de datos comprendidas en los supuestos de excepción del artículo 34 de la LOPD, y anuló también el apartado 1) de la Norma Cuarta de la misma Instrucción.

[61] BOE del 16 de diciembre de 2000.

[62] DAVARA RODRÍGUEZ, M. A: *El abogado y la protección de datos*. Ilustre Colegio de Abogados de Madrid. Madrid 2004, pág. 34.

[63] El mismo criterio se encuentra en el Informe Jurídico 0108/2008 de la AEPD: "sólo las empresas que están formalmente adheridas a puerto seguro y que aparecen recogidas en la página web http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list, tendrán la consideración de empresas adheridas a puerto seguro, y por ello, no necesitarán autorización del Director de la Agencia para efectuar la transferencia dado que la Comisión Europea ha declarado que tienen nivel adecuado de protección, debiendo sólo notificar la transferencia al Registro General de Protección de Datos". Documento disponible en la página electrónica de la AEPD: **https://www.agpd.es/**

El Grupo de Trabajo sobre protección de datos del artículo 29, en su Dictamen 4/2000 -WP 32- sobre el nivel de protección que proporcionan los "principios de puerto seguro", aprobado el 16 de mayo de 2000, expresó su posición crítica al acuerdo con Estados Unidos. Opina el Grupo de Trabajo que habría sido posible conseguir un mayor nivel de protección de los datos. En particular cree conveniente que se introduzcan mejoras para conseguir los siguientes objetivos:

- Claridad absoluta sobre el alcance del puerto seguro: por un lado, en términos de la legislación aplicable y, por otro, en términos de la jurisdicción de la Comisión Federal de Comercio.
- Limitación del número de excepciones introducidas por las preguntas más frecuentes y por el apartado 5 de los principios (la adhesión a estos principios puede limitarse por disposición legal o reglamentaria, o por jurisprudencia que originen conflictos de obligaciones o autorizaciones explícitas).
- Garantías adecuadas de recurso a título individual. El sistema adolece de insuficiencia en dos de las tres condiciones que indica el Grupo de Trabajo en su documento de trabajo WP 12, de 24 de julio de 1998: la necesidad de ofrecer apoyo y asistencia a los interesados (letra b) y de ofrecer vías adecuadas de recurso a quienes resulten perjudicados en el caso de que no se observen las normas (letra c).

Como bien señala Arenas Ramiro, "a pesar de las modificaciones del régimen jurídico del tratamiento de datos personales incorporada tras los atentados del 11 de

septiembre, Estados Unidos sigue estando en la *lista blanca* de países a los que Europa puede transmitir datos personales"[64].

3.2. LAS TRANSFERENCIAS INTERNACIONALES DE DATOS A CANADÁ

La Ley canadiense sobre datos personales y documentos electrónicos *Personal Information and Electronic Documents Act* de 13 de abril de 2000 se aplica a las entidades privadas que recojan, utilicen o divulguen datos personales en sus actividades comerciales. Entró en vigor en tres etapas:

A partir del 1 de enero de 2001, la Ley canadiense se aplica a los datos personales, excluidos los de carácter sanitario, que las entidades que operen como «empresa federal» recojan, utilicen o divulguen en el transcurso de sus actividades económicas. Dichas empresas operan en sectores como el transporte aéreo, la banca, la radiotelevisión, el transporte interprovincial y las telecomunicaciones. También se aplica a todas las entidades que comercian con datos personales fuera de su provincia o fuera del Canadá y a los datos laborales sobre los asalariados de las empresas federales[65].

A partir del 1 de enero de 2002, se aplica a los datos personales sanitarios de las entidades y actividades ya cubiertos en la primera etapa.

A partir del 1 de enero de 2004, se amplía a cualquier organismo que recoja, utilice o divulgue datos personales en el transcurso de una actividad comercial dentro de una provincia, independientemente de que dicho organismo esté o no regulado a escala

[64] ARENAS RAMIRO, M: *El derecho fundamental a la protección de datos personales en Europa*. Tirant lo Blanc. Valencia 2006, pág. 336.

[65] Es bueno recordar que Canadá es una federación compuesta de diez provincias y tres territorios.

federal. No están sujetas a la Ley canadiense las entidades a quienes se aplique la *Federal Privacy Act* o se regulen por el sector público de ámbito provincial. Del mismo modo, las actividades filantrópicas o sin fines lucrativos tampoco están sujetas a la Ley canadiense a no ser que tengan carácter comercial. No se aplica, por último, a los datos laborales utilizados con fines no comerciales siempre que no se refieran a los asalariados del sector privado sujeto a regulación federal. En tales casos, la autoridad canadiense de protección de la vida privada podrá proporcionar información adicional.

El Grupo de Trabajo sobre protección de datos del artículo 29, en su Dictamen 2/2001 -WP 39- sobre el nivel adecuado de protección de la ley canadiense *Personal Information and Electronic Documents Act*, hace una serie de consideraciones:

- Las organizaciones no lucrativas o caritativas no están sujetas a la Ley, salvo si se dedican a una actividad comercial.
- Los datos sensibles (identificados en el artículo 8 de la Directiva) no están identificados como tales, sino que tomarán esa consideración según el contexto en el que se utilizan. No hay una prohibición de recoger estos datos.
- En las transmisiones de datos al exterior del Canadá, el Grupo de Trabajo considera que se debería requerir la utilización de un contrato u otra medida obligatoria que pueda ofrecer un nivel de protección comparable, animando a las autoridades canadienses a establecer orientaciones en tal sentido.
- Si una provincia aprueba una Ley considerada *básicamente similar* a la Ley federal, los organismos o actividades cubiertos por la Ley provincial dejan de estar sujetos a la Ley federal en sus transacciones dentro de esa provincia. La Ley federal seguirá aplicándose a toda recogida, utilización o divulgación de datos interprovincial e internacional.

En vista a todas las limitaciones expuestas, el Grupo de Trabajo llegó a unas conclusiones en las que exponía sus dudas sobre la adecuación de la Ley canadiense.

Entre otros aspectos, recomendaba que cualquier resolución sobre la idoneidad del nivel de protección de la *Personal Information and Electronic Documents Act* reflejase sus limitaciones en cuanto a su ámbito y calendario de aplicación.

Asimismo, el Grupo de Trabajo solicitaba a la Comisión y al Comité del artículo 31 que examinasen el procedimiento de definición del concepto de «básicamente similar» y que considerasen si lo más apropiado era reconocer a cada Ley provincial un nivel adecuado de protección o si podría alcanzarse el mismo objetivo a escala federal mediante un decreto del Consejo.

Para finalizar, el Grupo de Trabajo vería con agrado toda iniciativa por parte de las autoridades canadienses tendente a ofrecer la máxima protección posible de los datos delicados y a garantizar un nivel de protección comparable en el caso de la transmisión de datos desde el Canadá al exterior.

Pese a las limitaciones expuestas anteriormente, de acuerdo al artículo 1 de la Decisión de la Comisión 2002/2/CE, Canadá garantiza un nivel adecuado de protección de los datos personales transferidos desde la Unión Europea a los receptores sujetos a la *Personal Information Protection and Electronic Documents Act.* Podemos tomar esta afirmación en sentido inverso: NO se garantiza un nivel adecuado de protección de los datos personales transferidos desde la Unión Europea a los receptores que NO están sujetos a la *Personal Information Protection and Electronic Documents Act.* Por dicho

motivo, “si el destinatario no está sujeto a dicha Ley la transferencia requerirá autorización del Director de la AEPD”[66].

3.3. LAS TRANSFERENCIAS INTERNACIONALES DE DATOS A LOS DEMÁS PAÍSES QUE OFRECEN UN NIVEL ADECUADO DE PROTECCIÓN

El Grupo de Trabajo sobre protección de datos del artículo 29, en varios de sus Dictámenes recuerda que adecuación no significa una equivalencia completa con el nivel de protección establecido por la Directiva 95/46/CE[67].

Ello supone que en los diferentes Dictámenes del Grupo de Trabajo se haga referencia a los puntos débiles de mayor relevancia que se producen en las normativas de los distintos países analizados.

Suiza

En el caso de Suiza, el Dictamen 5/99 efectúa precisiones acerca del principio de transparencia y de la protección de datos sensibles en la ley federal. En cuanto a la situación de los Cantones suizos, considera que la situación es más difícil de evaluar.

De los 26 Cantones con que cuenta la Confederación:

- 17 disponen de legislación propia en cuanto a protección de los datos; tres de ellos, por otra parte, introducen una disposición de protección de los datos en su constitución cantonal;

[66] VERDAGUER LÓPEZ, J. y BERGAS JANÉ, M. A: *1000 Soluciones de Protección de Datos*. Editorial CISS. Valencia 2010, pág. 512.

[67] Véase por ejemplo los *resultados de la evaluación* en el Dictamen 8/2007 sobre el nivel de protección de los datos personales en Jersey.

- 4 han adoptado directivas gubernamentales; dos también han introducido una disposición en su constitución cantonal y uno de ellos tiene un proyecto de ley;

- los demás cantones no tienen normativa cantonal específica (tres de ellos están desarrollando un proyecto de ley).

En el estudio de las legislaciones adoptadas por los cantones se comprueba que se inspiran ampliamente en el Convenio 108, lo que es coherente con los compromisos de Suiza que resultan de su ratificación del Convenio.

Argentina

En el caso de Argentina, el Dictamen 4/2002 efectúa varias consideraciones. En materia de transferencias sucesivas a otros terceros países, la Ley argentina las prohíbe cuando este último país no garantice un nivel de protección adecuado. Sin embargo incluye excepciones a dicho principio más amplias que las previstas en la Directiva comunitaria. El Grupo de Trabajo *lamenta este hecho, preferiría que se limitaran dichas excepciones e invita al Gobierno argentino a trabajar en este sentido.*

En cuanto al órgano de control de protección de datos, el Grupo de Trabajo resalta que el Director del órgano de control de protección de datos es designado y puede ser destituido por el Ministerio de Justicia y Derechos Humanos, que también decide sobre el personal de dicho organismo, integrado en la estructura del Ministerio de Justicia. El Grupo de Trabajo considera que *tal situación no garantiza que el organismo pueda actuar con plena independencia y, por tanto, insta a implementar los elementos necesarios a tal efecto, incluido un cambio en el procedimiento para designar y destituir al Director del organismo.*

El Grupo de Trabajo entiende que en los casos en que los registros, archivos o bancos de datos están bajo jurisdicción provincial y, por tanto, fuera de la jurisdicción de la Dirección Nacional de Protección de Datos Personales, deberían existir órganos de protección provinciales. El Grupo de Trabajo *invita a crear órganos de control de protección de datos en todas las provincias*, ya que es importante para garantizar que en todos los casos exista un sistema de verificación directo por parte de la administración y un mecanismo institucional que permita investigar las denuncias de manera independiente de la vía judicial.

Por otra parte, el artículo 5 de la Ley argentina permite el tratamiento de datos personales sin el consentimiento del titular de los datos si los datos se obtienen de fuentes de acceso público irrestricto. El Grupo de Trabajo considera que es necesario establecer normas que garanticen que los datos incluidos en una fuente de acceso público irrestricto sean de tal naturaleza que no sea probable que su tratamiento sin el consentimiento del titular pueda suponer un riesgo para los derechos fundamentales y las libertades del individuo y, concretamente, para su derecho a la intimidad.

Jersey

En el caso de Jersey, el Dictamen 8/2007 efectúa varias consideraciones a tener en cuenta. Por una parte, la definición de lo que son datos de carácter personal de su Ley difiere de la adoptada en la Directiva comunitaria. En cuanto a la Oficina del Comisario responsable de la protección de datos, el Grupo de Trabajo muestra su preocupación por los escasos poderes de la Comisión, lo que plantea ciertas dudas sobre la conveniencia del Comisario como instrumento para lograr un buen nivel de cumplimiento.

El Grupo de Trabajo, en sus resultados de la evaluación, manifiesta que aunque puede haber ciertas dudas en el sentido de si la Ley de Jersey cumple plenamente los requisitos impuestos a los Estados miembros por la Directiva sobre protección de datos, recuerda que adecuación no significa una equivalencia completa con el nivel de protección establecido por la Directiva. Concluyendo que no considera que las limitaciones sean significativas en relación con la protección de los datos personales transferidos desde Estados miembros de la UE a Jersey.

Israel

En el caso de Israel, el Dictamen 6/2009 considera que su normativa tiene un nivel adecuado de protección. Sin embargo el Grupo de Trabajo exhorta a las autoridades israelíes a que, en futuros cambios legislativos, adopten disposiciones que establezcan:

- La aplicación de la legislación israelí a las bases de datos manuales, a fin de ampliar la evaluación de adecuación a aquellos casos que no se han incluido en las conclusiones del dictamen.
- La aplicación explícita del principio de proporcionalidad en relación con la totalidad del tratamiento de datos personales realizado por el sector privado.
- Una interpretación de las excepciones en las transferencias internacionales de datos en línea que se ajuste a lo dispuesto en el artículo 26, apartado 1, de la Directiva.

Nueva Zelanda

El Grupo de Trabajo en su Dictamen 11/2011 considera que Nueva Zelanda garantiza un nivel de protección adecuado. Sin embargo anima a las autoridades

neozelandesas a adoptar las medidas necesarias para subsanar las deficiencias del actual marco jurídico. En particular, anima al Comisario para la intimidad a seguir solicitando el refuerzo de la normativa relativa a la comercialización directa; y a seguir manteniendo una supervisión eficaz de las transferencias desde Nueva Zelanda a los terceros países que no están sujetos a una decisión de adecuación. El Grupo de Trabajo también solicita que, además de tener en cuenta las directrices OCDE y la Directiva UE, el Comisario para la intimidad considere asimismo las decisiones pertinentes de la Comisión Europea y las directrices del Grupo de Trabajo del artículo 29 a la hora de dictar órdenes de decisión de transferencia.

Mónaco

Está pendiente de reconocimiento del nivel adecuado de protección por parte de la Comisión. El Grupo de Trabajo en su Dictamen 07/2012 considera que Mónaco garantiza un nivel de protección adecuado. Aun así, alienta a sus autoridades a tener en cuenta una serie de recomendaciones, de las que destacamos:

- La incorporación de definiciones de conceptos que no aparecen en su normativa.
- La necesidad de aclarar la aplicación de la ley a las personas jurídicas.
- La necesidad de aclarar el derecho de los interesados a ser informados de manera oportuna (especialmente cuando los datos no se obtienen directamente de ellos).
- La conveniencia de mejorar las competencias de ejecución que corresponden a la autoridad de control.

Guernesey, Isla de Man, Islas Feroe, Andorra y Uruguay

El Grupo de Trabajo no menciona limitaciones relevantes en su normativa.

4. TRANSMISIÓN DE DATOS DE LOS PASAJEROS

Tras los acontecimientos del 11 de septiembre de 2001, los Estados Unidos (y poco después Australia y Canadá) adoptaron una serie de normas que exigen a las compañías aéreas que operen vuelos con destino a su territorio que transfieran a la administración pertinente datos personales relativos a los pasajeros y los miembros de la tripulación de los vuelos con destino u origen en ese país. Especialmente en el llamado *registro de nombres de los pasajeros* (PNR) se exigen datos de tipo muy amplio y variado[68]. Si no se facilita esta información, o ésta es incorrecta o incompleta, se contempla la aplicación de fuertes sanciones penales, especialmente la pérdida de derechos de aterrizaje y el pago de cuantiosas multas.

[68] Tal como se indica en el Dictamen 6/2002 del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, pueden referirse a datos identificativos (apellidos, nombre, fecha de nacimiento, número de teléfono), número de reserva del PNR, fecha de la reserva, la agencia de viajes cuando corresponda, la información que se muestra en el billete, los datos financieros (número de tarjeta de crédito, fecha de caducidad, dirección del lugar de expedición, etc.), el itinerario, información sobre el transportista que opera el vuelo (número de vuelo, etc.), número de asiento y datos anteriores del PNR. En estos últimos pueden constar no solo los viajes completados en el pasado, sino también información de carácter religioso o étnico (elección de la comida, etc.), afiliación a un determinado grupo, datos relativos al lugar de residencia o los medios para contactar con una persona (dirección de correo electrónico, información sobre un amigo, lugar de trabajo, etc.), datos médicos (cualquier asistencia médica que se haya requerido, oxígeno, problemas relacionados con la vista, el oído o la movilidad, o cualquier otro problema que deba hacerse saber para garantizar un vuelo satisfactorio) y otros datos relacionados, por ejemplo, con los programas de viajeros frecuentes (*Frequent Fliers number*). Asimismo, para los países que participan en el programa de derogación de visados («*Visa Waiver Program*»), la transferencia de datos biométricos debe convertirse en obligatoria antes de octubre de 2004.

4.1. TRANSMISIÓN DE DATOS DE LOS PASAJEROS A LOS ESTADOS UNIDOS

La transmisión de datos de los pasajeros hace surgir un grave problema en materia de protección de datos. Los datos facilitados por las compañías aéreas se refieren a personas físicas identificadas. Estos datos son tratados por compañías en la Unión Europea, y por lo tanto están protegidos por las disposiciones de la Directiva 95/46/CE. Sin embargo, tal como se indica en el Dictamen 6/2002 del Grupo de Trabajo, la mayoría de las cuestiones en juego se encuentran fuera de la competencia de las compañías aéreas. Deben ser los Estados miembros, y la Comisión si resulta necesario, quienes se ocupen de ellas. El sistema debería negociarse con las autoridades estadounidenses, debiendo centrarse las mismas en: aclarar y definir los objetivos, las finalidades y los receptores de los datos, las categorías de los datos que puedan transferirse y las condiciones y garantías que rodean al tratamiento de datos personales, en particular su envío a las autoridades federales de los EE.UU. (y, si éste se produce, limitarlo a autoridades de las fuerzas de seguridad).

En el Dictamen 4/2003 del Grupo de Trabajo, relativo al nivel de protección garantizado en los EE.UU. para la transferencia de datos de pasajeros, se analiza, entre otros, el documento recibido de la Comisión con fecha 22 de mayo de 2003. Dicho documento de *compromiso* fue emitido por el *Servicio de aduanas y protección de fronteras de Estados Unidos* y la *Administración estadounidense para la seguridad de los transportes*. Los compromisos contraídos por las autoridades estadounidenses tenían como fin que la Comisión adoptase una Decisión que declarase que el nivel de protección era adecuado, de acuerdo al artículo 25.6 de la Directiva 95/46/CE.

El Grupo de Trabajo entiende que estos compromisos constituyen el resultado logrado hasta la fecha en las negociaciones en curso entre la administración estadounidense y la Comisión, y que ésta debe seguir presionando a la parte estadounidense para tratar de avanzar con respecto a una serie de cuestiones.

Tras analizar los compromisos adquiridos y la legislación de EE.UU. sobre la materia, en el Dictamen se expone la preocupación que, desde la perspectiva de la protección de los datos, suscita en el Grupo la evaluación del nivel de protección garantizado en los EE.UU. con vistas a una posible Decisión de la Comisión. El objetivo general es establecer, lo antes posible, un marco jurídico claro para todas las transferencias de datos de las compañías aéreas a los EE.UU. que sea compatible con los principios relativos a la protección de los datos. Aunque reconoce que en última instancia habrá que atender a consideraciones de carácter político, el Grupo insta a la Comisión a tener sus opiniones plenamente en cuenta en las negociaciones con las autoridades estadounidenses.

El Grupo de Trabajo emitió nuevo Dictamen 2/2004, de 29 de enero de 2004, sobre el carácter adecuado de la protección de los datos personales incluidos en los registros de nombres de los pasajeros (*Passenger Name Records*, PNR) que se transfieren al Servicio de aduanas y protección de fronteras de Estados Unidos (*Bureau of Customs and Border Protection*, CBP). El Grupo de Trabajo considera que conviene emitir un nuevo dictamen habida cuenta de los últimos acontecimientos relativos a la transferencia de datos del PNR sobre los pasajeros, y, en particular, de los resultados de las negociaciones entre la Comisión Europea y las autoridades estadounidenses.

En el Dictamen se insiste en que las libertades y los derechos fundamentales relativos a los principios de protección de datos que rigen el tratamiento de los datos

personales en la Unión Europea sólo deben restringirse cuando sea necesario en una sociedad democrática y a los efectos de protección de intereses públicos que se enumeran en la Directiva 95/46/CE y el artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos, y se consagran en los artículos 7 y 8 de la Carta de Derechos Fundamentales de la Unión Europea.

El Grupo de Trabajo después de un nuevo análisis, toma buena nota de los progresos registrados en el diálogo EE.UU./UE sobre los datos del PNR. En particular, en la última versión de los Compromisos, de 12 de enero de 2004, presentados por la administración estadounidense. Se congratula de las mejoras que implica en relación con la versión anterior. No obstante, considera que estos progresos no permiten concluir que se ha alcanzado un nivel adecuado de protección de los datos.

El Grupo de Trabajo sostiene que cualquier solución debe respetar, al menos, los siguientes principios de protección de datos:

a) Calidad de los datos:

- la finalidad de la transferencia de datos debe ser únicamente la lucha contra los actos de terrorismo y determinados delitos conexos que habrá que definir;
- la lista de los datos que deben transferirse debe ser proporcionada y no excesiva;
- el cotejo de datos con los de personas sospechosas debe atenerse a normas de elevada calidad que garanticen la certeza de los resultados;
- los períodos de conservación de los datos deben ser cortos y proporcionados;

- los datos de los pasajeros no deben utilizarse para implantar y/o probar el sistema CAPPS II (*Computer Assisted Passenger Pre-Screening System*)[69] o sistemas similares.

b) Los datos sensibles no deben transmitirse.

c) Derechos de los interesados:

- debe facilitarse a los pasajeros información clara, actual y comprensible;
- debe garantizarse sin discriminación un derecho de acceso y rectificación;
- deben preverse disposiciones suficientes que garanticen a los pasajeros el acceso a un mecanismo de recurso verdaderamente independiente.

d) Nivel de compromiso de las autoridades estadounidenses:

- los compromisos asumidos por las autoridades estadounidenses deben ser plenamente vinculantes para Estados Unidos;
- procede clarificar el ámbito de aplicación, la base jurídica y el valor de un posible «acuerdo internacional ligero».

e) Las transferencias posteriores de datos del PNR a otras administraciones o autoridades extranjeras deben limitarse estrictamente.

f) Método de transferencia: conviene establecer un método de transferencia «push», es decir, que los datos sean seleccionados y transferidos por las compañías aéreas a las autoridades estadounidenses.

[69] El CAPPS II coteja la identificación de cada pasajero con los registros de actividades criminales y las listas de sospechosos compiladas por las agencias de espionaje y asigna a cada viajero un color según su peligrosidad: verde, amarillo o rojo.

El uno de marzo de 2004 la Comisión sometió a la consideración del Parlamento el proyecto de Decisión sobre el carácter adecuado de la protección en base al artículo 25.6 de la Directiva.

El Parlamento adoptó una resolución el 31 de marzo de 2004, en la que exponía sus reservas de carácter jurídico sobre el proyecto de Decisión de la Comisión. En particular, se estimaba que el proyecto de Decisión sobre el carácter adecuado de la protección, sobrepasaba las competencias atribuidas por el artículo 25 de la Directiva a la Comisión.

A pesar del desacuerdo con el Parlamento, la Comisión adoptó la Decisión 2004/535/CE de 14 de mayo de 2004[70], relativa al carácter adecuado de la protección de los datos personales incluidos en los registros de nombres de los pasajeros que se transfieren al Servicio de aduanas y protección de fronteras de los Estados Unidos (*Bureau of Customs and Border Protection*).

De acuerdo con el artículo 1 de la Decisión, a efectos del apartado 2 del artículo 25 de la Directiva 95/46/CE, se considera que el Servicio de Aduanas y Protección de Fronteras de los Estados Unidos ofrece un nivel adecuado de protección de los datos de PNR que se transfieren desde la Unión Europea relativos a vuelos con destino u origen en los Estados Unidos, con arreglo a los Compromisos que figuran en el anexo publicado en el mismo Diario Oficial[71].

En el anexo anteriormente mencionado, se relacionan los compromisos adquiridos por EE.UU. a través de la negociación de la Comisión con el Departamento de

[70] DOUE L 235 de 6 de julio de 2004.

[71] Compromisos del Departamento de Seguridad Interior – Servicio de Aduanas y Protección de Fronteras (CBP).

Seguridad Interior de los Estados Unidos. Por medio de esos compromisos, las autoridades norteamericanas recogerán menos datos personales del registro de nombres de los pasajeros (PNR) de las compañías aéreas, dichos datos se conservarán durante un período de tiempo más breve y se utilizarán con fines más limitados (en particular para el objetivo común de la lucha contra el terrorismo).

Frits Bolkestein, Comisario responsable de Mercado Interior, que dirigió las negociaciones en nombre de la Comisión, expresó su convicción de que se había alcanzado una solución equilibrada[72]. El acuerdo debía suponer una mejora en la situación de las compañías aéreas y de los ciudadanos de la Unión Europea. Según el Comisario, la Comisión no buscó la confrontación con el Parlamento, sino que se actuó de la forma que consideraba que mejor garantizaba los objetivos perseguidos: una mejor protección de los datos y una mayor seguridad jurídica para las compañías aéreas, a quienes la legislación norteamericana obligaba a proporcionar estos datos. "La alternativa no habría sido la obtención de mayores concesiones por parte de EE.UU., sino la inseguridad jurídica y la posible anulación de los compromisos estadounidenses de proteger los datos transferidos; en otras palabras, una situación caótica para los pasajeros y las compañías aéreas de la UE".

El 17 de mayo de 2004, el Consejo adoptó la Decisión 2004/496/CE, relativa a la celebración de un Acuerdo entre la Unión Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de los datos de los expedientes de los pasajeros por las compañías aéreas al Departamento de seguridad nacional, Oficina de aduanas y

[72] Véase comunicado de prensa, Bruselas 17 de mayo de 2004, referencia IP/04/650.

protección de fronteras, de los Estados Unidos[73]. En dicha Decisión queda aprobado, en nombre de la Unión Europea, el Acuerdo entre la UE y los Estados Unidos de América. El texto del Acuerdo se adjuntaba a la Decisión.

El Grupo de Trabajo emitió un nuevo Dictamen el 30 de septiembre de 2004. Es el Dictamen 8/2004 sobre la información a los pasajeros relativa a la transferencia de datos PNR sobre los vuelos entre la Unión Europea y los Estados Unidos de América. En este Dictamen, el Grupo de Trabajo adopta las notas informativas que figuran en dos anexos del documento. Éstas deberían servir de orientación acerca de la información que debe suministrarse a los pasajeros en vuelos transatlánticos, y tanto las compañías aéreas, como las agencias de viajes y los sistemas de reservas por ordenador que participan en el proceso de reserva deberían utilizarlas de la manera más amplia posible[74].

[73] DOUE L 183 de 20 de mayo de 2004.

[74] En el ANEXO 1 se encuentra la información sucinta sobre los viajes entre la Unión Europea y los Estados Unidos.

En el ANEXO 2 se encuentran las preguntas más frecuentes sobre la recepción por el Servicio de aduanas y protección de fronteras del registro de nombres de los pasajeros en relación con los vuelos entre la Unión Europea y los Estados Unidos:

1. ¿Por qué se transfiere el registro con mi nombre de pasajero al Servicio de aduanas y protección de fronteras de los Estados Unidos antes de viajar a este país o de salir o atravesar el mismo?
2. ¿Cuál es el marco jurídico para la transferencia de datos PNR?
3. ¿Qué tipo de información recibirá el CBP acerca de mi persona a través del PNR?
4. ¿Figura información sensible en la transferencia de datos PNR?
5. ¿Se compartirán mis datos PNR con otras autoridades?
6. ¿Durante cuánto tiempo mantendrá el CBP mis datos PNR?
7. ¿Cómo se garantizará la seguridad de mis datos PNR?
8. ¿Quién ejercerá el control del cumplimiento de los compromisos PNR?
9. ¿Puedo solicitar una copia de mis datos PNR recogidos por el CBP?
10. ¿Puedo solicitar que se corrija mi PNR?
11. ¿A quién debo contactar en los EE.UU. con respecto a este programa?
12. ¿A quién debo contactar si no se resuelve mi queja?

El Parlamento Europeo, desde el primer momento de las negociaciones de la Comisión con los Estados Unidos, había mostrado su desacuerdo con las mismas. El 27 de julio de 2004 presentó dos recursos de anulación ante el Tribunal de Justicia de la Unión Europea:

- Mediante su recurso interpuesto en el asunto C-317/04, el Parlamento Europeo solicitaba que se anulase la Decisión 2004/496/CE del Consejo, de 17 de mayo de 2004, relativa a la celebración de un Acuerdo entre la Unión Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de los datos de los expedientes de los pasajeros por las compañías aéreas al Departamento de seguridad nacional, Oficina de aduanas y protección de fronteras, de los Estados Unidos (DO L 183, p. 83, y corrección de errores en DO 2005, L 255, p. 168).
- Mediante su recurso interpuesto en el asunto C-318/04, el Parlamento solicitaba que se anulase la Decisión 2004/535/CE de la Comisión, de 14 de mayo de 2004, relativa al carácter adecuado de la protección de los datos personales incluidos en los registros de nombres de los pasajeros que se transfieren al Servicio de aduanas y protección de fronteras de los Estados Unidos (DO L 235, p. 11).

En el recurso del asunto C-318/04, el Parlamento sostiene que la Decisión de la Comisión se adoptó *ultra vires* dado que no se respetó lo dispuesto en la Directiva y que infringía en particular el artículo 3, apartado 2, primer guión[75], de ésta, según el cual

13. ¿Dónde puedo obtener más información?

[75] Tal como nos indica dicho artículo, las disposiciones de la Directiva no se aplicarán al tratamiento de datos personales efectuado en el ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario, como las previstas por las disposiciones de los títulos V y VI del Tratado de la Unión Europea y, en cualquier caso, al tratamiento de datos que tenga por objeto la seguridad pública, la

quedan excluidas las actividades no comprendidas en el ámbito de aplicación del Derecho comunitario.

Tras analizar los argumentos de las partes, el Tribunal concluye que la Decisión sobre el carácter adecuado de la protección se refiere a un tratamiento de datos personales en el sentido del artículo 3, apartado 2, primer guión, de la Directiva. Por ello, dicha Decisión no está comprendida en el ámbito de aplicación de ésta. Y por lo tanto, procede anular la Decisión sobre el carácter adecuado de la protección.

En el recurso del asunto C-317/04, el Parlamento sostiene que el artículo 95 del Tratado constitutivo de la Comunidad Europea[76] no constituye una base jurídica adecuada para la adopción de la Decisión 2004/496. Afirma que esta Decisión no tiene por objeto y contenido el establecimiento y el funcionamiento del mercado interior, contribuyendo a la eliminación de obstáculos a la libre prestación de servicios, y no contiene disposiciones que persigan la consecución de este objetivo. En efecto, su finalidad consiste en legalizar el tratamiento de datos personales impuesto por la legislación de Estados Unidos. Además, el citado artículo 95 no puede constituir la base de la competencia de la Unión Europea para celebrar el Acuerdo, dado que éste se refiere a tratamientos de datos que no están comprendidos en el ámbito de aplicación de la Directiva.

Tras analizar los argumentos de las partes, el Tribunal concluye que el Acuerdo se refiere a la misma transferencia de datos que la Decisión sobre el carácter adecuado de

---

defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando dicho tratamiento esté relacionado con la seguridad del Estado) y las actividades del Estado en materia penal.

[76] Véase la versión consolidada del Tratado Constitutivo de la Comunidad Europea en el DOCE C 325 de 24 de diciembre de 2002.

la protección y, por tanto, a tratamientos de datos que, como ya se ha expuesto anteriormente, no están comprendidos en el ámbito de aplicación de la Directiva. Por consiguiente, la Decisión 2004/496 no pudo adoptarse válidamente sobre la base del mencionado artículo 95. Por dichos motivos debe anularse la Decisión.

En consecuencia, se anulaban la Decisión 2004/496/CE del Consejo y la Decisión 2004/535/CE de la Comisión.

El Tribunal decide que continuarán vigentes los efectos de la Decisión 2004/535 hasta el 30 de septiembre de 2006, si bien no se mantendrán más allá de la fecha de extinción del citado Acuerdo.

Con motivo de la sentencia del Tribunal de Justicia de la Unión Europea, se adopta la Decisión 2006/729/PESC/JAI del Consejo de 16 de octubre de 2006, relativa a la firma, en nombre de la Unión Europea, de un Acuerdo entre la Unión Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de datos del registro de nombres de los pasajeros (PNR) por las compañías aéreas al Departamento de Seguridad del Territorio Nacional de los Estados Unidos[77]. El Acuerdo faculta al Departamento de Seguridad del Territorio Nacional de los Estados Unidos, a acceder de forma electrónica a los datos del PNR procedentes de los sistemas de reserva de las compañías aéreas situados en el territorio de los Estados miembros de la Unión Europea, hasta que se haya establecido un sistema satisfactorio para la transmisión de esos datos por las compañías aéreas. A efectos de la aplicación del Acuerdo, se considera que el Departamento de Seguridad del Territorio Nacional ofrece un nivel adecuado de protección de los datos de PNR que se transfieren desde la Unión Europea

[77] DOUE L 298 de 27 de octubre de 2006.

en relación con vuelos internacionales de transporte de pasajeros con origen o destino en los Estados Unidos.

Dado que el anterior Acuerdo entre la Unión Europea y los Estados Unidos de América expiraba, a más tardar el 31 de julio de 2007 (salvo que se prorrogase mediante consentimiento recíproco por escrito), el 22 de febrero de 2007, el Consejo decidió autorizar a la Presidencia, asistida por la Comisión, a entablar negociaciones para un acuerdo a largo plazo sobre el mismo asunto. Dichas negociaciones culminaron satisfactoriamente con la redacción de un nuevo Acuerdo.

Como fruto del mismo, se adopta la Decisión 2007/551/PESC/JAI del Consejo de 23 de julio de 2007[78], relativa a la firma, en nombre de la Unión Europea, de un Acuerdo entre la Unión Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de datos del registro de nombres de los pasajeros (PNR) por las compañías aéreas al Departamento de Seguridad del Territorio Nacional de los Estados Unidos (Acuerdo PNR 2007)[79]. En base a este nuevo Acuerdo, el Departamento de Seguridad del Territorio Nacional efectuará de inmediato, y a más tardar el 1 de enero de 2008, la transición a un sistema de transmisión (*push system*) para la transmisión de datos por las mencionadas compañías aéreas, siempre que estas hayan implantado un

[78] DOUE L 204 de 4 de agosto de 2007.

[79] Véase al respecto la Referencia del Consejo de Ministros del Gobierno de España, de 20 de julio de 2007: **http://www.lamoncloa.gob.es/consejodeministros/referencias/_2007/refc20070720.htm**. En dicho Consejo de Ministros se aprueba "*el Acuerdo por el que se toma conocimiento del acuerdo entre la Unión Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de datos del registro de nombres de los pasajeros (PNR) por las compañías aéreas al departamento de seguridad del territorio nacional de los Estados Unidos y de su aplicación provisional, y se autoriza la formulación por España de una declaración, de acuerdo con lo previsto en el artículo 24.5 del tratado de la Unión Europea".*

sistema de este tipo que cumpla las prescripciones técnicas del Departamento de Seguridad del Territorio Nacional. Para las compañías aéreas que no hayan implantado dicho sistema, seguirán vigentes los sistemas actuales hasta que establezcan un sistema que cumpla las prescripciones técnicas del Departamento de Seguridad del Territorio Nacional. Por consiguiente, el Departamento de Seguridad del Territorio Nacional accederá de forma electrónica al PNR de los sistemas de reserva de las compañías aéreas situados en el territorio de los Estados miembros de la Unión Europea hasta que se haya establecido un sistema satisfactorio que permita a las compañías aéreas transmitir esos datos.

A efectos de la aplicación del Acuerdo PNR 2007, se considera que el Departamento de Seguridad del Territorio Nacional ofrece un nivel adecuado de protección de los datos de PNR transferidos desde la Unión Europea. En consecuencia, la UE no interferirá por motivos de protección de datos en las relaciones entre los Estados Unidos y terceros países en lo que respecta al intercambio de datos sobre pasajeros.

Deberíamos analizar ahora el Dictamen 5/2007 del Grupo de Trabajo (WP 138), adoptado el 17 de agosto de 2007, relativo al nuevo Acuerdo entre la Unión Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de datos del registro de nombres de los pasajeros (PNR) por parte de las compañías aéreas al Departamento de Seguridad del Territorio Nacional de los Estados Unidos, celebrado en julio de 2007. En este Dictamen, el Grupo de Trabajo se muestra muy crítico con el Acuerdo alcanzado por ambas partes. Considera que las garantías en materia de protección de datos se han reajustado a la baja. El Grupo deplora igualmente que la

Unión Europea haya considerado adecuado el Acuerdo en cuanto a las garantías relativas a la protección de los datos sin solicitar el dictamen de un organismo reconocido de protección de datos, y ello a pesar de que el Acuerdo deberá ser aplicado por los Estados miembros en estrecha colaboración con las autoridades de control nacionales.

El Grupo de Trabajo considera que los fines que justifican la transferencia de los datos PNR son demasiado extensos y lamenta que sobrepasen los reconocidos por la normativa de protección de datos. Las importantes excepciones a estos fines no están lo suficientemente detalladas.

El plazo de conservación se ha ampliado considerablemente, y también la lista de los elementos de información ha sido ampliada, al tiempo que las garantías otorgadas en el marco de los compromisos previos se han reajustado claramente a la baja. El hecho de que el filtrado de los datos sensibles siga siendo competencia del Departamento de Seguridad del Territorio Nacional y que este último pueda utilizarlos en casos excepcionales es contrario a las normas de protección de datos comúnmente admitidas (tal y como se recoge en el Convenio 108 y en la Directiva).

El Grupo de Trabajo se siente *extremadamente decepcionado* por el inadecuado nivel de protección de los datos. El nuevo Acuerdo ni siquiera mantiene el nivel de protección de la privacidad presente en el anterior Acuerdo, que el Grupo de trabajo ya había calificado de insuficiente en sus dictámenes previos. El balance sobre el nuevo Acuerdo PNR no es positivo al considerar que éste no se atiene a las normas de protección de datos comúnmente aceptadas.

A nivel nacional, la Agencia Española de Protección de Datos emitió una Nota Informativa el uno de agosto de 2007[80] en la que cuestionaba *el nivel de garantías del Acuerdo sobre la transmisión de datos, PNR*. Para la AEPD el nuevo Acuerdo contempla una serie de medidas que pueden suponer una disminución de las garantías del derecho fundamental a la protección de datos de los ciudadanos[81]. En su opinión, es necesario garantizar el derecho fundamental a la protección de datos buscando un equilibrio entre éste y las exigencias de seguridad frente al terrorismo, y por ello, cuestiona el nivel de garantías del Acuerdo. Además, la AEPD lamenta el hecho de que no se haya tenido en cuenta a las autoridades de protección de datos en las negociaciones.

Es conveniente hacer un breve análisis del Dictamen 2/2007 del Grupo de Trabajo (WP 132 y WP 151), emitido el 15 de febrero de 2007 y revisado y actualizado el 24 de junio de 2008, relativo a la información de los pasajeros en relación con la transferencia de datos PNR a las autoridades de los Estados Unidos. Este Dictamen y sus anexos

[80] El día uno de agosto de 2007 era la fecha de entrada en vigor del nuevo Acuerdo entre la UE y los Estados Unidos para la transferencia de datos PNR.

[81] Se destacan en la Nota Informativa las siguientes disminuciones de garantías: la ampliación del periodo de retención de los datos de tres años y medio a hasta 15 años; la posibilidad de que las autoridades americanas puedan hacer uso de datos sensibles que se puedan derivar de los datos de la reserva, como los referidos a salud u origen racial, en determinadas circunstancias, algo que no se preveía en acuerdos anteriores; la ampliación de las finalidades para las que puedan utilizarse estos datos, puesto que ahora los datos PNR pueden ser utilizados no sólo para casos en que sean necesarios para proteger intereses vitales del titular o de otras personas sino también en procedimientos judiciales; y el aumento de los potenciales receptores de los datos transferidos, puesto que en el acuerdo se recoge la posibilidad de acceso por parte de cualquier departamento de la Administración Americana competente para la lucha contra el terrorismo, y contempla además la posibilidad de que la información sea transmitida a terceros países, sin recogerse en el Acuerdo las garantías acerca del uso de los datos una vez que estén en posesión de estos terceros países.

(modelo de nota informativa y preguntas más frecuentes) están dirigidos a agencias de viajes, compañías aéreas y otras organizaciones que prestan servicios de transporte aéreo a pasajeros hacia o desde los Estados Unidos de América (EE.UU.). Este Dictamen y los anexos actualizan y reemplazan el anterior de 30 de septiembre de 2004 (WP97).

Las agencias de viajes, compañías aéreas y otras organizaciones siguen estando obligadas a proporcionar información a los pasajeros sobre el tratamiento de sus datos personales, y el presente Dictamen incluye orientaciones sobre qué información hay que dar, quién debe darla, cómo y cuándo.

En cuanto a los pasajeros, se ofrecen distintas notas informativas sobre la transferencia de sus datos a las autoridades de los Estados Unidos. La nota informativa extensa se ha elaborado en forma de preguntas más frecuentes y ofrece más detalles sobre el tratamiento[82]. En ella se da una información más general sobre los datos de los pasajeros y luego se abordan los datos PNR en concreto. Incluye enlaces al acuerdo en vigor y otros documentos pertinentes.

El 6 de noviembre de 2007, la Comisión presentó su propuesta de Decisión Marco del Consejo sobre utilización de datos del registro de nombres de los pasajeros

[82] Preguntas más frecuentes sobre la transferencia de información de los pasajeros a las autoridades de los EE.UU. en relación con los vuelos entre la Unión Europea y los EE.UU.:

1. ¿Qué tipo de información del pasajero se transmitirá a las autoridades de los EE.UU.?
2. ¿Por qué se transfieren mis datos PNR al DHS antes de viajar desde, hacia o vía los EE.UU.?
3. ¿Cuál es el marco jurídico para la transferencia de datos del PNR?
4. ¿La transferencia de datos del PNR incluye información sensible?
5. ¿Se permitirá el acceso de otras autoridades a mis datos PNR?
6. ¿Durante cuánto tiempo conservará mis datos PNR el DHS?
7. ¿Puedo solicitar una copia de mis datos PNR recogidos por el DHS y pedir su corrección?
8. ¿Cómo puedo obtener más información?

(Passenger Name Record - PNR) con fines represivos[83]. El Grupo de Trabajo sobre Protección de Datos previsto en el artículo 29 de la Directiva y el Grupo de Trabajo sobre Policía y Justicia adoptaron un Dictamen conjunto sobre la propuesta de Decisión marco del Consejo relativa al uso del registro de nombres de los pasajeros («*Passenger Name Record*» - PNR) a efectos de la aplicación de la ley, presentado por la Comisión el 6 de noviembre de 2007[84]. Este Dictamen se propone analizar el impacto en los derechos fundamentales y las libertades, en especial los derechos de los pasajeros a la intimidad, de la propuesta de Decisión Marco del Consejo. De acuerdo al Dictamen, la propuesta sigue fielmente el modelo del Acuerdo en materia de PNR entre la UE y los Estados Unidos, firmado en julio de 2007 y el proyecto se asemeja a él en muchas de sus características. La preocupación en cuanto a la protección de la intimidad manifestada por el Grupo de trabajo previsto en el artículo 29 en relación con dicho acuerdo del PNR sigue siendo, por lo tanto, válida por lo que respecta a varios puntos expresados en el Dictamen.

Las autoridades comunitarias responsables de la protección de datos consideran que la forma en que la propuesta está redactada no sólo es desproporcionada sino que también puede violar principios fundamentales de normas reconocidas en materia de protección de datos recogidas en el artículo 8 del Convenio Europeo sobre Derechos Humanos y del Convenio 108 del Consejo de Europa[85]. Por otra parte, consideran que

[83] COM (2007) 654 final. 2007/0237 (CNS).

[84] Adoptado el 5 de diciembre de 2007 por el Grupo de Trabajo previsto en el artículo 29 (WP 145) y el 18 de diciembre de 2007 por el Grupo de Trabajo sobre Policía y Justicia (Ref: 01/07).

[85] Las cuestiones relacionadas con la protección de datos de la propuesta tienen las siguientes características:

1 La propuesta no justifica una necesidad apremiante de recogida de datos, con excepción de los datos API de información previa sobre pasajeros (*Advanced Passenger Information*, API).

hay que poner en cuestión la aplicabilidad de la «Decisión marco sobre la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal» en lo relativo a los derechos de la persona a la que se refieren los datos que menciona la propuesta, ya que esa Decisión marco rige solamente la transferencia de datos personales entre los organismos de los Estados miembros de la UE encargados de la aplicación de la ley y no la transferencia de datos realizada por las compañías aéreas a las Unidades de Información sobre Pasajeros en la UE.

El 21 de septiembre de 2010, la Comisión Europea presentó su Comunicación sobre el enfoque global de las transferencias de datos de los registros de nombres de los pasajeros (PNR) a los terceros países[86]. Para analizarla, el Grupo de Trabajo emitió un nuevo Dictamen el 12 de noviembre de 2010. Es el Dictamen 7/2010 relativo a la Comunicación de la Comisión Europea sobre el enfoque global de las transferencias de datos de los registros de nombres de los pasajeros (PNR) a terceros países. En el Dictamen el Grupo de Trabajo entiende que, en conjunto, se puede estar satisfecho por el hecho de que la Comisión Europea demuestre entender claramente la necesidad de prestar más atención a la protección de datos en los futuros acuerdos PNR y esté

2 Es excesiva la cantidad de datos personales que deben transferir las compañías aéreas.

3 La filtración de datos sensibles debería ser hecha por la persona responsable del tratamiento de los datos.

4 El método de «*push*» debe aplicarse a todas las compañías aéreas.

5 El período de conservación de los datos es desproporcionado.

6 El régimen de protección de los datos es totalmente insatisfactorio: en ninguna parte se especifican los derechos de los interesados ni las obligaciones de los responsables del tratamiento de los datos.

7 El gran margen de discreción concedido a los Estados miembros podría dar lugar a interpretaciones diversas de la Decisión marco.

8 El régimen de protección de datos de las transferencias que se realizarán a terceros países es poco claro.

[86] Bruselas, 21.09.2010, COM(2010) 492 final.

dispuesta a celebrar acuerdos vinculantes para garantizar la seguridad jurídica y la igualdad de trato. La Comunicación presentada el 21 de septiembre de 2010 es un paso en la dirección correcta, aunque la utilidad del análisis a gran escala de los datos de los pasajeros debe cuestionarse a fondo, sobre la base de elementos científicos y de estudios recientes. El Grupo de Trabajo recalca que las normas y criterios generales incluidos en la Comunicación deben considerarse como el nivel mínimo de protección de datos que debe alcanzarse en los futuros acuerdos PNR. Sin embargo, en varios puntos las normas podrían y deberían desarrollarse más.

El 2 de febrero de 2011, la Comisión Europea publicó su propuesta de Directiva relativa a la utilización de datos del registro de nombres de los pasajeros para prevención, detección, investigación y enjuiciamiento de los delitos terroristas y delitos graves. Para analizar esta propuesta, el Grupo de Trabajo emitió un nuevo Dictamen el 5 de abril de 2011. Es el Dictamen 10/2011 relativo a la propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la utilización de datos del registro de nombres de los pasajeros para prevención, detección, investigación y enjuiciamiento de los delitos terroristas y delitos graves. El Grupo de Trabajo históricamente ha puesto en duda la necesidad y proporcionalidad de los sistemas de PNR y continúa haciéndolo en relación con la propuesta de 2011. Sigue criticando la vaguedad de los fines, muestra sus dudas sobre el ámbito potencialmente amplio de la definición de delito grave, dudas que se aplican también a las disposiciones que se proponen en la Directiva para compartir datos con otras autoridades de dentro y fuera de la UE y continúa considerando desproporcionada la propuesta de retener datos durante cinco años. El Grupo de Trabajo tiene también serias dudas sobre la proporcionalidad de que los datos de todos los pasajeros se analicen sistemáticamente según criterios predeterminados.

El 13 de diciembre de 2011, el Consejo adoptó un nuevo Acuerdo[87] sobre la transmisión de los registros de nombres de los pasajeros (PNR) y el 14 de diciembre de 2011, la UE y los EE.UU. firmaron dicho Acuerdo[88]. El Parlamento Europeo ha dado su aprobación al mismo[89] el 19 de abril de 2012. Los ministros de Justicia e Interior han dado su visto bueno al texto en el Consejo de Asuntos de Justicia e Interior (JAI) celebrado en Luxemburgo el 26 y 27 de abril de 2012[90].

El nuevo Acuerdo, ha entrado en vigor el uno de julio de 2012[91], sustituyendo al anterior que se aplicaba desde 2007. A partir de ahora, los datos PNR podrán conservarse durante un período de diez años en lo que se refiere a la delincuencia transfronteriza, y de quince años en lo que se refiere al terrorismo. Después de seis meses, debe enmascararse la información personal identificable incluida en los datos PNR y, después de cinco años, la información se trasladará a una base de datos inactiva,

---

[87] El contenido íntegro del *Acuerdo entre los Estados Unidos de América y la Unión Europea sobre la utilización y la transferencia de los registros de nombres de los pasajeros al Departamento de Seguridad del Territorio Nacional de los Estados Unidos* puede encontrarse en el DOUE L 215 de 11 de agosto de 2012.

[88] Véase comunicado de prensa, Bruselas 17 de noviembre de 2011, referencia IP/11/1368.

[89] Como se hace constar en la Resolución del Parlamento Europeo, de 11 de noviembre de 2010, sobre el enfoque global de las transferencias de datos de los registros de nombres de los pasajeros (PNR) a los terceros países y las Recomendaciones de la Comisión al Consejo para autorizar la apertura de negociaciones para un Acuerdo entre la Unión Europea y Australia, Canadá y los Estados Unidos, con la entrada en vigor del Tratado de Lisboa, el Parlamento ha de dar su aprobación a los Acuerdos de la UE con los Estados Unidos (u otro país) sobre la transferencia de datos del registro de nombres de los pasajeros (PNR) con vistas a la celebración de dichos Acuerdos.

[90] La Decisión del Consejo de 26 de abril de 2012 *relativa a la celebración del Acuerdo entre los Estados Unidos de América y la Unión Europea sobre la utilización y la transferencia de los registros de nombres de los pasajeros al Departamento de Seguridad del Territorio Nacional de los Estados Unidos* se ha publicado en el DOUE L 215 de 11 de agosto de 2012.

[91] DOUE L 174 de 4 de julio de 2012.

dotada de controles adicionales. Los pasajeros tendrán derecho a acceder a los datos que se refieran a ellos y podrán solicitar su rectificación y su supresión. Asimismo podrán solicitar reparación por vía administrativa y judicial.

Como señala el Supervisor Europeo de Protección de Datos en su Dictamen de nueve de diciembre de 2011[92], "siguen sin resolverse muchas preocupaciones, en especial respecto de la coherencia del enfoque global del PNR, la limitación a una finalidad específica, las categorías de datos que deben ser transferidas al DHS, el tratamiento de datos sensibles, el período de conservación, las excepciones al método push, los derechos de los interesados y las transferencias ulteriores".

Por todo lo señalado, este proceso tan largo y complejo ha llevado a duros enfrentamientos entre las autoridades europeas y las norteamericanas, pero también entre las propias autoridades de la Unión Europea. Cuando en 2001 el Gobierno de los Estados Unidos decide unilateralmente que las compañías aéreas que volaran sobre territorio americano deberían suministrar a la administración americana los datos personales relativos a los pasajeros y miembros de la tripulación, se inicia un serio conflicto con la Unión Europea ya que se vulneran los principios más elementales en materia de protección de datos.

Es cierto que la sociedad occidental necesita de seguridad, pero no a cualquier precio. Hay que buscar un punto intermedio que permita la lucha antiterrorista de forma eficaz, pero que no vulnere tan intensamente la legislación europea en el campo de la protección de datos.

[92] DOUE C 35 de 9 de febrero de 2012.

Un conflicto como éste no hubiera podido existir si la otra parte no fuera la superpotencia americana. Aparentemente lo único que ha conseguido la UE es dulcificar mínimamente las exigencias de la administración de los Estados Unidos.

Pese al nuevo Acuerdo que ha entrado en vigor en julio de 2012, las transferencias de PNR a Estados Unidos continúan siendo un problema mal resuelto y del que se desconoce el final.

4.2. TRANSMISIÓN DE DATOS DE LOS PASAJEROS A CANADÁ

El 11 de febrero de 2004, el Grupo de Trabajo del artículo 29 adoptó un Dictamen sobre el nivel de protección garantizado por Canadá para la transmisión de expedientes de viajeros (PNR) y de información anticipada sobre viajeros (API) por parte de las compañías aéreas[93]. En dicho Dictamen, el Grupo de Trabajo llegó a la conclusión de que el cumplimiento de los requisitos canadienses por parte de las líneas aéreas suscitaba inquietudes por lo que respecta a la Directiva 95/46/CE sobre protección de datos.

El Grupo invitó a la Comisión a que continuase las negociaciones con Canadá para abordar los problemas detectados por el Grupo, con el objetivo de encontrar las mejores soluciones posibles.

A partir de ese momento, la Comisión puso al día regularmente al Grupo de Trabajo sobre estas negociaciones realizadas con el fin de establecer las condiciones que le permitieran adoptar una Decisión que reconociera la adecuada protección garantizada por Canadá para la transferencia de datos de pasajeros en virtud del apartado 6 del artículo 25 de la Directiva 95/46/CE.

[93] Dictamen 3/2004, adoptado el 11 de febrero de 2004 por el Grupo de Trabajo previsto en el artículo 29 (WP 88).

En particular, el Grupo recibió de la Comisión un documento con fecha de 18 de enero de 2005 que contenía los *Compromisos* de la Agencia de servicios fronterizos de Canadá en relación a la aplicación de su programa PNR.

A la luz de los *Compromisos*, el Grupo de Trabajo adoptó un nuevo Dictamen[94]. En éste se resaltan los cambios sustanciales que se han obtenido en el programa PNR canadiense[95].

Sobre la base de las adaptaciones efectuadas, el Grupo admite que Canadá garantiza un nivel adecuado de protección en el sentido del apartado 6 del artículo 25 de 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 información anticipada sobre viajeros (API) y de expedientes de viajeros (PNR) transferida por las compañías aéreas a la Agencia de servicios fronterizos de Canadá en relación con los vuelos definidos en la sección 107.1 de la Ley de aduanas, por lo que respecta a cualquier persona a bordo de un medio de transporte que llegue a Canadá.

El 18 de julio de 2005 se adoptó la Decisión del Consejo (2006/230/CE) relativa a la celebración de un Acuerdo entre la Unión Europea y el Gobierno de Canadá sobre el tratamiento de datos API/PNR[96]. El 7 de marzo de 2005, el Consejo había autorizado a la Comisión a negociar con Canadá, en nombre de la Unión, un acuerdo sobre el tratamiento y la transferencia de datos procedentes del sistema de información

[94] Dictamen 1/2005, adoptado el 19 de enero de 2005 por el Grupo de Trabajo (WP 103).

[95] Se han producido mejoras importantes en el tratamiento de los datos API/PNR, en la finalidad del tratamiento de esos datos, en los datos personales transferibles, en el periodo de conservación de los datos, en la revelación de datos/transferencias posteriores y en los derechos de los interesados y cumplimiento.

[96] DOUE L 82 de 21 de marzo de 2006.

anticipada sobre pasajeros (*Advance Passenger Information*, API) y de los expedientes de los pasajeros (*Passenger Name Record*, PNR), por parte de las compañías aéreas, a la *Canada Border Services Agency* (CBSA: organismo de servicios fronterizos de Canadá). En la Decisión del Consejo se aprueba, en nombre de la Unión, el Acuerdo entre la UE y el Gobierno de Canadá sobre el tratamiento de datos API/PNR.

El 6 de septiembre de 2005 se adopta la Decisión de Comisión (2006/253/CE) relativa al carácter adecuado de la protección de los datos personales incluidos en los registros de nombres de los pasajeros (Passenger Name Records, PNR) que se transfieren a la Canada Border Services Agency (Agencia de Servicios de Fronteras de Canadá)[97]. De acuerdo a la Decisión, a efectos del artículo 25, apartado 2, de la Directiva 95/46/CE, se considera que la Canadian Customs Border Services Agency (Agencia de Servicios de Fronteras de Canadá) ofrece un nivel adecuado de protección de los datos del PNR que se transfieren desde la Unión Europea relativos a vuelos con destino a Canadá, con arreglo a los Compromisos[98] que figuran en el anexo de la Decisión. La Decisión expirará tres años y seis meses después de la fecha de su notificación, salvo que sea prorrogada con arreglo al procedimiento expuesto en el artículo 31, apartado 2, de la Directiva 95/46/CE.

El Acuerdo UE-Canadá sobre la transferencia de datos de los registros de nombres de los pasajeros (PNR) dejó de ser válido, debido a la expiración de la Decisión sobre el carácter adecuado de la protección en septiembre de 2009. A la espera de la firma de un

[97] DOUE L 91 de 29 de marzo de 2006.

[98] Compromisos de la Agencia de Servicios de Fronteras de Canadá en relación con la aplicación de su programa sobre el PNR.

nuevo Acuerdo, la transferencia de datos PNR tiene lugar desde esa fecha sobre la base de compromisos unilaterales por parte de Canadá ante los Estados miembros.

4.3. TRANSMISIÓN DE DATOS DE LOS PASAJEROS A AUSTRALIA

La legislación australiana sobre protección de fronteras autoriza al servicio de aduanas del país a evaluar los riesgos que presentan los datos del PNR de las compañías aéreas internacionales antes de la llegada de los pasajeros a Australia.

Las compañías aéreas tienen la obligación de facilitar al servicio de aduanas el acceso a determinados datos del PNR. El cumplimiento de los requisitos australianos por parte de las compañías aéreas puede plantear problemas en relación con la Directiva 95/46/CE sobre protección de datos. Por ello, la Comisión entabló negociaciones en 2003 con Australia para establecer las condiciones que permitieran adoptar una decisión en la que se reconociera que se garantiza una protección adecuada con arreglo al apartado 6 del artículo 25 de la Directiva 95/46/CE.

La Comisión puso al día al Grupo de Trabajo acerca de dichas negociaciones; en particular, el Grupo de Trabajo recibió de la Comisión un documento que contenía el *compromiso* adquirido por el servicio de aduanas australiano ante el Parlamento (federal) australiano en relación con el acceso a la información sobre los pasajeros y la no retención de dicha información, así como las averiguaciones del Senado en relación con este asunto.

Con la información aportada por la Comisión, el Grupo de Trabajo adoptó el Dictamen[99] sobre el nivel de protección garantizado por Australia en la transmisión de datos del registro de nombres de pasajeros de las compañías aéreas[100].

[99] Dictamen 1/2004, adoptado el 16 de enero de 2004 por el Grupo de Trabajo (WP 85).

El Dictamen 1/2004 concluye que, a condición de que se tengan en cuenta las cuestiones mencionadas en el propio Dictamen (apartados 3, 4 y 5), el Grupo de Trabajo considera que Australia garantiza un nivel adecuado de protección en el sentido contemplado en el apartado 6 del artículo 25 de 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, en cuanto al tratamiento de los datos del PNR de las compañías aéreas en su transmisión a las autoridades australianas en relación con los vuelos con destino a Australia, procedentes de ese país o con escala en él.

El 30 de junio de 2008, en aplicación del Título V del Tratado de la UE, se adoptó la Decisión 2008/651/PESC/JAI del Consejo[101], relativa a la firma, en nombre de la Unión Europea, de un Acuerdo entre la Unión Europea y Australia sobre el tratamiento y la transferencia de datos, generados en la Unión Europea, del registro de nombres de los pasajeros (PNR) por las compañías aéreas a los Servicios de Aduanas de Australia. Tal como se indica en el artículo 3 del Acuerdo (texto que se adjuntaba a la Decisión), sobre *adecuación*, el hecho de que los Servicios de Aduanas cumplan lo dispuesto en el Acuerdo constituirá, en el sentido de la normativa pertinente de la UE sobre protección de datos, un nivel adecuado de protección de los datos del PNR generados en la Unión Europea y transferidos a las Aduanas a los efectos del Acuerdo.

[100] En el Dictamen se analiza la legislación australiana sobre datos del PNR, así como el funcionamiento y características de los acuerdos de acceso al PNR del Servicio de Aduanas (tratamiento y retención de los datos del PNR, finalidad del Servicio de Aduanas al acceder a los datos del PNR, elementos de los datos del PNR a los que se tiene acceso, manera y forma de acceder a los datos del PNR, destinatario inicial de los datos del PNR, transmisiones posteriores, seguridad, datos sensibles, información, derecho de acceso y rectificación, mecanismos de cumplimiento).

[101] DOUE L 213 de 8 de agosto de 2008.

El Acuerdo firmado en 2008 entre la Unión Europea y Australia se aplicó provisionalmente desde su firma, pero no ha entrado en vigor. El Parlamento Europeo decidió, el 5 de mayo de 2010[102], posponer el voto sobre la solicitud de aprobación de dicho Acuerdo y, mediante su Resolución de 11 de noviembre de 2010[103], aceptó la recomendación de la Comisión Europea al Consejo de la Unión Europea de negociación de un nuevo Acuerdo.

El 19 de mayo de 2011 la Comisión adoptó una propuesta de Decisión del Consejo relativa a la celebración del Acuerdo entre la Unión Europea y Australia sobre el tratamiento y transferencia de datos de registros de nombres de pasajeros (PNR), por parte de los transportistas aéreos, al Servicio de Aduanas y de Protección de las Fronteras de Australia[104]. Esta propuesta es fruto de la Decisión del Consejo de 2 de diciembre de 2010, por la que, junto con las directrices de negociación, se autorizaba a la Comisión a entablar negociaciones en nombre de la Unión Europea entre la Unión Europea y Australia para la transferencia y utilización de datos del registro de nombres de los pasajeros (PNR) con objeto de prevenir y combatir el terrorismo y otros delitos graves de carácter transnacional.

La propuesta de Decisión del Consejo de 19 de mayo de 2011 contiene un anexo con el Acuerdo entre la Unión Europea y Australia sobre el tratamiento y la

[102] DOUE C 81 E de 15 de marzo de 2011.

[103] En la Resolución de 11 de noviembre de 2010, el Parlamento "acoge con satisfacción la Recomendación de la Comisión al Consejo para autorizar la apertura de negociaciones para un Acuerdo entre la Unión Europea y Australia, Canadá y los Estados Unidos para la transferencia y utilización de datos PNR con objeto de prevenir y combatir el terrorismo y otras formas graves de delincuencia transnacional; acoge con satisfacción la decisión del Consejo de iniciar todas las negociaciones al mismo tiempo, si bien reconoce que la duración de las negociaciones puede variar".

[104] Bruselas, 19.05.2011, COM (2011) 281 final.

transferencia de datos del registro de nombres de los pasajeros (PNR) por los transportistas aéreos al Servicio de Aduanas y de Protección de Fronteras de Australia.

El Supervisor Europeo de Protección de Datos fue consultado de manera informal durante el mes de mayo de 2011, en el contexto de un procedimiento de vía rápida, sobre la propuesta relativa al acuerdo entre la Unión Europea y Australia sobre el tratamiento y la transferencia de datos PNR. Consecuencia de esta consulta se formula un Dictamen del Supervisor Europeo, que es publicado en el Diario Oficial de la UE[105].

En el Dictamen del Supervisor Europeo se manifiesta su satisfacción por las garantías previstas en las propuestas, en especial respecto de la ejecución concreta del acuerdo. En particular, los aspectos de seguridad, las medidas de supervisión y de ejecución se han desarrollado de un modo satisfactorio. Sin embargo, el Supervisor Europeo también ha identificado un importante margen de mejora, en especial en cuanto al ámbito de aplicación del acuerdo, la definición de terrorismo y la inclusión de algunas finalidades excepcionales, así como el período de conservación de los datos del PNR. En comparación con el anterior sistema PNR de Australia, y también con la propuesta de un sistema PNR para la Unión Europea, este período de conservación resulta desproporcionado. Por otra parte, opina que debería reconsiderarse la base jurídica del acuerdo. Teniendo en cuenta lo establecido en la jurisprudencia reiterada, y aparte de lo dispuesto en el artículo 218, apartado 6, letra a) del Tratado de Funcionamiento de la UE, el Supervisor Europeo considera que en cualquier caso el acuerdo debería estar basado principalmente en el artículo 16 del TFUE y no en el artículo 82, apartado 1, letra d) y el artículo 87, apartado 2, letra a).

[105] DOUE C 322 de 5 de noviembre de 2011.

Según el artículo 82, “el Parlamento Europeo y el Consejo adoptarán, con arreglo al procedimiento legislativo ordinario, medidas tendentes a …. facilitar la cooperación entre las autoridades judiciales o equivalentes de los Estados miembros en el marco del procedimiento penal y de la ejecución de resoluciones”. En el artículo 87 se regula que para el desarrollo de la cooperación policial, “el Parlamento Europeo y el Consejo podrán adoptar, con arreglo al procedimiento legislativo ordinario, medidas relativas a … la recogida, almacenamiento, tratamiento, análisis e intercambio de información pertinente”.

Mientras que, de acuerdo al artículo 16 del TFUE:

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

b) El Parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos”.

Esta postura del Supervisor Europeo es totalmente conforme con lo dispuesto en la Declaración 21 (Declaración relativa a la protección de datos de carácter personal en el ámbito de la cooperación judicial en materia penal y de la cooperación policial) del Tratado de Lisboa.

El nuevo Acuerdo entre la Unión Europea y Australia sobre el tratamiento y la transferencia de datos del registro de nombres de los pasajeros (PNR) por los

transportistas aéreos al Servicio de Aduanas y de Protección de las Fronteras de Australia fue firmado el 29 de septiembre de 2011, y ha entrado en vigor el día uno de junio de 2012[106].

5. ESTADOS QUE PROPORCIONAN UN NIVEL ADECUADO DE PROTECCIÓN SEGÚN LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Hemos analizado las facultades de la Comisión Europea a la hora de considerar que un país garantiza un nivel adecuado de protección de los datos personales transferidos desde la Unión Europea. Ahora vamos a explorar una segunda vía: la AEPD también es competente para declarar la existencia de un nivel de protección adecuado respecto a un país de destino de los datos personales.

De acuerdo al artículo 25.2 de la Directiva 95/46/CE, "el carácter adecuado del nivel de protección que ofrece un país tercero se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos; en particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, así como las normas profesionales y las medidas de seguridad en vigor en dichos países".

En la normativa interna, encontramos que la LOPD, en su artículo 33.2 efectúa una regulación parecida, pero no idéntica: El carácter adecuado del nivel de protección que

[106] En el DOUE L 186 de 14 de julio de 2012 encontramos las Decisiones del Consejo y el texto del Acuerdo entre la UE y Australia.

ofrece el país de destino se evaluará por la Agencia Española de Protección de Datos atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos. En particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de derecho, generales o sectoriales, vigentes en el país tercero de que se trate, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.

En el Reglamento de desarrollo de la LOPD encontramos una regulación todavía más detallada que en la Ley. En su artículo 67, sobre el nivel adecuado de protección acordado por la Agencia Española de Protección de Datos, se regula que no será precisa autorización del Director de la Agencia Española de Protección de Datos a una transferencia internacional de datos cuando las normas aplicables al Estado en que se encontrase el importador ofrezcan dicho nivel adecuado de protección a juicio del Director de la Agencia Española de Protección de Datos. "El carácter adecuado del nivel de protección que ofrece el país de destino se evaluará atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos. En particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países".

A efecto de que sean de público conocimiento, las resoluciones del Director de la Agencia Española de Protección de Datos por las que se acordase que un determinado

país proporciona un nivel adecuado de protección de datos serán publicadas en el Boletín Oficial del Estado. El Director de la Agencia Española de Protección de Datos acordará la publicación de la relación de países cuyo nivel de protección haya sido considerado equiparable conforme a lo dispuesto en el apartado anterior. Esta lista se publicará y mantendrá actualizada asimismo a través de medios informáticos o telemáticos.

Desde la entrada en vigor de la LOPD no se ha producido ninguna resolución del Director de la AEPD en las que se acuerde que un país proporciona un nivel adecuado de protección. Distinto fue en la época que tuvo vigencia la anterior norma (la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, LORTAD). En la Disposición Final Primera del Reglamento de desarrollo de la LORTAD[107] se facultaba al Ministro de Justicia e Interior para que, previo informe del Director de la Agencia Española de Protección de Datos, aprobase la relación de países que, a efectos de lo dispuesto en el artículo 32[108] de la Ley Orgánica 5/1992, se entendiese que proporcionaban un nivel de protección equiparable al de dicha Ley.

En base a la habilitación otorgada, se aprobaron dos Órdenes Ministeriales. La inicial es la Orden de 2 de febrero de 1995[109], por la que se aprueba la primera relación de países con protección de datos de carácter personal equiparable a la española, a

[107] Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los datos de carácter personal. (Vigente hasta el 19 de abril de 2008).

[108] El contenido del artículo 32 de la LORTAD lo encontramos hoy con pocos cambios en el artículo 33.1 de la LOPD y en el artículo 67.1 del RLOPD.

[109] BOE del 10 de febrero de 1995.

efectos de transferencia internacional de datos. Se especifican de forma separada los países que proporcionan un nivel de protección equiparable al español, según se trate de ficheros de titularidad pública o de ficheros de titularidad privada.

Los países cuyo régimen legal de protección de datos de carácter personal se considera equiparable, tanto respecto a ficheros de titularidad pública como a los de titularidad privada, son los estados parte del Convenio para la Protección de las Personas con relación al Tratamiento Automatizado de los Datos de Carácter Personal, abierto a la firma en Estrasburgo el 28 de enero de 1981. En concreto son los siguientes: Alemania, Austria, Bélgica, Dinamarca -con la excepción del territorio de las Islas Feroe y de Groenlandia-, Eslovenia, Finlandia, Francia, Grecia, Irlanda, Islandia, Italia, Luxemburgo, Noruega -con la excepción del territorio de Svalbard-, Países Bajos, Portugal, Reino Unido -inclusive el territorio de las Islas de Man y Jersey- y Suecia.

Asimismo se considera que proporcionan un nivel de protección equiparable respecto a ficheros de titularidad pública y de titularidad privada, Australia, Israel, Hungría, Nueva Zelanda, República Checa, República de Slovakia, San Marino y Suiza.

Se entiende que tienen un nivel de protección equiparable respecto de los datos registrados en ficheros de titularidad pública, la República de Andorra y Japón.

También proporciona un nivel de protección equiparable la legislación de Canadá respecto de los ficheros de titularidad pública. Y respecto de los ficheros de titularidad privada, las provincias canadienses de Quebec, Ontario, Saskatchewan y Columbia Británica.

En la Orden se hace constar que lo que se aprueba es una primera relación de países, es decir una relación de carácter abierto, que deberá ser continuada y

completada, en paralelo con la evolución de las legislaciones extranjeras y de los estudios correspondientes.

La segunda Orden es la de 31 de julio de 1998 por la que se amplía la relación de países con protección de datos de carácter personal equiparable a la española, a efectos de transferencia internacional de datos[110]. Se hace constar que con posterioridad a la aprobación de la Orden de 2 de febrero de 1995 se han promulgado por Italia y Grecia las correspondientes Leyes de Protección de Datos, lo que unido a lo dispuesto en el artículo 1.2 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, que impide restringir o prohibir la libre circulación de datos personales entre los Estados miembros de la Unión Europea, aconsejan la inclusión de los citados países entre los comprendidos en el apartado primero de dicha Orden. Es por ello que se incluye a Italia y a Grecia entre los países relacionados en el apartado primero de la Orden de 2 de febrero de 1995.

Una vez aprobada la LOPD quedó la duda de si la lista aprobada anteriormente en las dos Órdenes seguía vigente. Se formuló la consulta a la Agencia Española de Protección de Datos por una determinada empresa, sobre si es necesaria la autorización del Director de la Agencia para llevar a cabo una transferencia internacional de datos a un tercer Estado no miembro de la Unión Europea ni del Espacio Económico Europeo y respecto de cuyo nivel de protección de datos no existe Decisión alguna por parte de la Comisión Europea, dado que dicho Estado figura en la Orden del Ministerio de Justicia

[110] BOE del 21 de agosto de 1998.

e Interior de 2 de febrero de 1995, por la que se declaran los Estados que ofrecen un nivel de protección de datos equiparable al establecido en la legislación española.

La AEPD respondió con el Informe titulado como "Vigencia de la Orden del Ministerio de Justicia e Interior de 2 de febrero de 1995"[111]. Según el Informe, si bien en el momento de su adopción la Orden de 2 de febrero de 1995 fue dictada por Órgano competente para resolver sobre la existencia o inexistencia de adecuación, dicho Órgano perdió la competencia para decidir sobre esta cuestión con la entrada en vigor de la LOPD, que atribuyó dicha competencia en exclusiva a la Agencia de Protección de Datos. Por este motivo, la Orden, válida en el momento de su adopción, devino contraria a lo establecido en la LOPD, lo que inequívocamente supone que la misma ha de entenderse derogada por ser contraria a la propia Ley, que atribuye en exclusiva a la Agencia la potestad de resolver sobre la existencia del nivel equiparable de protección en el Estado donde se encuentre el destinatario de los datos en una transferencia internacional.

En otro sentido, señala el Informe que la mera inclusión de un determinado país en la Orden de 2 de febrero de 1995 no podría determinar automáticamente el que su nivel de protección pueda ser considerado equiparable al previsto en la LOPD, aprobada casi cinco años después y reguladora de un régimen parcialmente distinto al de la norma derogada.

Hasta la fecha la AEPD no ha usado las herramientas de que dispone para evaluar el nivel adecuado, o no, de protección de ningún país. Como afirma Rebollo Delgado,

[111] Véase página 280 y siguientes de la Memoria Anual de 2002 de la Agencia Española de Protección de Datos.

"esta materia, en buena lógica-jurídica, ha de ser regulada por norma de ámbito supranacional, debido a que de lo contrario, se entraría en un sistema anárquico de cesión de datos a terceros países"[112]. Por dichos motivos los únicos países que han sido calificados con un nivel adecuado de protección son los que han sido examinados por la Comisión Europea. Tal como se indica en el artículo 25.6 de la Directiva comunitaria, los Estados miembros adoptarán las medidas necesarias para ajustarse a las Decisiones de la Comisión.

6. CUMPLIMIENTO DE LAS DISPOSICIONES LEGALES EN EL CASO DE LAS TRANSFERENCIAS A PAÍSES QUE OFRECEN UN NIVEL ADECUADO DE PROTECCIÓN

El artículo 65 del RLOPD dispone que la transferencia internacional de datos no excluye en ningún caso la aplicación de las disposiciones contenidas en la LOPD y en el propio Reglamento[113].

Como indican Barceló y Pérez[114], "el tratamiento debe contar con al menos una de las bases de legitimidad establecidas en los artículos 6, 7 y 11 de la LOPD. Dicho tratamiento debe respetar los principios enumerados en el artículo 4. El responsable del

[112] REBOLLO DELGADO, L: *Vida Privada y Protección de Datos en la Unión Europea*. Dykinson. Madrid 2008, p. 117-118.

[113] Así lo manifiesta también el Informe 101/2003 de la AEPD titulado "*Cumplimiento de la LOPD como requisito previo a la transferencia*". Documento disponible en la dirección electrónica de la AEPD: **https://www.agpd.es/**

[114] BARCELÓ R. y PÉREZ ASINARI, M. V: *Protección de datos. Comentarios al Reglamento de Desarrollo de la LOPD*. Tirant lo Blanc. Valencia 2009, pág. 142.

tratamiento debe informar al titular de los datos, a la luz del artículo 5; deberá adoptar medidas de seguridad (artículo 9), notificar a la AEPD (artículo 26), etc".

La transferencia internacional no deja de ser un acto de tratamiento que tiene su razón de ser en una cesión de datos o bien en el encargo de una prestación de servicios por cuenta de terceros. Por lo tanto, el exportador de los datos tendrá que cumplir, entre otras obligaciones, con el artículo 5 de la LOPD (deber de información), el artículo 11 de la LOPD (deber de obtener el consentimiento del interesado), el artículo 12 de la LOPD (deber de contar con un contrato especial) y el artículo 66.3 del RLOPD (deber de notificación de la transferencia).

El deber de información

En el artículo 5 de la LOPD se encuentra recogido el derecho de información en la recogida de datos. La Instrucción 1/2000 de la AEPD, relativa a las normas por las que se rigen los movimientos internacionales de datos, nos aclara el sentido que hemos de dar a este artículo en el caso de transferencias internacionales de datos. Así en la Norma segunda de la Instrucción se insiste en que la transferencia internacional de datos no excluye de la aplicación de las disposiciones contenidas en la LOPD, conforme a su ámbito de aplicación. Y en concreto, de conformidad con lo establecido en el artículo 5 de la citada norma, cualquier responsable de un fichero o tratamiento que se proponga transferir datos de carácter personal fuera del territorio español[115] deberá haber informado a los afectados de quiénes serán destinatarios de los datos, así como de la

[115] Es bueno recordar que tanto la LOPD como la Instrucción 1/2000 consideraban transferencia internacional de datos toda transmisión de los mismos fuera del territorio español (véase Norma primera de la Instrucción).

finalidad que justifica la transferencia internacional y el uso de los datos que podrá hacer el destinatario. Concluye la Norma segunda manifestando que el deber de información mencionado anteriormente no será de aplicación cuando la transferencia tenga por objeto la prestación de un servicio al responsable del fichero, en los términos establecidos por el artículo 12 de la LOPD.

El deber de obtener el consentimiento del interesado

De acuerdo al artículo 11 de la LOPD, los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el *previo consentimiento* del interesado. Como excepción, para unos pocos casos tasados el consentimiento exigido anteriormente no será preciso:

a. Cuando la cesión está autorizada en una ley.
b. Cuando se trate de datos recogidos de fuentes accesibles al público.
c. Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.
d. Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a

instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.

e. Cuando la cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.
f. Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.

El deber de contar con un contrato especial

En el artículo 12 de la LOPD se regula el acceso a los datos por cuenta de terceros. Según este artículo, no se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento. La realización de estos tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.

En el mismo sentido, según la Norma segunda de la Instrucción 1/2000, el deber de información no será de aplicación cuando la transferencia tenga por objeto la prestación de un servicio al responsable del fichero.

El deber de notificación de la transferencia

Conforme al artículo 66.3 del RLOPD, la transferencia internacional de datos deberá ser notificada a fin de proceder a su inscripción en el Registro General de Protección de Datos (RGPD), conforme al procedimiento establecido en la sección primera del capítulo IV del título IX del propio Reglamento. Si la transferencia ya está prevista, en el momento de notificar el fichero al RGPD ya se deberá hacer constar que se va a proceder a la transferencia internacional. En el caso de transferencias no previstas en el momento de la notificación de los ficheros, deberá procederse a modificar la inscripción inicial a efecto de hacerse constar dicha transferencia internacional.

Suspensión temporal de las transferencias

Ni la Directiva 95/46/CE ni la LOPD mencionan expresamente la suspensión temporal de las transferencias por parte de la autoridad de protección de datos. A falta de esa mención expresa tenemos que recurrir, en el caso de la Directiva, al artículo 28.3, según el cual la autoridad de control dispondrá de poderes efectivos de intervención, como, por ejemplo, el de ordenar el bloqueo, la supresión o la destrucción de datos, o incluso prohibir provisional o definitivamente un tratamiento.

En el caso de la LOPD, hemos de recurrir al artículo 37.1.f), en donde se atribuye a la Agencia Española de Protección de Datos la función de requerir a los responsables y los encargados de los tratamientos, previa audiencia de éstos, la adopción de las medidas necesarias para la adecuación del tratamiento de datos a las disposiciones de la LOPD y, en su caso, ordenar la cesación de los tratamientos y la cancelación de los ficheros, cuando no se ajuste a sus disposiciones.

En el apartado segundo de la Norma cuarta de la Instrucción 1/2000 de la Agencia Española de Protección de Datos se faculta a la Agencia para ordenar la suspensión temporal de las transferencias: El Director de la Agencia de Protección de Datos, en uso de la potestad que le otorga el artículo 37 f) de la LOPD, podrá acordar, previa audiencia del transmitente, la suspensión temporal de la transferencia de datos hacia un receptor ubicado en un tercer Estado del que se haya declarado la existencia de un nivel adecuado de protección, cuando concurra alguna de las circunstancias siguientes, previstas en las Decisiones de la Comisión Europea:

a) Que las Autoridades de Protección de Datos del Estado destinatario o cualquier otra, en caso de no existir las primeras, resuelvan que el destinatario ha vulnerado las normas de protección de datos de su derecho interno.
b) Que existan indicios racionales de que se estén vulnerando las normas o, en su caso, los principios de protección de datos por la entidad destinataria de la transferencia y que las autoridades competentes en el Estado en que se encuentre el destinatario no han adoptado o no van a adoptar en el futuro las medidas oportunas para resolver el caso en cuestión, habiendo sido advertidas de la situación por la Agencia de Protección de Datos. En este caso se podrá suspender la transferencia cuando su continuación pudiera generar un riesgo inminente de grave perjuicio a los afectados. La decisión del Director de la Agencia de Protección de Datos será notificada a la Comisión Europea.

Como señala Fanny Coudert, “considerando que la legislación española en materia de protección de datos es una de las más exigentes del mundo, se entiende fácilmente el recelo de la Agencia sobre las transferencias internacionales de datos. Cualquier

transferencia deberá estar respaldada por las máximas garantías, con el fin de que esta transferencia no burle la legislación española ni menoscabe la protección otorgada a los afectados"[116].

La regulación efectuada en la Instrucción 1/2000 no suponía una innovación normativa. En las primeras Decisiones de la Comisión relativas a países con nivel de protección adecuado de los datos personales (Suiza[117] Hungría[118] y principios de puerto seguro en Estados Unidos[119]), se venía empleando una fórmula muy parecida, en la que facultaba a las autoridades correspondientes de los Estados miembros para suspender los flujos de datos hacia un receptor en el país tercero, con la finalidad de proteger a los particulares contra el tratamiento de sus datos personales. Los motivos que permitían la suspensión son casi coincidentes con los que posteriormente encontramos en la Instrucción 1/2000.

En el artículo 69 del RLOPD, nuevamente sobre la base del artículo 37.1.f) de la LOPD, se vuelve a redactar un contenido muy similar al de la Instrucción 1/2000 y al de las Decisiones de la Comisión. Se añade en el punto 2 del artículo 69 el mecanismo a seguir para ordenar la suspensión temporal: ésta se acordará previa la tramitación del procedimiento establecido en la sección segunda del capítulo V del título IX del RLOPD (procedimiento que estudiaremos en detalle en el capítulo IV de esta tesis doctoral).

---

[116] COUDERT, F: *Estudio práctico sobre la protección de datos de carácter personal*. Lex Nova. Valladolid 2005, pág. 385.

[117] Decisión 2000/518/CE, de 26 de julio de 2000.

[118] Decisión 2000/519/CE, de 26 de julio de 2000.

[119] Decisión 2000/520/CE, de 26 de julio de 2000.

Como nos indica el artículo 144 del RLOPD, la suspensión se levantará tan pronto como cesen las causas que la hubieran justificado. El acuerdo de levantamiento de la suspensión temporal será notificado al exportador y al Ministerio de Justicia, al efecto de que se proceda a su notificación a la Comisión Europea y a los demás Estados miembros de la Unión Europea de acuerdo a lo previsto en el artículo 26.3 de la Directiva 95/46/CE.

Como valoración final de este apartado podemos destacar dos puntos muy llamativos de la normativa española en cuanto al cumplimiento de las disposiciones legales en las transferencias a países que ofrecen un nivel adecuado de protección:

En primer lugar, y como ya se ha comentado anteriormente, la normativa española es muy exigente en cuanto a los requisitos que se han de cumplir para que una transferencia internacional sea considerada lícita. Con ello se pretende obtener las máximas garantías para los afectados. Sin embargo ese nivel de exigencia puede tener un resultado totalmente contrario al buscado: ante la dificultad de cumplir con todas las exigencias de la normativa lo más cómodo es incumplir totalmente la ley y actuar al margen de la misma.

En segundo lugar podemos citar las duras sanciones que pueden aplicarse en el caso de incumplir con los requisitos exigidos por la LOPD y el RLOPD. Buena parte de dichos incumplimientos están recogidos en el artículo 44 de la LOPD como infracciones graves, sancionadas de acuerdo al artículo 45 de la Ley con multa de 40.001 a 300.000 euros.

7. LAS TRANSFERENCIAS A ESTADOS QUE PROPORCIONEN UN NIVEL ADECUADO DE PROTECCIÓN EN LA PROPUESTA DE REGLAMENTO DE PROTECCIÓN DE DATOS DE LA UE

La Directiva 95/46/CE ha sido un instrumento legislativo básico para la protección de datos personales en Europa. Sus objetivos siguen siendo válidos a día de hoy: asegurar el funcionamiento del mercado único y la protección efectiva de los derechos y las libertades de los ciudadanos. Sin embargo desde 1995 se han producido cambios tecnológicos tan importantes como la revolución de Internet. Ello hace imprescindible modificar la normativa para preservar en este nuevo escenario el derecho a la protección de datos personales. Esta normativa nueva en gestación se encuentra en la Propuesta de 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[120].

El nuevo Reglamento modifica la filosofía anterior en el sentido de que ya no se aprobará una nueva Directiva para que posteriormente los diferentes países transpongan su contenido a través de normas nacionales. En su lugar habrá una normativa única y válida en toda la UE sobre protección de datos.

Los cambios sobre la normativa actual son muy importantes, pero por la materia que aquí estudiamos nos centraremos en el ámbito de las transferencias internacionales de datos. Y dentro del campo de las transferencias veremos en el próximo Capítulo que

[120] Propuesta de 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 (Reglamento general de protección de datos). Bruselas, 25.1.2012. COM(2012) 11 final.

los cambios más relevantes se producirán en las transferencias a estados que no proporcionan un nivel adecuado de protección.

En la Exposición de Motivos de la propuesta de Reglamento se pone de relieve que, a día de hoy, “la complejidad de las normas en materia de transferencias internacionales de datos personales constituye un impedimento sustancial a su funcionamiento, ya que se necesita transferir con regularidad datos personales de la UE a otras partes del mundo”.

La rápida evolución tecnológica y la globalización han incrementado de manera espectacular la magnitud del intercambio y la recogida de datos. Tal como se indica en el Considerando 5 de la Propuesta de Reglamento, ello exige “que se facilite aún más la libre circulación de datos dentro de la Unión y la transferencia a terceros países, garantizando al mismo tiempo un elevado nivel de protección de los datos personales”.

En el Considerando 78 de la Propuesta de Reglamento se reconoce que “los flujos transfronterizos de datos personales son necesarios para la expansión del comercio y la cooperación internacionales”.

Y según el Considerando 80, la Comisión podrá determinar, con efectos para toda la Unión, que algunos terceros países, un territorio o un sector del tratamiento en un tercer país, o una organización internacional ofrecen un nivel adecuado de protección de datos, proporcionando así seguridad jurídica y uniformidad en toda la Unión en lo que se refiere a los terceros países u organizaciones internacionales que se considera aportan tal nivel de protección. En estos casos, se podrán realizar transferencias de datos personales a estos países sin tener que obtener ninguna otra autorización.

Al igual que en la Directiva 95/46/CE no se define el concepto de transferencia de datos. En el Dictamen del Comité Económico y Social Europeo sobre la Propuesta de Reglamento[121] se reclama que lo que se entienda por transferencia de datos debería recogerse en el artículo 4, titulado como *Definiciones*.

La transferencia de datos personales a terceros países u organizaciones internacionales se contempla en el capítulo V de la propuesta de Reglamento (artículos 40 a 45), siendo reguladas las transferencias con una decisión de adecuación en su artículo 41.

Según el artículo 41.1, podrá realizarse una transferencia cuando la Comisión haya decidido que el tercer país, o un territorio o un sector de tratamiento de datos en ese tercer país, o la organización internacional de que se trate garantizan un nivel de protección adecuado. Dichas transferencias no requerirán nuevas autorizaciones.

El Grupo de Trabajo en su Documento WP 191[122] opina que en este artículo debería incluirse la obligación de que la Comisión consulte al Consejo Europeo de Protección de Datos (organismo que sustituye al Grupo de protección de las personas en lo que respecta al tratamiento de datos personales creado con arreglo al artículo 29) sobre las decisiones de adecuación.

En el artículo 41.2 se regulan los elementos que la Comisión tomará en consideración al evaluar la adecuación del nivel de protección (materia que a día de hoy se encuentra esencialmente en los Documentos de Trabajo del Grupo del artículo 29):

[121] El Dictamen se encuentra publicado en el DOUE C 229 de 31 de julio de 2012.

[122] Dictamen 01/2012 sobre las propuestas de reforma de la protección de datos, WP 191, adoptado el 23 de marzo de 2012.

a) el Estado de Derecho, la legislación pertinente en vigor, tanto general como sectorial, en particular en lo que respecta a la seguridad pública, la defensa, la seguridad nacional y el Derecho penal, las normas profesionales y las medidas de seguridad en vigor en el país de que se trate o aplicables a la organización internacional en cuestión, así como los derechos efectivos y exigibles, incluido el derecho de recurso administrativo y judicial efectivo de los interesados, en particular los residentes en la Unión cuyos datos personales estén siendo transferidos;

b) la existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el tercer país u organización internacional de que se trate, encargadas de garantizar el cumplimiento de las normas en materia de protección de datos, de asistir y asesorar a los interesados en el ejercicio de sus derechos y de cooperar con las autoridades de control de la Unión y de los Estados miembros; y

c) los compromisos internacionales asumidos por el tercer país o la organización internacional de que se trate.

Como indica el Grupo de Trabajo en su Documento WP 191, las decisiones de adecuación son una ayuda a los responsables, proporcionándoles “recintos protegidos” a los que podrán efectuar transferencias sin necesidad de obtener autorizaciones.

En sentido contrario, de acuerdo al artículo 41.5, la Comisión podrá decidir que un tercer país, o un territorio o un sector de tratamiento de datos en ese tercer país, o una organización internacional no garantizan un nivel de protección adecuado.

En relación al contenido del artículo 41.5, el Dictamen del Supervisor Europeo de Protección de Datos sobre el paquete de reforma de la protección de datos[123] considera que sería oportuno que el artículo 41, junto con el Considerando 82 de la Propuesta de Reglamento, aclarasen que en el caso de una decisión de falta de adecuación, las transferencias deberían permitirse únicamente con las garantías adecuadas o si dicha transferencia está sujeta a alguna de las excepciones establecidas en el artículo 44.

También incide en el mismo tema el Grupo de Trabajo en su documento WP 191. Opina que debe aclararse si en caso de una decisión de adecuación negativa de la Comisión, las transferencias de datos al país tercero en cuestión son, sin embargo, posibles en base a los artículos 42 a 44 (transferencias mediante garantías apropiadas y por medio de excepciones).

Resulta llamativo que el artículo 41 reserve las evaluaciones de adecuación del nivel de protección a la Comisión. Con la normativa actual, las diferentes autoridades nacionales en materia de protección de datos también tienen la posibilidad de efectuar dichas evaluaciones. En este sentido se expresa el artículo 67 del RLOPD, si bien en la práctica no se ha tomado ninguna determinación de adecuación por parte de la Agencia Española de Protección de Datos.

El Supervisor Europeo de Protección de Datos en su Dictamen de 7 de marzo de 2012 opina que debería incluirse la posibilidad de la "información y consulta del Comité de empresa europeo con ocasión de las transferencias internacionales de datos de los empleados, en especial a terceros países.

[123] Puede encontrarse el Resumen del Dictamen de 7 de marzo del SEPD en el DOUE C 192 de 30 de junio de 2012, o bien su versión íntegra en el sitio web del SEPD **http://www.edps.europa.eu**

Otro tema que ha generado mucha polémica y una lucha sin cuartel entre las instituciones de la Unión Europea tampoco tiene una solución clara en la Propuesta de Reglamento. Se trata de las transmisiones de datos de los pasajeros. Parece ser que en la nueva normativa tampoco se resolverá este asunto tan espinoso y difícil de encauzar, ya que quien decide en esta materia son los Estados Unidos y no los países europeos.

CAPÍTULO III

TRANSFERENCIAS A ESTADOS QUE NO PROPORCIONEN UN NIVEL ADECUADO DE PROTECCIÓN

INTRODUCCIÓN

De acuerdo al artículo 33.1 de la LOPD, "no podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley[124], salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas"[125].

Es importante aclarar que la AEPD es la única que tiene competencias en cuestión de transferencias internacionales de datos, tal como regulan los artículos 37 y 41 de la LOPD. Las Agencias de Protección de Datos autonómicas (Madrid, Cataluña y País Vasco) tienen competencias en el marco de los ficheros de datos de carácter personal creados o gestionados por las Comunidades Autónomas y por la Administración Local

[124] Es interesante la lectura del documento de María José Blanco Antón, Subdirectora General del Registro General de Protección de Datos, *Cloud Computing y protección de datos personales*, para el Seminario SOCINFO: Compartición de Recursos y Cloud Computing, Madrid, 11 de enero de 2011. En dicho documento se contempla el caso de que los datos se encuentren en algún país tercero sin nivel adecuado de protección. Documento disponible en la dirección electrónica de la AEPD: **https://www.agpd.es/**

[125] De acuerdo al artículo 44.4.d) de la LOPD (tras la modificación efectuada en la Ley 2/2011, de 4 de marzo, de Economía Sostenible), es una infracción muy grave la transferencia internacional de datos de carácter personal con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Director de la Agencia Española de Protección de Datos salvo en los supuestos en los que conforme a esta Ley y sus disposiciones de desarrollo dicha autorización no resulta necesaria. En el artículo 45.3 de la LOPD se cuantifica la sanción para las infracciones muy graves: multa de 300.001 a 600.000 euros.

de su ámbito territorial. Pero incluso en este tipo de ficheros las competencias relativas a las transferencias internacionales de datos son de la AEPD.

De acuerdo con el artículo 25.1 de la Directiva 95/46/CE, los Estados miembros dispondrán que la transferencia a un país tercero de datos personales que sean objeto de tratamiento o destinados a ser objeto de tratamiento con posterioridad a su transferencia, únicamente pueda efectuarse cuando, sin perjuicio del cumplimiento de las disposiciones de Derecho nacional adoptadas con arreglo a las demás disposiciones de la Directiva, el país tercero de que se trate garantice un nivel de protección adecuado. Se complementa dicho artículo con el 26.2, según el cual "los Estados miembros podrán autorizar una transferencia o una serie de transferencias de datos personales a un tercer país que no garantice un nivel de protección adecuado con arreglo al apartado 2 del artículo 25, cuando el responsable del tratamiento ofrezca garantías suficientes respecto de la protección de la vida privada, de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los respectivos derechos; dichas garantías podrán derivarse, en particular, de cláusulas contractuales apropiadas".

Según el artículo 66.1 del RLOPD, para que la transferencia internacional de datos pueda considerarse conforme a lo dispuesto en la LOPD y al propio Reglamento "será necesaria la autorización del Director de la Agencia Española de Protección de Datos, que se otorgará en caso de que el exportador aporte las garantías a las que se refiere el artículo 70 del propio reglamento".

El contenido de la Directiva y la normativa española que la transpone no son coincidentes en el sentido de que no solo se exige la formalización de dicho contrato sino que, adicionalmente habrá que obtener la autorización del Director de la AEPD.

Así lo señala de forma acertada Álvarez Rigaudias: "a diferencia de lo que ocurre en otros Estados miembros, el mero otorgamiento de estas cláusulas contractuales tipo aprobadas por la Comisión no ha sido considerado por la norma española como una excepción a la autorización previa de la AEPD, sobre la base de que la excepción a esta autorización de la letra k) del art. 34 de la LOPD se refiere a Estados y no a contratos de *nivel adecuado*. Esta diferencia en la transposición de la Directiva 95/46/CE ha sido objeto de crítica constante, por resultar contrario al principio de *interpretación conforme*, dado que las transferencias realizadas al amparo de estas cláusulas contractuales tipo aprobadas por la Comisión gozarían, por definición, de un nivel *adecuado* de protección con la Directiva 95/46/CE"[126].

El artículo 70 del RLOPD nos indica las posibles vías de aportación de garantías:

- La autorización podrá ser otorgada en caso de que el responsable del fichero o tratamiento aporte un contrato escrito, celebrado entre el exportador y el importador, en el que consten las necesarias garantías de respeto a la protección de la vida privada de los afectados y a sus derechos y libertades fundamentales y se garantice el ejercicio de sus respectivos derechos.
- También podrá otorgarse la autorización para la transferencia internacional de datos en el seno de grupos multinacionales de empresas cuando hubiesen sido adoptados por los mismos normas o reglas internas en que consten las necesarias garantías de respeto a la protección de la vida privada y el derecho fundamental a la protección de datos de los afectados y se garantice asimismo el

[126] ÁLVAREZ RIGAUDIAS, C: "Condiciones para las transferencias internacionales de datos personales en servicios de cloud". Forma parte de la obra de VV. AA: *Derecho y Cloud Computing*. Civitas. Navarra 2012. Pág. 120-121.

cumplimiento de los principios y el ejercicio de los derechos reconocidos en la LOPD y el propio Reglamento.

1. LOS CONTRATOS ENTRE EL EXPORTADOR Y EL IMPORTADOR

En el capítulo anterior habíamos comentado extensamente el Documento de Trabajo, elaborado por el Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, referente 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*[127] -WP 12-. El capítulo cuatro de dicho Documento de Trabajo está referido a la función de las disposiciones contractuales, analizándose entre otros elementos, los requisitos específicos de una solución contractual.

Si analizamos nuestra normativa interna, en la Norma quinta de la Instrucción 1/2000, relativa a las normas por las que se rigen los movimientos internacionales de datos, se establece que la autorización a una transferencia internacional será otorgada en caso de que el responsable del fichero aporte un contrato escrito, celebrado entre el transmitente y el destinatario, en el que consten las necesarias garantías de respeto a la protección de la vida privada de los afectados y a sus derechos y libertades fundamentales y se garantice el ejercicio de sus respectivos derechos. El citado contrato deberá contener, al menos, las siguientes menciones:

a) La identificación del transmitente y el destinatario de los datos.

b) La indicación de la finalidad que justifica la transferencia internacional, así como de los datos que son objeto de la transferencia.

[127] Aprobado por el Grupo de Trabajo el 24 de julio de 1998.

c) El compromiso del transmitente de que la recogida y tratamiento de los datos en territorio español respeta íntegramente las normas contenidas en la LOPD y que el fichero en que se encuentran los datos objeto de la transferencia está inscrito en el Registro General de Protección de Datos o se ha solicitado su inscripción.

d) El compromiso del destinatario de que los datos recibidos serán tratados exclusivamente para la finalidad que motiva la transferencia, así como que procederá a su tratamiento de acuerdo con las normas de protección de datos del derecho español. Asimismo, el destinatario deberá comprometerse a no comunicar los datos a ningún tercero en tanto no haya sido recabado el consentimiento del afectado para ello.

e) Que el destinatario adoptará las medidas de seguridad requeridas por la normativa de protección de datos de carácter personal vigente en España.

f) Que el transmitente y el destinatario responderán solidariamente frente a los particulares, a la Agencia de Protección de Datos y a los Órganos Jurisdiccionales españoles por los eventuales incumplimientos del contrato en que pudiera incurrir el receptor, cuando los mismos sean constitutivos de infracción de lo dispuesto en la LOPD o produzcan un perjuicio a los afectados.

g) Que se indemnizará al afectado que resulte perjudicado como consecuencia del tratamiento efectuado por el destinatario, según el régimen de responsabilidad al que se refiere el apartado anterior.

h) La garantía de que el afectado podrá ejercitar los derechos de acceso, rectificación, cancelación y oposición, tanto ante el transmitente como ante el destinatario de los datos. Asimismo, deberá indicarse que el interesado podrá

recabar la tutela de la Agencia de Protección de Datos en los supuestos previstos en la LOPD en caso de que sus derechos no sean atendidos.

i) El compromiso del destinatario de los datos de autorizar el acceso al establecimiento donde se estén tratando los mismos, así como a la documentación y a los equipos físicos y lógicos, de representantes de la Agencia de Protección de Datos o de la entidad independiente en quien ésta delegue, cuando la Agencia lo requiera con el fin de verificar el cumplimiento de las obligaciones derivadas del contrato.

j) La obligación de que, una vez extinguida la relación contractual, los datos de carácter personal deberán ser destruidos o devueltos al transmitente, al igual que cualquier soporte o documento en que conste algún dato de carácter personal objeto de la transferencia.

k) Que los afectados podrán exigir el cumplimiento de lo estipulado en el contrato en todas aquellas cuestiones en que el mismo les resulte beneficioso.

El artículo 26.4 de la Directiva 95/46/CE regula que cuando la Comisión decida, según el procedimiento establecido en el apartado 2 del artículo 31, que determinadas cláusulas contractuales tipo ofrecen las garantías suficientes establecidas en el apartado 2, los Estados miembros adoptarán las medidas necesarias para ajustarse a la decisión de la Comisión.

Los contratos representan una alternativa jurídica excepcional para facilitar la circulación internacional de datos personales. Como indica Remolina Angarita, “es útil para las empresas de países no catalogados con nivel adecuado de protección que deseen *importar* datos personales provenientes de los Estados miembros de la UE, pero

también favorece a las empresas de la Comunidad que deseen *exportar* tal información a terceros países bajo la precitada circunstancia"[128].

La Instrucción 1/2000 hace constar que surtirán el mismo efecto jurídico los contratos que atiendan a la regulación de la propia Instrucción y aquellos que pudieran celebrarse en el futuro al amparo de lo que, en su caso, dispongan las Decisiones de la Comisión Europea que den cumplimiento a lo establecido en el artículo 26.4 de la Directiva 95/46/CE, siempre que se acredite su íntegro cumplimiento[129].

El artículo 70 del RLOPD, considera que establecen las adecuadas garantías los contratos que se celebren de acuerdo con lo previsto en las Decisiones de la Comisión Europea 2001/497/CE, de 15 de Junio de 2001, 2002/16/CE, de 27 de diciembre de 2001, y 2004/915/CE, de 27 de diciembre de 2004 o de lo que dispongan las Decisiones de la Comisión[130] que den cumplimiento a lo establecido en el artículo 26.4 de la Directiva 95/46/CE[131].

---

[128] REMOLINA ANGARITA, N. y otros: *Obligaciones y Contratos en el Derecho Contemporáneo*. Universidad de La Sabana. Bogotá 2010, pág. 387.

[129] Se ha de tener en cuenta que a la fecha de aprobación de la Instrucción (uno de diciembre de 2000) todavía no se había regulado ningún contrato por parte de la Comisión Europea.

[130] En la página 25 del documento denominado *FREQUENTLY ASKED QUESTIONS RELATING TO TRANSFERS OF PERSONAL DATA FROM THE EU/EEA TO THIRD COUNTRIES*, elaborado por la Comisión Europea, se plantea la cuestión de si las empresas pueden emplear contratos aprobados a nivel nacional. La respuesta es afirmativa. La existencia de cláusulas contractuales tipo no impide la existencia presente o futura de contratos autorizados por las autoridades de protección de datos de un país, en cumplimiento de su legislación nacional. Estas autorizaciones pueden ser concedidas si la autoridad nacional de protección de datos considera que ofrecen las debidas salvaguardas para los datos exportados a terceros países. El contenido de estos contratos puede ser distinto al de las cláusulas contractuales tipo de la Comisión. Estos contratos necesitan notificarse por el Estado miembro a la Comisión y a los otros Estados miembros.

La Instrucción 1/2000, en el punto 7 de la Norma quinta, regula la denegación de la autorización o la suspensión temporal de la transferencia. Dicha denegación o suspensión temporal la podrá resolver el Director de la Agencia Española de Protección de Datos, previa audiencia del transmitente, cuando concurra alguna de las circunstancias siguientes:

a) Que la situación de protección de los derechos fundamentales y libertades públicas en el país de destino o su legislación **impidan garantizar el íntegro cumplimiento del contrato** y el ejercicio por los afectados de los derechos que el contrato garantiza.

b) Que la entidad destinataria **haya incumplido previamente** las garantías establecidas en cláusulas contractuales de este tipo.

c) Que existan indicios racionales de que las **garantías ofrecidas** por el contrato **no están siendo o no serán respetadas** por el destinatario.

d) Que existan **indicios racionales** de que los **mecanismos de aplicación del contrato no son o no serán efectivos**.

e) Que la transferencia, o su continuación, en caso de haberse iniciado, pudiera crear una **situación de riesgo de daño efectivo** a los afectados.

Las resoluciones del Director de la Agencia de Protección de Datos por las que se deniegue o suspenda una transferencia internacional de datos serán notificadas a la Comisión Europea cuando así sea exigible.

Documento disponible en la web:

http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf

[131] El RLOPD fue aprobado el 21 de diciembre de 2007. Los tres contratos que hace constar de forma expresa eran los vigentes en esa fecha.

El artículo 70.3 del RLOPD reproduce casi literalmente el contenido del punto 7 de la Norma quinta de la Instrucción 1/2000. Añade una cuestión de procedimiento al indicar que la suspensión se acordará previa la tramitación del procedimiento establecido en la sección segunda del capítulo V del título IX del propio Reglamento.

1.1. CLÁUSULAS CONTRACTUALES TIPO DE LA COMISIÓN EUROPEA

Las reglas contractuales del punto 2 de la Norma quinta de la Instrucción 1/2000 tuvieron en la práctica una vida muy efímera. Tan pronto como fueron apareciendo las cláusulas contractuales tipo de la Comisión Europea cesó el uso de las primeras[132]. Es por ello que centraremos este apartado en el análisis de las cláusulas contractuales aprobadas por la Comisión[133].

Podremos comprobar que el alma del contrato no es la autonomía de la voluntad de las partes cuando se está negociando la exportación o importación de datos personales. Como señala Remolina Angarita, "el libre albedrío de las partes no puede comprometer

[132] En la página web de la AEPD podemos observar la evolución de las autorizaciones del Director de la Agencia. A 31-03-2011, de un total de 613 autorizaciones, 526 estaban basadas en las Decisiones 2002/16/CE y 2010/87UE (responsable a encargado) y 82 se basaban en la Decisión 2001/497/CE (responsable a responsable).

[133] Como indica la CNIL (Commission Nationale de l'Informatique et des Libertés) en un documento descargable de su web: *Les Clauses Contractuelles Types de la Commission Europeenne*, las "cláusulas contractuales tipo" son modelos de cláusulas contractuales adoptadas por la Comisión Europea que permiten encuadrar las transferencias de datos personales efectuadas por responsables de tratamiento hacia destinatarios situados fuera de la UE. Pretenden facilitar la tarea de los responsables de tratamiento a la hora de elaborar contratos de transferencia. En el mismo documento se ofrece una guía práctica para las distintas hipótesis de transferencia en términos prácticos, lo cual puede ser una guía muy valiosa a la hora de plantearse un caso real de transferencia.

El documento se puede encontrar en:

http://www.cnil.fr/fileadmin/documents/Vos_responsabilites/Transferts/CNIL-transferts-CCT.pdf

los derechos de los titulares de los datos frente al tratamiento indebido de los mismos"[134].

De conformidad con la Directiva 95/46/CE, el nivel de protección de los datos debe apreciarse teniendo en cuenta todas las circunstancias relacionadas con la transferencia o la serie de transferencias. El Grupo de Trabajo ha emitido directrices que ayudan a realizar la evaluación[135]. Si nos centramos en las cláusulas contractuales tipo[136], también ha elaborado varios documentos en los que expresa su punto de vista[137].

---

[134] REMOLINA ANGARITA, N. y otros: *Obligaciones y Contratos en el Derecho Contemporáneo*. Universidad de La Sabana. Bogotá 2010, pág. 402.

[135] Las principales directrices se contienen en los siguientes documentos de trabajo:

- WP 4 «Primeras orientaciones sobre la transferencia de datos personales a terceros países. Posibles formas de evaluar la adecuación», documento adoptado por el Grupo de trabajo el 26 de junio de 1997.

- WP 7 «Evaluación de la autorregulación industrial: ¿En qué casos realiza una contribución significativa al nivel de protección de datos en un tercer país?», documento adoptado por el Grupo de trabajo el 14 de enero de 1998.

- WP 9 «Conclusiones preliminares sobre la utilización de disposiciones contractuales en caso de transferencia de datos personales a terceros países», documento adoptado por el Grupo de trabajo el 22 de abril de 1998.

- WP 12 «Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE», documento adoptado por el Grupo de trabajo el 24 de julio de 1998.

[136] Véase el documento MEMO/05/3 emitido en Bruselas el 7 de enero de 2005 por la Comisión Europea, titulado *Standard contractual clauses for the transfer of personal data to third countries - Frequently asked questions*. En este documento se responde a las dudas más frecuentes sobre las cláusulas contractuales tipo.

[137] Los principales se contienen en los siguientes documentos de trabajo:

- WP 9 (ya citado anteriormente).

- WP 38 final «Dictamen 1/2001 sobre el proyecto de Decisión de la Comisión relativa a las cláusulas contractuales tipo para la transferencia de datos personales a terceros países al amparo del apartado 4 del artículo 26 de la Directiva 95/46», documento adoptado por el Grupo de trabajo el 26 de enero de 2001.

- WP 47 «Dictamen 7/2001 relativo al proyecto de Decisión de la Comisión (versión de 31 de agosto de 2001) sobre las cláusulas contractuales tipo para la transferencia de datos personales a

Tal como nos dice el Documento de trabajo **WP 9** del G29, la idea de utilizar un contrato para regular las transferencias internacionales de datos personales no proviene, obviamente, de la Directiva. Ya en 1992, el Consejo de Europa, la Cámara Internacional de Comercio y la Comisión Europea iniciaron conjuntamente un estudio del tema. Posteriormente, un número importante de expertos y analistas, inspirados quizá por la referencia explícita de la Directiva, también comentaron el uso de contratos en estudios y artículos. Pero los contratos ya venían utilizándose de forma habitual en el "mundo real" con el objeto de resolver los problemas de protección planteados por el envío de datos personales desde algunos Estados miembros de la UE. En Francia, se venía haciendo un uso extensivo de ellos desde finales de la década de los ochenta.

Dentro de la Unión Europea se utilizan contratos para determinar el reparto de responsabilidades en materia de protección de datos entre el responsable del tratamiento

---

encargados del tratamiento establecidos en terceros países, al amparo de lo dispuesto en el apartado 4 del artículo 26 de la Directiva 95/46», documento aprobado por el Grupo de trabajo el 13 de septiembre de 2001.

- WP 84 «Dictamen 8/2003 sobre el proyecto de cláusulas tipo presentado por un grupo de asociaciones empresariales ("The alternative model contract")», documento adoptado por el Grupo de trabajo el 17 de diciembre de 2003.

- WP 161 «Dictamen 3/2009 sobre el proyecto de Decisión de la Comisión relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE (de los responsables a los encargados del tratamiento)», documento emitido por el Grupo de trabajo el 5 de marzo de 2009.

- WP 176 «Liste des questions les plus fréquentes soulevées par l'entrée en vigueur de la décision 2010/87/UE de la Commission du 5 février 2010 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE du Parlement européen et du Conseil")», documento adoptado por el Grupo de trabajo el 12 de julio de 2010.

y el subcontratista encargado de llevarlo a cabo[138]. En el supuesto de que se utilice un contrato en relación con transferencias de datos a terceros países, debe esperarse mucho más del mismo: ha de ofrecer a la persona a la que se refieran los datos salvaguardas adicionales, puesto que el receptor establecido en el tercer país no está sujeto a una serie de normas obligatorias en la materia que garanticen un nivel de protección adecuado.

Para evaluar la idoneidad de las salvaguardas ofrecidas por una solución contractual debe partirse de la misma base que para evaluar el nivel general de protección en un tercer país. Una solución contractual debe contener todos los principios básicos para la protección de datos y ofrecer los medios necesarios para que pueda velarse por su observancia.

El contrato debe fijar pormenorizadamente la finalidad, los medios y las condiciones del tratamiento de los datos transferidos, así como la forma en que se aplicarán los principios básicos de protección de datos. Los contratos que limitan la posibilidad de que el receptor de los datos los procese por cuenta propia de forma autónoma ofrecen una mayor seguridad jurídica. Por consiguiente, en la medida de lo posible, el contrato debería servir para atribuir al remitente de los datos un poder decisorio sobre el tratamiento efectuado en el tercer país.

[138] En España tenemos esta obligación regulada en el artículo 12.2 de la LOPD: "La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas. En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar".

Si el receptor disfruta de cierta autonomía en relación con el tratamiento de los datos transferidos, la situación es más compleja y es posible que un simple contrato entre las partes de la transferencia no siempre permita a las personas a las que se refieren los datos ejercer sus derechos. Puede resultar necesario un mecanismo por el cual el remitente establecido en la Unión Europea conserve la responsabilidad por los daños que pudieran derivarse del tratamiento llevado a cabo en el tercer país.

El contrato debería excluir expresamente la posibilidad de que los datos sean transmitidos posteriormente por el receptor a organismos no vinculados por el contrato, a menos que pueda obligarse a terceros mediante disposiciones contractuales a respetar los mismos principios de protección de datos.

La confianza en el respeto de tales principios, una vez efectuada la transferencia, mejoraría si el cumplimiento de los mismos por parte del receptor quedase sujeto a una verificación externa, de la que podría encargarse, por ejemplo, una empresa de auditoría especializada o un organismo de normalización o certificación.

En el supuesto de que la persona a la que se refieren los datos tope con algún problema, como consecuencia, en su caso, del incumplimiento de las cláusulas sobre protección de datos contenidas en el contrato, resulta, en general, difícil asegurarse de que la queja del interesado se investiga convenientemente. Las autoridades supervisoras de los Estados miembros experimentarán dificultades de orden práctico a la hora de llevar a cabo tales indagaciones.

Las soluciones contractuales resultan probablemente más adecuadas para las grandes redes internacionales (tarjetas de crédito, reservas de billetes de avión), que se caracterizan por un elevado volumen de transferencias de datos similares y repetitivas, y por la existencia de un número relativamente reducido de grandes empresas que operan

en sectores ya sujetos a supervisión y regulación públicas. Otro caso en el que la utilización de contratos presenta un potencial considerable es el de las transferencias de datos entre distintas sucursales o empresas del mismo grupo[139].

Los países en los que las prerrogativas con que cuentan los poderes públicos para acceder a la información son más amplias de lo que autorizan las normas sobre protección de los derechos humanos aceptadas a nivel internacional no constituyen un destino seguro para las transferencias basadas en cláusulas contractuales.

En el Dictamen 1/2001 -WP 38 final- sobre el proyecto de Decisión de la Comisión relativa a las cláusulas contractuales tipo para la transferencia de datos personales a terceros países al amparo del apartado 4 del artículo 26 de la Directiva 95/46, el G29 analiza el proyecto de lo que acabará convirtiéndose en la **Decisión de la Comisión 2001/497/CE**, de 15 de junio de 2001 relativa a cláusulas contractuales tipo para la transferencia de datos personales a un tercer país.

El Grupo de Trabajo reconoce la labor efectuada por el Subgrupo de cláusulas contractuales (representado en el caso de España por la Agencia Española de Protección

[139] En la página 29 del documento denominado *FREQUENTLY ASKED QUESTIONS RELATING TO TRANSFERS OF PERSONAL DATA FROM THE EU/EEA TO THIRD COUNTRIES*, elaborado por la Comisión Europea, se plantea la cuestión de si las cláusulas contractuales tipo son necesarias para las empresas de Estados Unidos cubiertas por el sistema de puerto seguro. Como regla general no es necesario el uso de cláusulas contractuales tipo. Sin embargo, si la transferencia se refiere a datos personales que no están cubiertos por los principios de puerto seguro o se trata de un sector que queda fuera de la supervisión de la FTC o del Departamento de Transporte, el uso de cláusulas contractuales tipo es una vía para proveer las salvaguardias necesarias.

Documento disponible en la web:

http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf

de Datos), los servicios de la Comisión y los representantes de la industria. Acoge favorablemente la propuesta de la Comisión, considerando que dichas cláusulas contractuales tipo cubrirán, no sólo el papel establecido en el artículo 26.4 de la Directiva, sino que, al mismo tiempo, se convertirán en un documento de referencia para la protección de datos a nivel internacional.

El Grupo destaca en el Documento de Trabajo que el ámbito de la Decisión se limita a las transferencias en las que ambas partes actúan como responsables del tratamiento. Anima a la Comisión a abordar urgentemente en una futura decisión las cláusulas contractuales para las transferencias que no queden comprendidas por el proyecto de Decisión, es decir, aquéllas en las que el destinatario de los datos situado fuera de la Unión Europea es un encargado del tratamiento que actúa en nombre de un responsable del tratamiento de los datos establecido en la UE.

Tras analizar el documento, y proponer a la Comisión que considere alguna modificación textual en el mismo, el Grupo emite un dictamen favorable sobre el proyecto de Decisión de la Comisión al amparo del apartado 4 del artículo 26, porque ofrece suficientes garantías para la transferencia de datos personales a terceros países, junto con las observaciones recogidas en el propio Dictamen. El Grupo invita a la comunidad empresarial a emplear estas cláusulas una vez que hayan sido aprobadas por la Comisión Europea.

En el Dictamen 7/2001 -WP 37- relativo al proyecto de Decisión de la Comisión sobre las cláusulas contractuales tipo para la transferencia de datos personales a encargados del tratamiento establecidos en terceros países, al amparo de lo dispuesto en el apartado 4 del artículo 26 de la Directiva 95/46, el Grupo de Trabajo sobre protección de datos efectúa el estudio del proyecto de lo que acabará convirtiéndose en la **Decisión**

de la Comisión 2002/16/CE, de 27 de diciembre de 2001 relativa a cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países (Decisión derogada a partir de 15 de mayo de 2010).

El Grupo de Trabajo, en el Dictamen 7/2001, acoge favorablemente el proyecto de Decisión de la Comisión y considera que es necesario que esta Decisión se adopte rápidamente. Recalca la importancia del proyecto de Decisión con vistas a facilitar las incontables transferencias de datos que habitualmente se efectúan desde la Unión Europea al resto del mundo y establecer, al mismo tiempo, las oportunas salvaguardas para proteger la vida privada de las personas cuando los datos personales se transfieran fuera de la Unión.

El Grupo de Trabajo establece en el Dictamen una clara distinción entre las cláusulas de los contratos a que se refiere el artículo 17.3 de la Directiva[140] y las cláusulas contractuales tipo objeto del Dictamen. Si bien es cierto que, a primera vista, ambas transferencias son muy similares, dado que las partes del contrato son idénticas (responsable del tratamiento y encargado del tratamiento) y el objeto de la transferencia es el mismo (servicios de tratamiento de datos), a efectos de lo previsto en el Directiva 95/46/CE, el hecho de que el encargado del tratamiento esté establecido fuera de la UE

[140] Artículo 17.3 de la Directiva 95/46/CE:

La realización de tratamientos por encargo deberá estar regulada por un **contrato** u otro acto jurídico que vincule al encargado del tratamiento con el responsable del tratamiento, y que disponga, en particular:

- que el encargado del tratamiento sólo actúa siguiendo instrucciones del responsable del tratamiento;

- que las obligaciones del apartado 1, tal como las define la legislación del Estado miembro en el que esté establecido el encargado, incumben también a éste.

modifica por completo la naturaleza de la transferencia (transferencia en el interior de la Unión o internacional), así como las normas por las que se rige el contenido del contrato (artículo 17 o artículo 26.4).

A este respecto, el Grupo de Trabajo desea resaltar que el cumplimiento, por parte del responsable del tratamiento, de las disposiciones nacionales adoptadas en virtud de lo previsto en el artículo 17 de la Directiva 95/46/CE, no satisface en sí mismo la exigencia señalada en el artículo 26.2 de la Directiva, esto es, el ofrecer garantías suficientes para que un Estado miembro pueda autorizar una transferencia o una serie de transferencias a tenor de lo establecido en el artículo 26.2, puesto que los contratos considerados deben suplir la falta de una protección adecuada en el país de destino, lo cual no es el objeto del artículo 17 de la Directiva 95/46/CE.

El Grupo de Trabajo opina que, en el caso de transferencia internacional de datos, el importador debe aplicar las medidas de seguridad que se definan en el ordenamiento jurídico del Estado miembro en el que esté establecido el exportador, lo cual es coherente tanto con el principio general con arreglo al cual el importador de los datos queda vinculado por la legislación del país del exportador, como con el hecho de que el exportador dé instrucciones al importador de conformidad con lo previsto en su propia legislación.

El Grupo de Trabajo opina que es extremadamente difícil definir las transferencias posteriores de forma plenamente satisfactoria. Es por ello que recomienda la supresión de la cláusula destinada a regular parcialmente las transferencias posteriores.

El Grupo de Trabajo, junto a una serie de recomendaciones, emite un dictamen favorable en relación con el proyecto de Decisión de la Comisión sobre las cláusulas contractuales tipo para la transferencia de datos personales a encargados del tratamiento

establecidos en terceros países, manifestando su deseo de que la Decisión de la Comisión pudiera surtir efecto lo antes posible.

En el Dictamen 8/2003 -WP 84- sobre el proyecto de cláusulas contractuales tipo presentado por un grupo de asociaciones empresariales («The alternative model contract»), el Grupo de Trabajo sobre protección de datos analiza el proyecto de lo que acabará convirtiéndose en la **Decisión de la Comisión 2004/915/CE**, de 27 de diciembre de 2004, por la que se modifica la Decisión 2001/497/CE, de 15 de junio de 2001.

El Grupo acoge con satisfacción el proyecto de cláusulas contractuales tipo presentado por la Cámara de Comercio Internacional y otras asociaciones empresariales y coincide con la opinión manifestada por la Comisión Europea en cuanto a que debería ser posible adoptar otras cláusulas contractuales tipo, de manera que los operadores económicos tuvieran más variedad donde elegir. Esto ayudaría a las empresas a transferir datos personales a terceros países y, al mismo tiempo, les permitiría garantizar la protección de los derechos y libertades fundamentales de las personas que se benefician de la protección de la Directiva comunitaria sobre protección de datos y de las leyes nacionales de aplicación de dicha Directiva.

Para el Grupo de Trabajo la adopción de un nuevo conjunto de cláusulas contractuales tipo deberá estar condicionada al pleno cumplimiento de dos cuestiones básicas:

a) que las cláusulas contractuales tipo propuestas aporten un nivel de protección comparable al de las adoptadas en virtud de la Decisión 2001/497/CE de la Comisión;

b) que las cláusulas propuestas ofrezcan un valor añadido que supere el mero hecho de ser más favorables para las empresas, y sean también más favorables para los ciudadanos.

El Grupo de Trabajo manifiesta sus dudas acerca de que la propuesta que se le presentó cumpla plenamente con ambas condiciones. Sin embargo considera que se han conseguido avances sustanciales y puesto que las propuestas definitivas no distan mucho de lo que podría considerarse un nivel aceptable de protección de datos, al Grupo le gustaría emitir un dictamen favorable. Para ello se incluyen tres asuntos pendientes que preocupan y constituyen reservas fundamentales que han de ser subsanadas. El Grupo de trabajo insta a la Comisión Europea a velar por que se resuelvan de manera satisfactoria los problemas planteados en el Dictamen y se subsanen las ambigüedades detectadas en el texto de una futura Decisión de la Comisión.

Concluye el dictamen del Grupo de trabajo del artículo 29 manifestándose a favor de la propuesta de cláusulas contractuales tipo para la transferencia de datos personales desde la UE a terceros países (transferencias de responsable a responsable), siempre y cuando se superen las tres deficiencias importantes antes mencionadas.

En el Dictamen 3/2009 -WP 161- sobre el proyecto de Decisión de la Comisión relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE (de los responsables a los encargados del tratamiento), el Grupo de Trabajo sobre protección de datos estudia el texto del proyecto de lo que acabará convirtiéndose en la **Decisión de la Comisión 2010/87/UE**, de 5 de febrero de 2010 relativa a cláusulas contractuales tipo para la transferencia de datos personales a los

encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo.

Durante varios años las empresas y las autoridades de protección de datos habían trabajado con las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en los terceros países, aprobadas por la Comisión Europea el 27 de diciembre de 2001.

Las cláusulas contractuales tipo 2002/16/CE necesitaban una actualización. La razón principal de esa actualización se encontraba en la llamada *externalización global*. Aumenta el número de empresas que no sólo transfieren sus datos a un encargado de tratamiento sino también a *subencargados* y, en ocasiones, a sucesivos *sub-subencargados.* Las cláusulas contractuales tipo 2002/16/CE no eran un medio adecuado para asegurar estas complejas transferencias sucesivas. En consecuencia, la Comisión Europea consideraba necesario modificar dichas cláusulas contractuales, a fin de que el contrato estuviera mejor adaptado a las nuevas prácticas empresariales. Con las nuevas cláusulas contractuales quedarán cubiertas las transferencias internacionales de datos a encargados de tratamiento ubicados fuera del EEE, e incluso la subcontratación que se pueda efectuar con subencargados que se encuentren también fuera del EEE.

En el Dictamen 3/2009 el Grupo de protección formula algunas observaciones sobre la subcontratación internacional del tratamiento de datos fuera del Espacio Económico Europeo (EEE) por un encargado establecido en el EEE, una situación que no está prevista en el proyecto de Decisión de la Comisión y que se está convirtiendo en una práctica cada vez más corriente.

La mayor flexibilidad que se pretende conseguir con el proyecto de Decisión no se aplicará por igual a los diferentes actores en un mercado cada vez más global. De hecho, el proyecto de Decisión de la Comisión permitiría a un encargado de tratamiento establecido en un tercer país realizar transferencias sucesivas con fines de subcontratación con una mera autorización del responsable del tratamiento, mientras que los encargados de tratamiento establecidos en el EEE que deseen subcontratar parte de sus actividades de tratamiento con un subcontratista en un tercer país seguirían sujetos a la actual normativa. Esta situación crearía una desventaja competitiva para las empresas europeas que deberían soportar una carga administrativa superior a la de empresas equivalentes en los terceros países, con el fin de prestar servicios similares de tratamiento de datos.

El Grupo de Trabajo considera necesario encontrar una solución jurídica que permita la subcontratación internacional por encargados establecidos en el EEE sin que se generen desigualdades innecesarias en el mercado. A este respecto se insta a la Comisión a que desarrolle sin demora un nuevo instrumento jurídico específico y separado que permita la subcontratación internacional del tratamiento de datos por los encargados establecidos en la Unión con subcontratistas de terceros países. Dicho instrumento podría consistir, por ejemplo, en un nuevo conjunto de cláusulas contractuales tipo, a través de las cuales el responsable y el encargado establecidos en el EEE podrían proceder a la subcontratación transfronteriza del tratamiento de datos, de acuerdo con las garantías adecuadas que necesitan estas transferencias.

Además de estas observaciones, y de expresar su opinión sobre varios puntos del documento, el Grupo de Trabajo emite su Dictamen favorable al proyecto de Decisión

de la Comisión sobre cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento de datos establecidos en terceros países.

1.1.1. Cláusulas contractuales tipo entre responsables de tratamiento

Decisión 2001/497/CE[141]

Con arreglo a la Directiva 95/46/CE, los Estados miembros dispondrán que la transferencia a un tercer país de datos personales únicamente pueda efectuarse cuando el tercer país de que se trate garantice un nivel de protección de datos adecuado y las disposiciones de Derecho nacional de los Estados miembros, adoptadas con arreglo a los preceptos de la Directiva, se cumplan con anterioridad a la transferencia.

No obstante, el apartado 2 del artículo 26 de la Directiva 95/46/CE establece que los Estados miembros podrán autorizar, con sujeción a determinadas garantías, una transferencia o una serie de transferencias de datos personales a terceros países que no garanticen un nivel de protección adecuado. Dichas garantías podrán derivarse, en particular, de cláusulas contractuales apropiadas.

El establecimiento de cláusulas contractuales tipo es esencial para mantener el necesario flujo de datos personales entre la Unión Europea y terceros países sin imponer cargas innecesarias a los operadores económicos. Ello tiene especial importancia en vista de la escasa probabilidad de que la Comisión adopte resoluciones de adecuación de conformidad con el apartado 6 del artículo 25 para numerosos países a corto o incluso medio plazo.

[141] DOCE L 181 de 4 de julio de 2001.

Como manifiesta el considerando 6 de la Decisión 2001/497/CE, las Decisiones de la Comisión tendrán como efecto únicamente exigir a los Estados miembros que no se nieguen a reconocer que las cláusulas contractuales descritas en ellas proporcionan las garantías adecuadas, por lo que no afectarán de ninguna manera a otras cláusulas contractuales[142].

En el considerando 7 de la Decisión, se limita el ámbito de la misma a establecer que las cláusulas contenidas en su anexo pueden ser utilizadas por un responsable del tratamiento establecido en la UE para ofrecer garantías suficientes a efectos del apartado 2 del artículo 26 de la Directiva 95/46/CE[143]. La transferencia de datos personales a terceros países es una operación de tratamiento en un Estado miembro, cuya legitimidad está sujeta a las disposiciones de Derecho nacional. Las autoridades de control de los Estados miembros seguirán siendo competentes para evaluar si el exportador de datos

---

[142] Como indica la CNIL (Commission Nationale de l'Informatique et des Libertés) en el documento descargable de su web: *Les Clauses Contractuelles Types de la Commission Europeenne*, si se emplean las "cláusulas contractuales tipo" es conveniente tomarlas en su totalidad. Si bien no hay requisito legal que obligue a usarlas sin modificaciones, es preferible no hacerlo. Esto obligaría a su estudio particular por parte de las autoridades de protección de datos para comprobar que ofrecen las garantías adecuadas. El empleo de las cláusulas contractuales tipo garantiza un procedimiento de autorización más rápido y aumenta la seguridad jurídica de las transferencias.

[143] En la página 28 del documento denominado *FREQUENTLY ASKED QUESTIONS RELATING TO TRANSFERS OF PERSONAL DATA FROM THE EU/EEA TO THIRD COUNTRIES*, elaborado por la Comisión Europea, se plantea la cuestión de si las empresas pueden modificar las cláusulas contractuales tipo. La respuesta es negativa. Si se modifican las cláusulas contractuales tipo, éstas pierden el carácter de estándares, y los Estados miembros pueden negarse a reconocer que proporcionen las garantías adecuadas.

Documento disponible en la web:

http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf

ha cumplido la legislación nacional y, en particular, toda regla específica relativa a la obligación de comunicar la información a tenor de la misma.

El considerando 8 de la Decisión 2001/497/CE determina que la misma no cubre la transferencia de datos personales por responsables del tratamiento establecidos en la UE a destinatarios establecidos fuera del territorio de la Unión que actúen solamente como encargados del tratamiento, ya que estas transferencias no exigen las mismas garantías, porque el encargado del tratamiento actúa exclusivamente en nombre del responsable.

El problema que puede surgir en muchas ocasiones es dilucidar si el importador de datos que se encuentra en un país tercero está actuando como responsable o como encargado del tratamiento. Existen multitud de casos en que la frontera de separación entre ambas figuras es muy borrosa. Para clarificar este punto, el Grupo de Trabajo adoptó el 16 de febrero de 2010 el Documento WP 169: Dictamen 1/2010 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento».

En la Decisión se enumeran las garantías para el interesado. Los datos deben tratarse y ser usados o comunicados posteriormente sólo con objetivos precisos, sin que deban conservarse más tiempo del necesario. El interesado debe tener el derecho de acceder a todos los datos que le conciernan y, en lo que proceda, a la rectificación, destrucción o bloqueo de determinados datos. Las posteriores transferencias de datos personales a otros responsables del tratamiento establecidos en un tercer país deben permitirse sólo bajo determinadas condiciones, a fin, en particular, de garantizar que se facilite a los interesados información correcta y que tengan éstos la posibilidad de formular objeciones o, en determinados casos, de denegar su consentimiento.

Las cláusulas contractuales tipo deben ser exigibles no solamente por las organizaciones que sean parte del contrato, sino también por los interesados, en

particular cuando éstos sufran un daño como consecuencia del incumplimiento del contrato. La legislación aplicable al contrato debe ser la que esté en vigor en el Estado miembro en el que se halle establecido el exportador de datos y que permita a un tercer beneficiario exigir el cumplimiento de un contrato. Con objeto de reducir las dificultades prácticas que pudieran experimentar los interesados al intentar exigir el respeto de sus derechos a tenor de estas cláusulas contractuales tipo, el exportador de datos y el importador de datos se considerarán responsables solidarios de los daños y perjuicios resultantes de un incumplimiento de las estipulaciones sujetas a la cláusula de tercer beneficiario. El interesado tiene derecho a emprender acciones y percibir una indemnización del exportador de datos, del importador de datos o de ambos por daños y perjuicios resultantes de cualquier acción incompatible con las obligaciones estipuladas en las cláusulas contractuales tipo.

Si nos centramos en la estructura de las cláusulas contractuales tipo de la Decisión 2001/497/CE, observamos que se parte en primer lugar de la identificación de las partes que acuerdan las cláusulas contractuales: el exportador de los datos y el importador de los datos.

En la cláusula 1 se establecen las *definiciones* de una serie de términos: datos personales, categorías especiales de datos, tratamiento, responsable del tratamiento, encargado del tratamiento, interesado, autoridad de control, exportador de datos e importador de datos.

En la cláusula 2 sobre *detalles de la transferencia*, se exige que se informe sobre los mismos y, en particular, las categorías de datos personales y la finalidad para la que estos se transfieren. Dicha información se aportará en el formato del *Apéndice 1*, que forma parte integrante de las cláusulas.

La cláusula 3, *cláusula de tercero beneficiario*, informa de todos aquellos apartados sobre los cuales los interesados podrán exigir la ejecución como terceros beneficiarios. También se acuerda que las partes no se opondrán a que los interesados estén representados por una asociación u otras entidades si así lo desean y lo permite el Derecho nacional.

En la cláusula 4, sobre *obligaciones del exportador de datos*, éste acuerda y garantiza que el tratamiento ha sido efectuado con las normas pertinentes del Estado miembro de su establecimiento, que si se incluyen categorías especiales de datos, se ha informado al interesado, o será informado antes de la transferencia, de que sus datos podrían ser transferidos a un tercer país que no proporcione una protección adecuada, que a petición de los interesados les facilitará una copia de las cláusulas, y que responderá en un periodo de tiempo razonable y en la medida posible, a las consultas de la autoridad de control sobre el tratamiento de los datos pertinentes por parte del importador de datos y a cualquier consulta del interesado relativa al tratamiento de sus propios datos personales por parte del importador de datos.

En la cláusula 5, sobre *obligaciones del importador de datos*, éste acuerda y garantiza que:

- No tiene motivos para creer que la legislación que le es aplicable le impida cumplir sus obligaciones a tenor del contrato. En caso de cambios en el futuro en dicha legislación, deberá notificarlos al exportador y a la autoridad de control del establecimiento del anterior, para que puedan tomar las medidas que correspondan (suspensión de la transferencia o rescisión del contrato).

- Tratará los datos personales de acuerdo a los principios establecidos en el *Apéndice 2*[144], o bien, con sujeción a los principios establecidos en el *Apéndice 3*[145], efectuará el tratamiento en todos los demás casos de conformidad con las disposiciones pertinentes de Derecho nacional en el país de establecimiento del exportador de datos, o con las normas correspondientes de toda Decisión de la Comisión de conformidad con el apartado 6 del artículo 25 de la Directiva, donde se haga constar que un tercer país garantiza un nivel de protección adecuado en determinados sectores de actividad, si el importador está establecido en dicho tercer país y no está afectado por dichas normas, en la medida en que éstas, por su naturaleza, sean aplicables en el sector de la transferencia.
- Tratará con diligencia las consultas procedentes del exportador o de los interesados y cooperará con la autoridad de control.
- Se someterá a auditoría a petición del exportador.
- A petición de los interesados, entregará una copia de las cláusulas e indicará la oficina encargada de gestionar las quejas.

En la cláusula 6, sobre *responsabilidad*, las partes acuerdan que los interesados que hayan sufrido daños tendrán derecho a una compensación. Ambas partes serán

---

[144] En el Apéndice 2 se recogen los nueve principios básicos de protección cuyo cumplimiento pudiera considerarse un requisito mínimo para juzgar adecuada la protección, contenidos 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", aprobado por el Grupo de Trabajo el 24 de julio de 1998 -WP 12-.

[145] En el Apéndice 3 los tres únicos principios que se recogen son: limitación de la finalidad, restricciones a la transferencia ulterior y derechos de acceso, rectificación, supresión y bloqueo de los datos.

responsables de forma solidaria, pudiendo los interesados interponer una demanda contra cualquiera de ellas o contra ambas.

En la cláusula 7, sobre *mediación y jurisdicción*, las partes acuerdan que en caso de conflicto con el interesado que no se resuelva de forma amistosa, aceptan someter el conflicto a mediación o a los tribunales del Estado del exportador, a voluntad del interesado.

En la cláusula 8, sobre *cooperación con las autoridades de control*, las partes acuerdan el depósito de una copia del contrato ante la autoridad de control si así lo requiere o es exigido por el Derecho nacional.

En la cláusula 9, sobre *resolución de las cláusulas*, las partes acuerdan que la resolución de las cláusulas no eximirá de su cumplimiento en lo que respecta al tratamiento de los datos transferidos.

En la cláusula 10, sobre *legislación aplicable*, se hace constar el Estado del establecimiento del exportador. Las cláusulas se regirán por la legislación de dicho Estado.

En la cláusula 11, sobre *variación del contrato*, las partes se comprometen a no variar los términos de las cláusulas.

Decisión 2004/915/CE[146]

Las cláusulas contractuales tipo constituyen una herramienta de gran utilidad que permite transferir datos personales desde todos los Estados miembros con arreglo a un conjunto de normas comunes. En este sentido, la Decisión 2001/497/CE de la Comisión,

[146] DOUE L 385 de 29 de diciembre de 2004.

de 15 de junio de 2001, establece un conjunto de cláusulas contractuales tipo que prevé garantías adecuadas para la transferencia de datos a terceros países.

Desde la adopción de dicha Decisión se había adquirido una rica experiencia. Además, un consorcio de asociaciones empresariales presentó un conjunto alternativo de cláusulas contractuales tipo, pensado para ofrecer un nivel de protección de datos equivalente al proporcionado por el conjunto de cláusulas adoptado por la Decisión 2001/497/CE, aunque utilizando mecanismos diferentes. Las cláusulas contractuales tipo propuestas por las asociaciones empresariales potenciaban el uso de cláusulas contractuales entre los operadores, por ejemplo flexibilizando los requisitos en materia de auditoría o precisando las normas que regulan el derecho de acceso.

El conjunto alternativo de cláusulas contiene, como alternativa al sistema de responsabilidad solidaria previsto en la Decisión 2001/497/CE, un régimen de responsabilidad basado en la obligación de diligencia debida, en virtud del cual el exportador y el importador de datos responderían ante los interesados por el incumplimiento de sus obligaciones contractuales respectivas. El exportador es asimismo responsable si no realiza esfuerzos razonables para determinar si el importador es capaz de cumplir las obligaciones jurídicas que le incumben en virtud de las cláusulas (*culpa in eligendo*), pudiendo el interesado emprender acciones contra el exportador de datos a este respecto.

En cuanto al ejercicio de los derechos de tercero beneficiario por parte de los interesados, se prevé una mayor intervención del exportador de datos en la resolución de las reclamaciones de los interesados.

A fin de evitar los abusos a que pudiera dar lugar esta mayor flexibilidad del conjunto alternativo de cláusulas, se reconoce a las autoridades de protección de datos la

facultad de prohibir o suspender más fácilmente las transferencias de datos cuando el exportador de datos rehúse tomar medidas apropiadas contra el importador de datos para hacerle cumplir las obligaciones contractuales o este último se niegue a cooperar de buena fe con las autoridades de control competentes en materia de protección de datos.

Los responsables del tratamiento podrán optar por uno de los conjuntos (el antiguo de la Decisión 2001/497/CE o bien el conjunto alternativo de cláusulas). Sin embargo, no podrán modificar las cláusulas ni combinar elementos de distintas cláusulas ni los conjuntos.

Si nos centramos en el conjunto alternativo de cláusulas contractuales tipo de la Decisión 2004/915/CE, observamos que se parte en primer lugar de la identificación de las partes que acuerdan las cláusulas contractuales: el exportador de los datos y el importador de los datos. Seguidamente se establecen las *definiciones* de una serie de términos: datos personales, categorías especiales de datos/datos sensibles, tratar/tratamiento, responsable del tratamiento, encargado del tratamiento, interesado, autoridad de control/autoridad, exportador de datos, importador de datos y cláusulas.

Los detalles de la transferencia (así como los datos personales transferidos) se especifican en el anexo B, que forma parte integrante de las cláusulas.

En la cláusula I, sobre *obligaciones del exportador de datos*, éste acuerda y garantiza que:

- La recopilación, el tratamiento y la transferencia de los datos personales se han efectuado de conformidad con la legislación aplicable al exportador de datos.
- Ha realizado esfuerzos razonables para determinar si el importador de datos es capaz de cumplir las obligaciones jurídicas que le incumben.

- Facilitará al importador de datos copias de las leyes pertinentes en materia de protección de datos del país en que esté establecido.
- Responderá en un período de tiempo razonable a las consultas de los interesados y de la autoridad relativas al tratamiento de los datos personales por parte del importador de datos, a menos que las partes hayan acordado que sea el importador quien responda a estas consultas.
- Pondrá a disposición de los interesados una copia de las cláusulas, a menos que éstas contengan información confidencial, en cuyo caso podrá suprimir dicha información.

En la cláusula II, sobre *obligaciones del importador de datos*, éste acuerda y garantiza que:

- Habrá puesto en práctica las medidas técnicas y organizativas que resulten necesarias para proteger los datos, y que garanticen el nivel de seguridad apropiado.
- Habrá puesto a punto procedimientos que garanticen que cualquier tercero al que dé acceso a los datos personales, incluidos los encargados del tratamiento, respetarán y preservarán la confidencialidad y seguridad de los datos personales. Ninguna persona que actúe bajo la autoridad del importador de datos deberá tratar los datos personales a menos que reciba instrucciones del importador.
- No tiene motivos para creer, en el momento de suscribir las presentes cláusulas, en la existencia de ninguna disposición legal de ámbito local que pueda tener un efecto negativo importante sobre las garantías estipuladas. E informará al exportador de datos si tuviera conocimiento de la existencia de alguna disposición de esta índole.

- Tratará los datos personales para los fines descritos en el contrato.
- Comunicará al exportador de datos un punto de contacto dentro de su organización autorizado a responder a las consultas que guarden relación con el tratamiento. Cooperará de buena fe con el exportador, el interesado y la autoridad respecto de tales consultas dentro de un período de tiempo razonable.
- Facilitará al exportador pruebas que demuestren que dispone de suficientes recursos financieros para cumplir las responsabilidades que le incumben.
- Pondrá a disposición del exportador sus instalaciones de tratamiento de datos, sus ficheros y toda la documentación necesaria, a efectos de revisión, auditoría o certificación.
- Tratará los datos personales, a su discreción, de conformidad con la legislación en materia de protección de datos del país en que esté establecido el exportador de datos o con las disposiciones pertinentes de cualquier decisión de la Comisión adoptada de conformidad con el apartado 6 del artículo 25 de la Directiva 95/46/CE, cuando el importador de datos cumpla las disposiciones pertinentes de dicha autorización o decisión y esté establecido en un país en el que una u otra sean aplicables, pero él mismo no esté cubierto por las mismas a efectos de la transferencia o transferencias de datos personales, o con los principios relativos al tratamiento de datos recogidos en el anexo A[147].

[147] El Anexo A se recogen ocho de los nueve principios básicos de protección cuyo cumplimiento pudiera considerarse un requisito mínimo para juzgar adecuada la protección, contenidos 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", aprobado por el Grupo de Trabajo el 24 de julio de 1998 -WP 12-. El principio que no queda recogido es el de restricciones a la transferencia ulterior, que ya se encuentra en las cláusulas obligatorias.

- No revelará ni transferirá datos personales a terceros responsables del tratamiento establecidos fuera del Espacio Económico Europeo a menos que notifique la transferencia al exportador de datos y
  a) el tercero responsable del tratamiento someta los datos a tratamiento de conformidad con una decisión de la Comisión en la que se haga constar que un tercer país ofrece la protección adecuada,
  b) el tercero responsable del tratamiento suscriba las presentes cláusulas o cualquier otro acuerdo de transferencia de datos aprobado por una autoridad competente en la Unión Europea,
  c) se haya brindado a los interesados, tras haber sido informados de los fines de la transferencia, de las categorías de destinatarios y del hecho de que los países a los cuales se exportan los datos podrían tener una normativa diferente en materia de protección de datos, la oportunidad de formular objeciones, o
  d) por lo que respecta a las transferencias ulteriores de datos sensibles, los interesados hayan dado su consentimiento inequívoco.

Cláusula III, sobre *responsabilidad y derechos de terceros*. Cada una de las partes será responsable ante la otra por los daños que le hubiese provocado como resultado del incumplimiento de las cláusulas. Asimismo, cada una de las partes deberá responder ante los interesados por los daños que le hubiese provocado como resultado de la conculcación de los derechos de terceros reconocidos en las cláusulas. Los interesados podrán invocar, frente al importador o el exportador de datos, varias de las cláusulas del contrato por incumplimiento de sus obligaciones contractuales respectivas. Importador y exportador se someten a la jurisdicción del país de establecimiento del exportador de datos. Los interesados podrán proceder contra el exportador de datos cuando éste no

haya realizado esfuerzos razonables para determinar si el importador de datos es capaz de cumplir las obligaciones jurídicas que le incumben.

Cláusula IV, sobre *legislación aplicable*. La normativa aplicable será la del país en que esté establecido el exportador de datos[148].

Cláusula V, sobre *resolución de conflictos con los interesados o con la autoridad.* En caso de conflicto o de reclamación por un interesado o por la autoridad, ambas partes cooperarán con objeto de alcanzar una solución amistosa. Asimismo acuerdan responder a cualquier procedimiento de mediación no vinculante y de acceso no restringido que haya sido iniciado por un interesado o por la autoridad. Por otra parte, se comprometen a acatar cualquier decisión de los tribunales competentes o de la autoridad del país de establecimiento del exportador de datos cuyas decisiones sean finales y contra la que no pueda entablarse recurso alguno.

Cláusula VI, sobre *resolución de las cláusulas.* En caso de que el importador de datos incumpla sus obligaciones, el exportador podrá suspender temporalmente la transferencia hasta que se subsane el incumplimiento o se resuelva el contrato. Incluso, en el caso de que se den unos requisitos tasados, tanto el exportador de datos como el importador podrán resolver las cláusulas[149]. Las partes acuerdan que la resolución de las cláusulas, por regla general, no las eximirá del cumplimiento de las obligaciones y condiciones estipuladas en las mismas.

[148] A excepción de las disposiciones relativas al tratamiento de datos personales por parte del importador de datos con arreglo a la letra h) de la cláusula II.

[149] Véanse dichos requisitos en la cláusula VI de la Decisión de la Comisión 2004/915/CE.

En la cláusula VII, sobre *variaciones de las cláusulas*, las partes se comprometen a no modificar las cláusulas a no ser para actualizar parte de la información contenida en el anexo B.

Cláusula VII, sobre *descripción de la transferencia*. Los detalles de la transferencia y de los datos personales se especifican en el anexo B. Las partes acuerdan que dicho anexo podrá contener información empresarial de carácter confidencial que, en principio, no revelarán a terceros.

1.1.2. La Decisión 2010/87/UE[150]

La Decisión de la Comisión de 5 de febrero de 2010 viene a regular las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento[151]. Dicha Decisión debe entenderse sin perjuicio de las autorizaciones nacionales que puedan conceder los Estados miembros de conformidad con las disposiciones nacionales de aplicación del artículo 26, apartado 2, de la Directiva 95/46/CE. La Decisión tendrá como efecto únicamente exigir a los Estados miembros que no se nieguen a reconocer que las cláusulas contractuales tipo establecidas en ella

[150] DOUE L 39 de 12 de febrero de 2010.

[151] Como se indica en el documento de la Comisión IP/10/130, emitido en Bruselas el 5 de febrero de 2010 y titulado "*Des normes plus strictes pour les transferts de données à caractère personnel de citoyens européens vers des sous-traitants établis dans des pays tiers*", el vicepresidente de la Comisión Europea, Jacques Barrot, declaró con respecto de las nuevas cláusulas contractuales tipo: "*Cette version mise à jour des clauses contractuelles types tient compte des nouveaux modèles commerciaux et de la progression constante du traitement et de l'externalisation à l'échelle mondiale. Les clauses contractuelles types actualisées garantissent un équilibre entre les besoins des entreprises au niveau international et la protection des données à caractère personnel des citoyens de l'UE"*.

proporcionan las garantías adecuadas, por lo que no afectará de ninguna manera a otras cláusulas contractuales.

Anteriormente a la Decisión 2010/87/UE ya existía la Decisión 2002/16/CE de la Comisión, de 27 de diciembre de 2001, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países. La anterior Decisión se adoptó para facilitar la transferencia de datos personales de un responsable del tratamiento de datos establecido en la Unión Europea a un encargado del tratamiento de datos establecido en un tercer país que no ofrezca el nivel adecuado de protección. Sin embargo, la Decisión 2002/16/CE necesitaba una actualización que abordase entre otros temas, algunos problemas que no fueron regulados por dicha Decisión[152].

La Decisión 2010/87/UE contiene cláusulas contractuales tipo específicas para la subcontratación por un encargado del tratamiento de datos establecido en un tercer país (el importador de datos) de sus servicios de tratamiento a otros encargados (subencargados del tratamiento de datos) establecidos en terceros países. Además establece las condiciones que ha de cumplir el subtratamiento para garantizar que los datos personales que se están transfiriendo sigan protegidos con independencia de la sucesiva transferencia a un subencargado del tratamiento.

El subtratamiento no podrá exceder de las operaciones acordadas en el contrato entre el exportador de datos y el importador de datos. No se referirá a operaciones de

[152] Había propuestas de actualización por parte de las siguientes partes interesadas: Cámara Internacional de Comercio (ICC), Japan Business Council in Europe (JBCE), EU Committee of the American Chamber of Commerce in Belgium (Amcham) y Federation of European Direct Marketing Associations (FEDMA).

tratamiento o finalidades diferentes para respetar así el principio de limitación de la finalidad establecido en la Directiva 95/46/CE. Además, si el subencargado del tratamiento de datos no cumple sus propias obligaciones de tratamiento de datos, el importador de datos seguirá siendo responsable frente al exportador de datos. La transferencia de datos personales a encargados del tratamiento establecidos fuera de la Unión Europea se hará sin perjuicio de que las actividades de tratamiento se rijan por la legislación de protección de datos aplicable.

Las cláusulas contractuales tipo serán exigibles no solamente por las organizaciones que sean parte en el contrato, sino también por los interesados, en particular cuando estos sufran un daño como consecuencia del incumplimiento del contrato. El interesado tendrá derecho a emprender acciones y, en su caso, percibir una indemnización del exportador de datos que sea el responsable del tratamiento de los datos personales transferidos. Excepcionalmente, bajo ciertas condiciones, también tendrá derecho a emprender una acción y, en su caso, percibir una indemnización del importador de datos o del subencargado del tratamiento de datos. El contrato se regirá por la legislación del Estado miembro de establecimiento del exportador de datos.

La Decisión 2010/87/UE solo se aplica a la subcontratación por un encargado del tratamiento establecido en un tercer país, de sus servicios de tratamiento a un subencargado establecido en un tercer país, por lo que no se aplicará a la situación en la que un encargado del tratamiento establecido en la Unión Europea y que realice el tratamiento de datos personales en nombre de un responsable del tratamiento establecido en la Unión Europea subcontrate sus operaciones de tratamiento a un subencargado del tratamiento establecido en un tercer país.

La Decisión 2010/87/UE se aplica desde el 15 de mayo de 2010, quedando derogada la Decisión 2002/16/CE con efectos a partir de la misma fecha.

Los contratos concluidos entre un exportador de datos y un importador de datos de conformidad con la Decisión 2002/16/CE antes del 15 de mayo de 2010 seguirán en vigor y producirán todos sus efectos jurídicos mientras permanezcan sin cambios las transferencias y operaciones de tratamiento de datos que son objeto del contrato. Si las partes contratantes deciden realizar cambios a este respecto o subcontratar las operaciones de tratamiento que son objeto del contrato, estarán obligadas a concluir un nuevo contrato que cumpla las cláusulas contractuales tipo establecidas en la nueva Decisión.

Si nos centramos en el conjunto de cláusulas contractuales tipo de la Decisión 2010/87/UE, observamos que se encabezan con la identificación de las partes que acuerdan las cláusulas contractuales: el exportador de los datos y el importador de los datos. El exportador de datos transferirá al importador de datos los datos personales especificados en el apéndice 1[153].

En la cláusula 1, sobre *definiciones*, se definen una serie de términos: datos personales, categorías especiales de datos, tratamiento, responsable del tratamiento, encargado del tratamiento, interesado, autoridad de control, exportador de datos, importador de datos, subercargado del tratamiento, legislación de protección de datos aplicable y medidas de seguridad técnicas y organizativas.

[153] En el apéndice 1 se especifican las actividades del exportador y del importador correspondientes a la transferencia, las categorías de interesados, las categorías de datos y las categorías especiales de datos a los que se refieren los datos personales transferidos, así como las operaciones básicas de tratamiento a las que serán sometidos los datos personales.

En la cláusula 2, sobre *detalles de la transferencia*, se indica que los mismos quedan especificados en el apéndice 1.

Cláusula 3, *de tercero beneficiario*. El interesado podrá exigir al exportador de datos, y en determinadas circunstancias al importador de datos y al subencargado del tratamiento, el cumplimiento de determinadas partes del contrato como tercer beneficiario. Las partes no se oponen a que los interesados estén representados por una asociación u otras entidades, si así lo desean expresamente y lo permite el Derecho nacional.

En la cláusula 4, sobre *obligaciones del exportador de datos*, éste acuerda y garantiza lo siguiente:

- El tratamiento de datos ha sido, y será, efectuado de conformidad con la legislación aplicable.
- Ha dado, y dará, al importador de datos, instrucciones para que el tratamiento que efectúa se lleve a cabo en nombre del exportador de datos, y de conformidad con la ley aplicable y con las cláusulas.
- El importador ofrecerá garantías suficientes en cuanto a medidas de seguridad técnicas y organizativas.
- Ha verificado que dichas medidas sean apropiadas para proteger los datos personales y que garantizan un nivel de seguridad apropiado.
- Asegurará que dichas medidas se lleven a la práctica.
- Si la transferencia incluye categorías especiales de datos, se habrá informado de dicha transferencia a los interesados, o serán informados antes de que se produzca aquella.

- Pondrá a disposición de los interesados una copia de las cláusulas y una descripción de las medidas de seguridad.

- En caso de subtratamiento, el subencargado proporcionará por lo menos el mismo nivel que el importador.

En la cláusula 5, sobre *obligaciones del importador de datos*, el importador de datos acuerda y garantiza que:

- Tratará los datos transferidos solo en nombre del exportador de datos, de conformidad con sus instrucciones y las cláusulas.

- No tiene motivos para creer que la legislación que le es de aplicación le impida cumplir las instrucciones del exportador de datos y sus obligaciones a tenor del contrato. En caso de modificación de la legislación notificará al exportador de datos dicho cambio.

- Ha puesto en práctica las medidas de seguridad técnicas y organizativas que se indican en el apéndice 2[154] antes de efectuar el tratamiento de los datos personales transferidos.

- Notificará al exportador de datos sobre toda solicitud jurídicamente vinculante de divulgar los datos personales, todo acceso accidental o no autorizado, o toda solicitud sin respuesta recibida directamente de los interesados.

- Tratará adecuadamente todas las consultas del exportador de datos y se atendrá a la opinión de la autoridad de control en lo que respecta al tratamiento de los datos transferidos.

[154] En el apéndice 2 se efectúa la descripción de las medidas de seguridad técnicas y organizativas puestas en marcha por el importador de datos.

- Ofrecerá a petición del exportador de datos sus instalaciones de tratamiento de datos para que se lleve a cabo la auditoría de las actividades de tratamiento cubiertas por las cláusulas.

- Pondrá a disposición de los interesados una copia de las cláusulas, o de cualquier contrato existente para el subtratamiento de los datos.

- En caso de subtratamiento de los datos, habrá informado previamente al exportador de datos y obtenido previamente su consentimiento por escrito.

- Los servicios de tratamiento por el subencargado del tratamiento se llevarán a cabo de conformidad con la cláusula 11.

- Enviará sin demora al exportador de datos una copia de cualquier acuerdo con el subencargado del tratamiento que concluya con arreglo a las cláusulas.

En la cláusula 6, sobre *responsabilidad*, las partes acuerdan que los interesados que hayan sufrido daños como resultado del incumplimiento de las obligaciones mencionadas en la cláusula 3 o en la cláusula 11 por cualquier parte, o por el subencargado del tratamiento, tendrán derecho a percibir una indemnización del exportador de datos por el daño sufrido. En casos determinados, el importador o el subencargado aceptan que el interesado pueda demandarles a ellos en lugar de al exportador.

En la cláusula 7, sobre *mediación y jurisdicción*, el importador de datos acuerda que, si el interesado invoca en su contra derechos de tercero beneficiario o reclama una indemnización por daños y perjuicios, aceptará la decisión del interesado de someter el conflicto a mediación o a los tribunales del Estado miembro de establecimiento del exportador de datos.

Cláusula 8, de *cooperación con las autoridades de control*. El exportador de datos acuerda depositar una copia del contrato ante la autoridad de control si así lo requiere o si el depósito es exigido por la legislación de protección de datos aplicable. Las partes acuerdan que la autoridad de control está facultada para auditar al importador, o a cualquier subencargado. El importador de datos informará sin demora al exportador de datos en el caso de que la legislación existente aplicable a él o a cualquier subencargado no permita auditarles.

En la cláusula 9, sobre *legislación aplicable*, deberá indicarse la legislación del Estado (de establecimiento del exportador de datos) que regirá las cláusulas.

En la cláusula 10, sobre *variación del contrato*, las partes se comprometen a no variar o modificar las cláusulas contractuales tipo.

Cláusula 11, sobre *subtratamiento de datos*. El importador de datos no subcontratará ninguna de sus operaciones de procesamiento llevadas a cabo en nombre del exportador de datos sin previo consentimiento por escrito del exportador de datos. Si el importador de datos subcontrata sus obligaciones, lo hará exclusivamente mediante un acuerdo escrito con el subencargado del tratamiento de datos, en el que se le impongan a éste las mismas obligaciones impuestas al importador de datos con arreglo a las cláusulas. En los casos en que el subencargado del tratamiento de datos no pueda cumplir sus obligaciones de protección de los datos con arreglo a dicho acuerdo escrito, el importador de datos seguirá siendo plenamente responsable frente al exportador del cumplimiento de las obligaciones del subencargado del tratamiento.

El contrato escrito previo entre el importador de datos y el subencargado del tratamiento contendrá asimismo una cláusula de tercero beneficiario, tal como se establece en la cláusula 3, para los casos en que el interesado no pueda interponer la demanda contra el exportador de datos o el importador de datos.

Cláusula 12, sobre *obligaciones una vez finalizada la prestación de los servicios de tratamiento de los datos personales.* Las partes acuerdan que, una vez finalizada la prestación de los servicios de tratamiento de los datos personales, el importador y el subencargado deberán, a discreción del exportador, o bien devolver todos los datos personales transferidos y sus copias, o bien destruirlos por completo y certificar esta circunstancia al exportador. El importador de datos y el subencargado garantizan que, a petición del exportador o de la autoridad de control, pondrá a disposición sus instalaciones de tratamiento de los datos para que se lleve a cabo una auditoría de las medidas de seguridad técnicas y organizativas.

Documento WP 176 del Grupo de Trabajo

A efecto de aclarar el contenido de la Decisión 2010/87/UE, el Grupo de Trabajo sobre protección de datos adoptó el 12 de julio de 2010 el documento "Lista de las preguntas más frecuentes planteadas por la entrada en vigor de la Decisión 2010/87/UE de la Comisión de 5 de febrero de 2010, relativa a las cláusulas contractuales tipo para la transferencia de datos de carácter personal a subcontratistas establecidos en terceros países en virtud de la Directiva 95/46/CE del Parlamento Europeo y del Consejo".

Entre las cuestiones tratadas resaltan por su interés las dos siguientes:

- ¿Las cláusulas de la Decisión 2010/87/UE se aplican en el caso de transferencias de datos de un responsable del tratamiento establecido en el EEE hacia un encargado del tratamiento establecido en el EEE y luego a un subencargado del tratamiento establecido fuera del EEE? No. La Decisión solo se aplica a la subcontratación por un encargado del tratamiento establecido en un tercer país de sus servicios de tratamiento a un subencargado establecido en un tercer país.

- En el mismo caso de la pregunta anterior ¿Cómo encuadrar jurídicamente las transferencias de datos de un responsable del tratamiento establecido en el EEE hacia un encargado del tratamiento establecido en el EEE y luego a un subencargado del tratamiento establecido fuera del EEE? Mientras no se adopte ningún instrumento específico para este caso, el Grupo de Trabajo encuentra tres posibles soluciones:

a) Un contrato directo entre el responsable del tratamiento y el subencargado del tratamiento establecido fuera del EEE, conforme a la Decisión 2010/87/UE.

b) Un mandato expreso por el cual el responsable da al encargado del tratamiento establecido en el EEE el poder de utilizar las cláusulas tipo de la Decisión 2010/87/UE por su cuenta.

c) Un contrato *ad hoc*. Tal como se indica en el Considerando 23 de la Decisión 2010/87/UE, "en tales situaciones, los Estados miembros son libres de tener en cuenta el hecho de que los principios y las garantías de las cláusulas contractuales tipo establecidas en la presente Decisión se hayan utilizado para subcontratar a un subencargado establecido en un tercer país con la intención de prestar la adecuada protección de los derechos de aquellos interesados cuyos datos personales se estén transfiriendo para operaciones de subtratamiento".

Nuevo modelo de cláusulas contractuales de la AEPD: Encargado a Subencargado

La postura que venía manteniendo la AEPD en el caso de la subcontratación de un encargado establecido en España a un subencargado radicado en un tercer país que no ofrece un nivel adecuado de protección, la encontramos en el Informe de la Agencia 582/2004[155]. En dicho Informe se señala que los supuestos planteados en la Instrucción 1/2000 únicamente se refieren a aquellos casos en que la transferencia sea realizada por un responsable del tratamiento, bien a otro responsable, bien a un encargado. Del mismo modo, la Comisión Europea únicamente ha adoptado Decisiones en las que una parte del contrato sea el responsable del tratamiento, efectuándose la transferencia bien a un responsable (Decisiones 2001/497/CE y 2004/915/CE), bien a un encargado del tratamiento (Decisión 2002/16/CE). Si nos centramos en este caso, "la transferencia amparada en las cláusulas contenidas en la Decisión 2002/16/CE únicamente es posible en caso de que el contrato sea celebrado entre el responsable del tratamiento y el encargado ubicado en el tercer estado que no ofrezca un nivel adecuado de protección, de modo que no será posible en ningún caso que el mismo sea suscrito por dos encargados del tratamiento, ya que el encargado exportador no podría asumir las obligaciones estipuladas en el contrato sin convertirse en responsable, lo que implicaría la existencia de una previa cesión de datos al mismo, que habría de resultar conforme a lo dispuesto en el artículo 11 de la Ley Orgánica 15/1999 y desnaturalizaría la posición del propio encargado". Para que la transferencia pueda considerarse conforme a lo

[155] "Subcontratación de un encargado del tratamiento en tercer país que no ofrece nivel adecuado de protección. Necesidad de intervención del responsable. Informe 582/2004". Disponible en la web de la AEPD.

dispuesto en la LOPD, es necesario que, en las cláusulas contractuales que se firmen, el responsable del tratamiento tenga la condición de exportador, a los efectos previstos en la Decisión 2002/16/CE.

Esta postura ha cambiado en fecha muy reciente. La AEPD ha elaborado a primeros de 2012 un nuevo conjunto de cláusulas contractuales[156] aplicables a contratos de subcontratación de servicios entre encargados establecidos en España y subencargados radicados en terceros países[157]. Estas cláusulas contractuales se basan en el contenido del Considerando 23[158] de la Decisión 2010/87/UE, que otorga a las autoridades nacionales en materia de protección de datos, la posibilidad de dar mayor flexibilidad en la subcontratación que puedan llevar a cabo encargados nacionales con subencargados que operan en terceros países.

---

[156] Estas cláusulas contractuales (encargados a subencargados de tratamiento) están disponibles en la página electrónica de la AEPD.

[157] Véase el documento "El régimen de transferencias internacionales de datos a encargados de tratamiento" elaborado por la señora María José Blanco Antón, Subdirectora General del Registro General de Protección de Datos, para para la "Cuarta sesión anual abierta de la AEPD", celebrada en Madrid el 27 de enero de 2012.

[158] Según el Considerando 23 de la Decisión 2010/87/UE, dicha Decisión solo se aplica a la subcontratación por un encargado del tratamiento establecido en un tercer país de sus servicios de tratamiento a un subencargado establecido en un tercer país, por lo que no se aplicará a la situación en la que un encargado del tratamiento establecido en la Unión Europea y que realice el tratamiento de datos personales en nombre de un responsable del tratamiento establecido en la Unión Europea subcontrate sus operaciones de tratamiento a un subencargado del tratamiento establecido en un tercer país. En tales situaciones, los Estados miembros son libres de tener en cuenta el hecho de que los principios y las garantías de las cláusulas contractuales tipo establecidas en la Decisión 2010/87/UE se hayan utilizado para subcontratar a un subencargado establecido en un tercer país con la intención de prestar la adecuada protección de los derechos de aquellos interesados cuyos datos personales se estén transfiriendo para operaciones de subtratamiento.

El nuevo conjunto de cláusulas contractuales prevé que el solicitante de la autorización de la transferencia internacional sea el encargado del tratamiento (y no el responsable del tratamiento, como se venía exigiendo hasta la fecha). Dicha solicitud de transferencia se inspira en la Cláusula 11[159] de la Decisión 2010/87/UE, sobre subtratamiento de datos.

Bajo el nuevo modelo de cláusulas contractuales, el responsable deberá autorizar previamente al encargado la posterior subcontratación a un subencargado importador y, si es el caso, a posteriores subencargados. El contrato marco responsable-encargado (regulado en el artículo 12 de la LOPD y en los artículos 20 a 22 del RLOPD), deberá dar garantías por parte del responsable y del encargado de que los tratamientos de datos han sido efectuados y seguirán efectuándose de conformidad con la LOPD. En el contrato deberán constar las autorizaciones a la subcontratación y a las transferencias internacionales de datos, debiendo identificarse los ficheros y la notificación al Registro General de Protección de Datos.

El encargado de tratamiento en todo momento deberá tener a disposición de la AEPD, por una parte, la relación de responsables a los que presta servicios, y por otra,

[159] Según el punto 1 de la Cláusula 11 de la Decisión, el importador de datos no subcontratará ninguna de sus operaciones de procesamiento llevadas a cabo en nombre del exportador de datos con arreglo a las cláusulas sin previo consentimiento por escrito del exportador de datos. Si el importador de datos subcontrata sus obligaciones con arreglo a las cláusulas, con el consentimiento del exportador de datos, lo hará exclusivamente mediante un acuerdo escrito con el subencargado del tratamiento de datos, en el que se le impongan a éste las mismas obligaciones impuestas al importador de datos con arreglo a las cláusulas. En los casos en que el subencargado del tratamiento de datos no pueda cumplir sus obligaciones de protección de los datos con arreglo a dicho acuerdo escrito, el importador de datos seguirá siendo plenamente responsable frente al exportador de datos del cumplimiento de las obligaciones del subencargado del tratamiento de datos con arreglo a dicho acuerdo.

la relación de importadores y de subencargados ulteriores que intervengan en el tratamiento. En el contrato se describirán los servicios prestados por el subencargado, la descripción de finalidades y categorías de datos objeto de tratamiento así como la descripción de las medidas de seguridad que va a aplicar el subencargado.

En un primer momento el modelo de cláusulas contractuales se mantuvo en secreto por parte de la AEPD. Solo se facilitaría por parte de la Agencia a aquellas entidades que tuvieran un interés real en emplearlas para sus transferencias internacionales de datos. Esta postura ha cambiado completamente a partir de la solicitud de autorización para la transferencia internacional de datos efectuada a 16 de julio de 2012 por una empresa en calidad de encargada del tratamiento[160]. En la Resolución de Autorización de transferencias internacionales de datos correspondiente a esta solicitud de autorización, la AEPD ha añadido como anexo el nuevo conjunto de cláusulas contractuales. El punto de partida del nuevo modelo contractual se encuentra, como ya se había indicado anteriormente, en la Decisión 2010/87/UE. De este modo, las nuevas cláusulas contractuales incluyen:

- Cláusula de tercero beneficiario para hacer exigible el clausulado por el interesado, aun no siendo parte, cuando sufra un daño como consecuencia del incumplimiento del contrato.
- Obligaciones del exportador.
- Obligaciones del importador.

[160] Véase el número de Expediente TI/00126/2012 en la página de la AEPD, así como la publicación oficial del "Acuerdo de Apertura del Período de Información Pública" en el BOE de 20-09-2012.

- Cláusula de responsabilidad por la que el interesado tiene derecho a emprender acciones y percibir una indemnización del exportador y/o del importador de datos por daños y perjuicios resultantes de cualquier acción incompatible con las obligaciones estipuladas en las cláusulas.
- Mediación y arbitraje en caso de conflicto entre las partes y el interesado que no se resuelva de manera amistosa.
- Cooperación con las autoridades de control, en este caso la Agencia Española de Protección de Datos.
- Legislación aplicable, en este caso la española.
- Compromiso de las partes de no variar o modificar los términos de las cláusulas.
- Subtratamiento de datos, que necesita el consentimiento por escrito del exportador y del responsable del tratamiento.
- Obligaciones una vez finalizada la prestación de los servicios de tratamiento de datos personales.

También incluye el contrato, en el apéndice 1, la información relativa al exportador e importador de datos, los colectivos a los que se refieren los datos de carácter personal a transferir, sus categorías, incluyendo los datos especialmente protegidos, y las operaciones básicas de tratamiento, así como, en el apéndice 2, las medidas de seguridad, técnicas y organizativas, que ha de poner en práctica el importador de datos antes de efectuar el tratamiento de los datos personales transferidos.

Es decir, el contrato viene a estipular un clausulado similar al de la citada Decisión 2010/87/UE. No obstante, como no puede ser de otro modo, dicho clausulado no puede ser idéntico al de dicha Decisión, tanto por la naturaleza de las partes intervinientes

como por la necesaria relación que el contrato de transferencia internacional debe guardar con el contrato marco firmado por el exportador con el responsable del tratamiento. Así por ejemplo, se incluyen una serie de obligaciones del exportador de datos, adicionales a las establecidas en la Decisión 2010/87/UE. Se contienen en las letras i) a n) de las cláusula 4.2, de forma que el exportador:

"i) mantendrá una lista actualizada de los responsables del tratamiento y ficheros a cuyos datos se refiera la transferencia, que pondrá a disposición de la Agencia Española de Protección de Datos y notificará cualquier modificación en la misma;

j) comunicará al responsable del tratamiento cualquier acuerdo que el importador de datos pretenda concluir al amparo de la cláusula 11 para obtener su autorización;

k) enviará, sin demora, al responsable del tratamiento una copia de cualquier acuerdo del importador de datos con el subencargado ulterior del tratamiento que concluya con arreglo a las cláusulas;

l) comunicará, sin demora, al responsable del tratamiento cualquier notificación del importador de datos conforme a la letra d) de la cláusula 5 del presente contrato;

m) promoverá las medidas de auditoría previstas en la letra f) de la cláusula 5 cuando así lo solicite el responsable del tratamiento, dándole traslado en todo caso de los resultados de dichas medidas, así como, en su caso, la identificación del organismo que las hubiera llevado a cabo;

n) comunicará al responsable del tratamiento las medidas que se adopten conforme a la cláusula 12 en relación con el destino final de los datos".

Para concluir, podemos afirmar que cualquier transferencia que se efectúe dentro del marco de una autorización obtenida en base a las nuevas cláusulas contractuales no precisará de una posterior autorización singular del Director de la Agencia Española de Protección de Datos, siempre y cuando:

- Las transferencias internacionales de datos se ajusten a lo establecido en las cláusulas del contrato presentado entre el exportador e importador de los datos, es decir, no afecten nada más que a los colectivos establecidos en el apéndice 1 del contrato de transferencia, y se refieran a las categorías de datos y a las operaciones de tratamiento establecidas en dicho apéndice.
- Se haya suscrito, y pueda ponerse en cualquier momento a disposición de la AEPD el denominado contrato marco entre el responsable del tratamiento y el exportador de datos, incluyendo el contenido y las garantías derivados del marco objeto de la autorización.
- Con anterioridad al comienzo de una transferencia internacional de datos se haya notificado la misma por el responsable del tratamiento, a fin de que se proceda a su inscripción en el RGPD, quedando identificados el fichero o ficheros a cuyos datos se refiera la transferencia internacional, con referencia a la resolución en que se había autorizado la transferencia internacional.

2. REGLAS CORPORATIVAS VINCULANTES (BCR)

La transferencia internacional de datos a países terceros que no proporcionan un nivel adecuado de protección en materia de protección de datos ha sido un problema para las empresas multinacionales desde la aprobación de la Directiva 95/46/CE. Como señala Valverde López, “el marco legislativo de la protección de datos de carácter

personal ha causado importantes quebraderos de cabeza a las empresas privadas, principalmente multinacionales con representación en diferentes países dentro y fuera de la Unión Europea, para encontrar soluciones innovadoras que pudieran conjugar el correcto cumplimiento de la normativa en materia de protección de datos con sus necesidades comerciales"[161]. Una de esas soluciones innovadoras ha sido la aparición de las reglas corporativas vinculantes. La Comisión Europea las entiende como "los códigos de buenas prácticas basados en las normas de protección de datos europeas y aprobados al menos por una autoridad de control de la protección de datos, que las entidades elaboran de manera voluntaria y suscriben a fin de asegurar las salvaguardias necesarias para determinadas categorías de transferencias de datos personales entre empresas que forman parte del mismo grupo de sociedades y están vinculadas por esas normas"[162].

2.1. REGULACIÓN EN EL ÁMBITO DE LA UE

Como señala Álvarez Rigaudias[163], "en 2002, y sobre la base de la experiencia alemana que contemplaba expresamente en su legislación desde 2001 los reglamentos

---

[161] VALVERDE LÓPEZ, M: *Las Reglas Corporativas Vinculantes (Binding Corporate Rules) en materia de protección de datos*. 2009, pág. 3. Documento disponible en varias direcciones electrónicas, entre las cuales está la siguiente: **http://www.scribd.com/full/52311596?access_key=key-1i6r2esa8i5og7zl0ta9**

[162] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. *La protección de la privacidad en un mundo interconectado. Un marco europeo de protección de datos para el siglo XXI*. Bruselas, 25.01.2012, COM(2012) 9 final. Pág. 12.

[163] ÁLVAREZ RIGAUDÍAS, C. y otros: *Comentario al Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (aprobado por RD 1720/2007, de 21 de diciembre)*. Aranzadi. Pamplona 2008, pág. 533.

corporativos obligatorios, las autoridades de control en materia de protección de datos de Austria, Holanda y de Alemania valoraron por primera vez la posibilidad de coordinar los procedimientos de homologación referidos a los reglamentos corporativos, identificando unos criterios que habrían de servir de punto de referencia a una autoridad encargada de la coordinación en Europa". Las conclusiones a las que se llegó en esta reunión se trasladaron al Documento WP 74 del Grupo de Trabajo.

Es por ello que para el estudio de las reglas corporativas vinculantes partiremos de dicho Documento de Trabajo, adoptado el tres de junio de 2003[164].

Las autoridades de protección de datos gestionan las solicitudes de transferencia de datos personales a terceros países en virtud del artículo 26.2 de la Directiva. En general, estas peticiones han requerido soluciones contractuales propuestas por las autoridades nacionales a la luz de los principios establecidos en el Documento WP 12 del Grupo de Trabajo y particularmente por las Decisiones de la Comisión sobre cláusulas contractuales tipo.

El uso de soluciones contractuales no es nuevo para las empresas multinacionales, y algunos Estados miembros están estudiando la posibilidad de la ampliación de su uso. Sin embargo, como bien indica Álvarez Rigaudias, "la Directiva ha sido criticada como una seria barrera regulatoria para el comercio internacional, particularmente en el

[164] Documento denominado "Transferts de données personnelles vers des pays tiers: Application de l'article 26 (2) de la directive de l'UE relative à la protection des données aux règles d'entreprise contraignantes applicables aux transferts internationaux de données".

contexto de los grupos multinacionales que tratan de operar bajo unos mismos estándares en todas la jurisdicciones donde están presentes"[165].

Por sus especiales características, y debido a sus ramificaciones internacionales complejas, a algunas empresas multinacionales les gustaría tener la posibilidad de adoptar *códigos de conducta* en relación con las transferencias internacionales. Estos códigos permitirían encuadrar la transferencia internacional de datos personales dentro de un mismo grupo multinacional, bajo la sujeción de la autorización de las autoridades de protección de datos, de conformidad con el artículo 26.2 de la Directiva. De acuerdo con estas empresas multinacionales, la vía de los compromisos unilaterales, con garantías sólidas, debería ser explotada.

Para el Grupo de Trabajo, en tanto los compromisos unilaterales impliquen efectos reales vinculantes en el plano jurídico no hay ninguna razón para excluir esta posibilidad. Sin embargo es importante tener en cuenta que bajo las leyes nacionales de algunos Estados miembros, los compromisos unilaterales no crean obligaciones ni derechos jurídicamente vinculantes[166].

Para el Grupo de Trabajo las *reglas corporativas vinculantes* no deben considerarse como una panacea en el contexto de las transferencias internacionales, sino sólo como

---

[165] ÁLVAREZ RIGAUDIAS, C: "Las transferencias internacionales de datos personales y el nivel equiparable o adecuado de protección". Actualidad Jurídica Uría Menéndez, nº 12 sept-dic 2005.

[166] A nivel nacional, el RLOPD en su artículo 70.4 dispone que la autorización del Director de la Agencia Española de Protección de Datos implicará la exigibilidad de lo previsto en las normas o reglas internas tanto por la Agencia como por los afectados cuyos datos hubieran sido objeto de tratamiento.

un instrumento adicional[167] a usar allí donde los medios existentes parecen particularmente problemáticos[168].

En cuanto al contenido sustancial de las reglas corporativas vinculantes, el Grupo de Trabajo reitera los principios contenidos en el Documento WP 12, especialmente en el capítulo 3 (Aplicación del enfoque a la autorregulación industrial) y en menor medida, en el capítulo 6 (Cuestiones de procedimiento).

Estos principios deben ser desarrollados y detallados en el marco de las reglas corporativas vinculantes con el fin de encajar de una forma práctica y realista en las operaciones de tratamiento efectuadas por la organización en otros países. Los principios deberán ser comprendidos y efectivamente aplicados por los responsables de protección de datos en la organización.

Como indica el artículo 26.2 de la Directiva, la autorización puede incluir una transferencia o un conjunto de transferencias, pero en todos los casos las transferencias autorizadas deben ser definidas. El nivel de detalle debe ser suficiente para permitir a las autoridades de protección de datos la evaluación de la adecuación del tratamiento realizado en el país tercero.

---

[167] A este respecto, se puede consultar un artículo de Leonardo Cervera Navas, Administrador de la Unidad de Protección de Datos en la Dirección General de Mercado Interior de la Comisión Europea, "Primera aproximación a las *Binding Corporate Rules* para la transferencia de datos personales a terceros países". Revista Electrónica Datospersonales.org, nº 4, 2003.

[168] Como indica la CNIL (Commission Nationale de l'Informatique et des Libertés) en un documento descargable de su web: *Les BCR – Binding Corporte Rules ou Regles Internes d'Enterprise*, las reglas corporativas vinculantes constituyen una alternativa a las cláusulas contractuales tipo, ya que permiten asegurar un nivel de protección suficiente a los datos transferidos fuera de la UE. En este sentido también constituyen una alternativa a los principios de Puerto Seguro para las transferencias a Estados Unidos.

Las reglas corporativas vinculantes pueden concretar las reglas aplicables a los diferentes países o regiones fuera de la Unión Europea si este es el deseo del grupo que las implementa. Sin embargo esta particularización hace obviamente el sistema más complejo, mientras que el objetivo de este último es el diseño de las políticas globales.

En cuanto a la actualización de las transferencias efectuadas y, consecuentemente, de las reglas corporativas vinculantes, el Grupo de Trabajo reconoce que los grupos son entidades que mutan. Las filiales y las prácticas pueden cambiar de vez en cuando y, por lo tanto, no se pueden corresponder al 100% con la realidad imperante en el momento de la concesión la autorización. Las actualizaciones son posibles, bajo ciertas condiciones, sin tener que volver a solicitar la autorización.

En cuanto a las garantías de cumplimiento y de puesta en aplicación interna, el Documento de Trabajo indica que, además de los principios sustantivos de protección de datos, todas las reglas corporativas vinculantes aplicables a las transferencias internacionales de datos deben contener también:

- **Disposiciones para garantizar un buen nivel de cumplimiento**

Las reglas han de establecer un sistema que garantice la transparencia y la aplicación de estas normas, tanto dentro como fuera de la Unión Europea.

El mero desarrollo de un grupo de medidas internas para la protección de la privacidad no puede ser considerado sino como un primer paso hacia la presentación de garantías suficientes en el sentido del artículo 26.2 de la Directiva. El grupo solicitante debe ser capaz de demostrar que esta política es conocida, entendida y efectivamente aplicada por los empleados.

El grupo tendrá como objetivo designar el personal necesario, con ayuda de la dirección, para supervisar y asegurar el cumplimiento.

- **Auditorías**

Las reglas deben permitir el control interno y / o externo realizado regularmente por supervisores, quienes transmitirán directamente al órgano de administración de la empresa matriz del grupo. Las autoridades de protección de datos recibirán una copia de estas auditorías.

Las reglas también deben establecer que el deber de cooperar con las autoridades de protección de datos puede requerir auditorías por inspectores de la autoridad de supervisión o por auditores independientes, en nombre de la autoridad supervisora. Este análisis externo puede ser preciso cuando las auditorías previstas en el párrafo anterior no están disponibles por una razón u otra, cuando no contienen la información necesaria para la monitorización normal de la autorización concedida, o cuando la urgencia de la situación requiere la participación directa de la autoridad de protección de datos competente o de controladores independientes en su nombre.

- **Gestión de reclamaciones**

Las normas deben establecer un sistema de gestión de las reclamaciones individuales en un departamento claramente identificado. Los responsables de protección de datos o cualquier otra persona responsable de la tramitación de las reclamaciones deben gozar de un grado apropiado de independencia en el ejercicio de sus funciones. El uso de mecanismos alternativos de resolución de conflictos, con la

posible participación de las autoridades de protección de datos, en su caso, también se debe promover en el cumplimiento de las leyes y reglamentos nacionales aplicables.

- **El deber de cooperación con las autoridades de protección de datos**

Como se señaló en el documento WP 12, uno de los criterios más importantes utilizado para evaluar la adecuación de la protección de un sistema de autorregulación es el grado de apoyo y asistencia que se ofrece a los afectados.

Este es de hecho uno de los elementos más importantes de las reglas corporativas vinculantes aplicable a las transferencias internacionales de datos: las normas deben indicar claramente el deber de cooperar con las autoridades de protección de datos, para que los individuos puedan beneficiarse de un apoyo institucional.

Debe quedar claro que el grupo en su conjunto y cada una de sus entidades por separado seguirán los consejos de la autoridad competente responsable de la protección de datos en todos los asuntos relativos a la interpretación y aplicación de estas reglas corporativas vinculantes.

- **Responsabilidad**

Las reglas estipularán que las personas involucradas se beneficiarán de los derechos de reparación y responsabilidad en virtud de los artículos 22 y 23 de la Directiva (o de disposiciones similares en aplicación de estos artículos de la Directiva en la legislación de los Estados miembros), en las mismas condiciones y en la misma medida que si el tratamiento estuviera realizado por el grupo en el ámbito de la Directiva sobre protección de datos o cualquier legislación nacional de aplicación de la misma.

El propósito de estas reglas se limita a asegurar que los permisos expedidos por las autoridades de protección de datos no hipotecan ningún derecho de los interesados a reparación o indemnización, como habría sido el caso si los datos no hubieran abandonado el territorio de la UE.

Para completar este derecho general, y para facilitar el ejercicio en la práctica, las normas también deben contener disposiciones sobre responsabilidad y jurisdicción.

La casa matriz (si está establecida en la UE) o la compañía europea responsable por delegación de la protección de datos debería asumir la responsabilidad y tomar las medidas necesarias para corregir los actos cometidos por otras entidades del grupo fuera de la Unión Europea y, en su caso, pagar una indemnización por cualquier perjuicio resultante del incumplimiento de las reglas corporativas vinculantes de cualquiera de las subsidiarias obligadas por ellas.

El grupo presentará, junto a la solicitud de aprobación, los documentos que demuestren que la casa matriz europea o la compañía europea responsable por delegación de la protección de datos, disponen de suficientes recursos financieros dentro de la Unión Europea para cubrir el pago de una indemnización por la violación de las reglas corporativas vinculantes en un contexto normal, o que se han tomado medidas para hacer frente a tales reclamaciones (por ejemplo, contratación de un seguro de responsabilidad).

- **Disposiciones en materia de jurisdicción**

El grupo debe aceptar que las personas interesadas tienen derecho a interponer un recurso en su contra y para elegir la jurisdicción:

a) la de la compañía donde está el origen de la transferencia o

b) la de la matriz del grupo o la de la compañía europea responsable por delegación de la protección de datos.

- **Transparencia**

Además de la divulgación de conformidad con los artículos 10 y 11 de la Directiva y de la legislación nacional de transposición, los grupos deben ser capaces de demostrar que los interesados son conscientes de la divulgación de sus datos de carácter personal a otras filiales fuera de la Unión Europea, de conformidad con las autorizaciones concedidas por las autoridades de protección de datos sobre la base de reglas corporativas vinculantes.

Las personas tendrán acceso fácil a la información sobre los principales compromisos asumidos por el grupo en materia de protección de datos, la información actualizada sobre los miembros sujetos a las normas y los medios a disposición de los interesados para verificar el cumplimiento de estas normas.

El Grupo de Trabajo adoptó un nuevo documento (WP 102) el 25 de noviembre de 2004: *Lista de comprobación tipo – Solicitud de aprobación de reglas corporativas vinculantes.* El Grupo confeccionó esta lista con el objetivo de ayudar a aquel grupo de empresas interesado en presentar una solicitud de aprobación de sus reglas corporativas vinculantes y, en particular, para mostrar cómo se cumple con el Documento de Trabajo WP 74.

El Grupo adoptó otro Documento (WP 107) el 14 de abril de 2005[169]. En éste se establecen criterios orientadores en cuanto a la elección de la autoridad que tomará el liderazgo en el proceso de autorización, así como de la cooperación que debe existir entre las autoridades de protección de datos involucradas[170].

Cualquier grupo que quiera someter a aprobación un proyecto de reglas corporativas vinculantes ante diferentes autoridades encargadas de la protección de datos, debe proponer a una de ellas como la autoridad de referencia, a los fines del procedimiento de cooperación. La elección de la autoridad investida de esta misión deberá estar motivada por el grupo y basará su elección sobre la base de criterios pertinentes, tales como:

- La ubicación de la sede principal europea.
- La ubicación de la compañía a la que ha delegado las responsabilidades en materia de protección de datos.
- La ubicación de la compañía que está en mejores condiciones (en términos de gestión, apoyo administrativo, etc.) para tramitar la solicitud y poner en práctica las reglas corporativas vinculantes en el grupo.
- El lugar donde se toman la mayoría de las decisiones en relación con los fines y los medios de tratamiento.

[169] Document de travail relatif à une procédure de coopération en vue de l'émission d'avis communs sur le caractère adéquat de la protection offerte par les «règles d'entreprise contraignantes».

[170] Como señala Fréderic Blas, el sistema de reglas corporativas vinculantes es un instrumento muy avanzado. Sin embargo, queda mucho por desarrollar ya que viendo los costes necesarios y la complejidad y variedad de los criterios para tener aprobadas las reglas en 30 países, es un ejercicio extremadamente lento y costoso. Artículo "Transferencias internacionales de datos, perspectiva española de la necesaria búsqueda de estándares globales". Revista Derecho del Estado nº 23, diciembre de 2009, p. 58.

- Los Estados miembros de la UE de donde provienen la mayoría de las transferencias de datos hacia los países fuera del EEE.

La autoridad responsable de la protección de datos a la que se haga la solicitud[171] tendrá competencia exclusiva para decidir si es, de hecho, la autoridad más adecuada. Las autoridades encargadas de la protección de datos podrán decidir entre ellas si se envía la solicitud a una autoridad distinta a aquella a la que el grupo había elegido inicialmente.

Asimismo, el solicitante deberá aportar al órgano propuesto como autoridad de referencia, toda la información pertinente para justificar su propuesta: la naturaleza y la

[171] Es muy relevante la información ofrecida en la web de la APD del Reino Unido (ICO): **http://www.ico.gov.uk/for_organisations/data_protection/overseas/binding_corporate_rules.aspx**

La APD de Reino Unido ha sido muy activa en el campo de las reglas corporativas vinculantes, habiendo autorizado en base a las mismas, las transferencias de datos personales a las siguientes entidades (información obtenida en su web a uno de enero de 2013):

15 Diciembre 2005 - The General Electric Company for employee data.

2 Abril 2007 - Koninklijke Philips Electronics NV for employee data.

22 Abril 2009 - The Atmel Corporation for employee data.

30 Abril 2009 - Accenture Limited.

15 Septiembre 2009 - The Hyatt Hotel Corporation for employee and guest data.

26 Febrero 2010 - JPMorgan Chase & Co.

31 Marzo 2010 - British Petroleum plc.

12 Mayo 2010 - IMS Health Incorporated.

16 Febrero 2011 - Spencer Stuart Management Consultants N.V.

31 Marzo 2011 - CareFusion Incorporated.

14 Noviembre 2011 - First Data Corporation.

26 Marzo 2012 - eBay Incorporated

21 Mayo 2012 - Novo Nordisk A/S

1 Junio 2012 - Linklaters LLP

14 Junio 2012 - Citigroup Incorporated

5 Septiembre 2012 - Intel Corporation

29 Octubre 2012 - American Express Company

estructura general de las operaciones de tratamiento en el EEE, en particular con respecto a los lugares donde se toman las decisiones, la ubicación y naturaleza de las compañías en la UE, el número de empleados o interesados, los medios y los fines del tratamiento, los lugares a partir de los cuales se efectúan las transferencias a terceros países y la relación de los países terceros a los que se transfieren los datos. Esta documentación deberá facilitarse impresa y en formato electrónico para hacer más fácil su distribución.

A partir de este momento, y siguiendo a Norman Heckh[172], podríamos clasificar los siguientes pasos de la forma siguiente:

- El solicitante debe remitir a la autoridad de referencia la información apropiada que justifique su solicitud, incluido su borrador de BCR.
- La autoridad de referencia distribuye la documentación facilitada por el solicitante a las autoridades de protección de datos de los Estados desde los que se puedan hacer transferencias. Éstas podrán formular observaciones en relación al cumplimiento de las condiciones exigidas en su derecho nacional para la autorización de las transferencias. También podrán exigir aclaraciones o modificaciones que consideren necesarias para proceder a dicha autorización.
- La autoridad de referencia entabla negociaciones con el solicitante. De estas negociaciones debe salir un borrador consolidado de BCR, que se remitirá a las demás autoridades de protección de datos para que puedan formular nuevamente observaciones.

[172] HECKH, N. y otros: *Memento Experto Protección de Datos*. Francis Lefebvre. Madrid 2012, pág. 124.

- La autoridad de referencia envía las nuevas observaciones al solicitante y en caso necesario pueden reanudarse las conversaciones entre ambas partes. En respuesta las observaciones recibidas, el solicitante debería preparar un borrador final de BCR. Dicho documento se envía al resto de autoridades para que den su conformidad al nuevo texto que se ha formulado.
- Una vez aprobadas las BCR se deben solicitar a las autoridades nacionales las autorizaciones de transferencia internacional de datos.

Esta decisión será notificada al Presidente del Grupo de Trabajo, quien informará sin demora a las autoridades de protección de datos de los otros países del EEE.

Como indica Aparicio Salom, en este procedimiento se "excluye de participar a aquellas autoridades de control que no estuvieran afectadas, es decir, donde el grupo que solicita la aprobación del código no tiene filiales en el momento de la solicitud. Esta circunstancia priva de pronunciarse a estas autoridades respecto del borrador presentado y de participar en el acuerdo resultante de la tramitación, de modo que si posteriormente el grupo abre una filial en dicho país, esta filial no podrá verse beneficiada de la elasticidad que se pretende conseguir con este sistema, sino que tendrá que solicitar de la autoridad de control correspondiente que acepte el código como habilitante para la autorización"[173].

[173] APARICIO SALOM, J: *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal*. Aranzadi. Navarra 2009, pág. 369.

El Grupo de Trabajo adoptó otro documento, el WP 108, en la misma fecha que había adoptado el WP 107, el 14 de abril de 2005[174]. En este documento se establece una lista de control tipo para las solicitudes de aprobación de reglas corporativas vinculantes. Las cuestiones tratadas por el documento son las siguientes:

- ¿A qué autoridad encargada de la protección de datos se debe dirigir la solicitud?
- ¿Qué información se debe comunicar?
- Pruebas del carácter jurídicamente vinculante de las medidas.
- Verificación del respeto a las reglas.
- Descripción del tratamiento y de los flujos de información.
- Garantías en la protección de los datos.
- Modalidades de comunicación y de registro de las modificaciones.

Podríamos mencionar también la Recomendación 1/2007 (WP 133) del Grupo de Trabajo, adoptada el 10 de enero de 2007[175]. En este documento se incluye un cuestionario estandarizado para la solicitud de aprobación de reglas corporativas vinculantes. Está preparado sobre la base de un documento elaborado por la Cámara Internacional de Comercio. Se basa en los documentos publicados por el Grupo de Trabajo y, en particular, tiene la intención de ayudar a los solicitantes para cumplir con los requisitos establecidos en el WP 74 y WP 108.

[174] Document de travail établissant une liste de contrôle type pour les demandes d'approbation des règles d'entreprise contraignantes.

[175] Recommendation 1/2007 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data.

El Grupo de Trabajo adoptó tres documentos adicionales el 24 de junio de 2008: WP 153[176], WP 154[177] y WP 155[178] (si bien este último se revisó por última vez y se adoptó el 8 de abril de 2009).

En el documento WP 153 se quiere facilitar la aplicación de las reglas corporativas vinculantes. Para ello se ha desarrollado una tabla cuyo objetivo es:

- Especificar el contenido requerido de las reglas corporativas vinculantes como se establece en dos documentos distintos, el WP 74 y WP 108.
- Distinguir entre lo que debería ser incluido en las reglas corporativas vinculantes y lo que hay que presentar a las autoridades responsables de la protección de datos en el contexto de una solicitud de aprobación (WP 133).
- Para cada principio, indicar las referencias a los documentos WP 74 y WP 108 para más detalles.
- Dar explicaciones y comentarios sobre cada principio.

El Documento divide los criterios para la aprobación de las reglas corporativas vinculantes en seis categorías, subdividida cada una de ellas en subapartados de mayor detalle[179].

[176] Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules.

[177] Working Document Setting up a framework for the structure of Binding Corporate Rules.

[178] Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules.

[179] Los criterios para la aprobación de las reglas corporativas vinculantes se dividen en las siguientes categorías:

- Caractère contraignant.
- Efficacité.
- Devoir de coopération.

El Documento WP 154 establece una guía que integra todos los elementos indispensables descritos en los documentos WP 74 y WP 108. El Grupo de Trabajo advierte que esta guía no es un modelo que se pueda usar directamente. Es una simple propuesta en cuanto al contenido y la forma en la que las reglas podrían estar estructuradas en un único documento que pueda ser vinculante en el grupo de empresas. Las reglas corporativas vinculantes deberán ser adaptadas con el fin de tener en cuenta la estructura del grupo al que se aplican, las operaciones de tratamiento que las filiales efectúan y las políticas y procedimientos que aplican para proteger los datos de carácter personal.

En el Documento de Trabajo WP 155 el Grupo de Trabajo, en conjunto con las autoridades de protección de datos, publican las preguntas más frecuentes (FAQ) que se apoyan en la experiencia obtenida en las solicitudes de aprobación de reglas corporativas vinculantes y en las solicitudes de información sobre la interpretación de los documentos WP 74 y WP 108. Las preguntas más frecuentes están destinadas a aclarar los requisitos específicos para ayudar a los solicitantes a obtener la aprobación de sus reglas corporativas vinculantes.

Entre las preguntas más relevantes podríamos citar las cuatro siguientes[180]:

- Description du traitement et des flux des données.
- Modalités de communication et d'enregistrement des modifications.
- Garanties concernant la protection des données.

[180] El conjunto de preguntas del Documento es el siguiente:

Les règles d'entreprise contraignantes doivent-elles s'appliquer à toutes les données à caractère personnel traitées par le groupe? Les règles d'entreprise contraignantes doivent-elles s'appliquer aux sous-traitants qui ne font pas partie du groupe? Si une violation des règles d'entreprise contraignantes est commise en dehors de l'UE, quelle filiale du groupe en est responsable? Les règles d'entreprise contraignantes doivent-elles toujours conférer à la personne concernée le droit de déposer une plainte

1 – ¿Las reglas corporativas vinculantes deben aplicarse a todos los datos de carácter personal tratados por el grupo?

No. Las reglas corporativas vinculantes son un medio jurídico para proteger adecuadamente los datos personales cubiertos por la Directiva 95/46/CE y transferidos fuera de la UE a países que no ofrecen un nivel adecuado de protección. Para los otros datos de carácter personal tratados por el grupo y no sometidos a ningún tratamiento en la UE no existe la obligación de quedar sometidos a las reglas. Sin embargo, se recomienda encarecidamente a los grupos multinacionales que aplican reglas corporativas vinculantes que adopten un único conjunto de políticas o de reglas globales para proteger todos los datos personales que tratan.

2 - Si una violación de las reglas corporativas vinculantes se comete fuera de la UE, ¿qué filial del grupo es la responsable?

Las reglas corporativas vinculantes deben designar una entidad en el seno de la Unión Europea que acepta asumir la responsabilidad de cualquier infracción a las reglas cometida por una compañía del grupo fuera de la UE.

El Documento WP 74 prevé que en la mayoría de los casos será la sede del grupo, si está establecida en la UE, quien asumirá la responsabilidad de la infracción. Si la sede

---

auprès de l'autorité de protection des données pour violation des règles d'entreprise contraignantes? Les informations sur les droits de tiers bénéficiaires doivent-elles être facilement accessibles aux personnes concernées qui en bénéficient? Les règles d'entreprise contraignantes doivent-elles décrire les traitements et les transferts de données à caractère personnel effectués au sein du groupe, et jusqu'à quel niveau de détail? Les règles d'entreprise contraignantes doivent-elles être exposées dans un document unique qui consacre l'ensemble des obligations du groupe et des droits des individus? Quelle terminologie les demandeurs doivent-ils utiliser pour rédiger leurs règles d'entreprise contraignantes? Quels droits doivent être conférés aux personnes en vertu de la clause relative aux droits de tiers bénéficiaires? Quelle relation y a-t-il entre les législations relatives à la protection des données en vigueur dans l'EEE et les règles d'entreprise contraignantes? Que signifie le renversement de la charge de la preuve en pratique?

del grupo está establecida en el exterior de la UE, se permite a dicho grupo que designe la compañía adecuada dentro de la UE para que sea quien asuma las responsabilidades de las infracciones cometidas en el exterior de la UE. Esta responsabilidad incluye, si ha lugar, el pago de una indemnización para reparar el perjuicio resultante de la infracción.

Cuando no sea factible la designación de una filial que se haga cargo de todas las responsabilidades, el grupo podrá proponer otros mecanismos que puedan responder frente a las mismas.

3 – Las reglas corporativas vinculantes ¿deben dar siempre a la persona interesada el derecho a presentar una denuncia ante la Autoridad de Protección de Datos por la violación dichas reglas corporativas vinculantes?

Sí. Es importante consagrar el derecho a presentar una denuncia en caso de violación de las reglas por una compañía del grupo.

4 – La información sobre los derechos de terceros beneficiarios ¿debe ser fácilmente accesible a las personas interesadas a las que beneficia?

Sí. El Documento WP 74 exige que las reglas corporativas vinculantes y las vías de reclamación y de reparación en caso de infracción de las reglas sean fácilmente accesibles a las personas interesadas.

Podríamos citar un último Documento del Grupo de Trabajo, adoptado el 6 de junio de 2012 (WP 195)[181]. Al igual que los Documentos de Trabajo antes mencionados tiene como misión la de facilitar el uso de las reglas corporativas vinculantes.

[181] Working Document 02/2012 setting up a table with the elements and principles to be found in Processor Binding Corporate Rules.

2.2 NORMATIVA ESPAÑOLA EN CUANTO A LA REGLAS CORPORATIVAS VINCULANTES

En la LOPD no se hace mención alguna a las reglas corporativas vinculantes[182]. El Reglamento de desarrollo de la Ley, de fecha mucho más reciente (21 de diciembre de 2007), ya las contempla como herramienta a través de la cual pueda otorgarse la autorización para llevar a cabo una transferencia internacional de datos.

De acuerdo al artículo 70.4 del RLOPD podrá otorgarse la autorización para la transferencia internacional de datos en el seno de grupos multinacionales de empresas cuando hubiesen sido adoptados por los mismos normas o reglas internas en que consten las necesarias garantías de respeto a la protección de la vida privada y el derecho fundamental a la protección de datos de los afectados y se garantice asimismo el cumplimiento de los principios y el ejercicio de los derechos reconocidos en la LOPD y en el propio Reglamento.

Para que proceda la autorización del Director de la Agencia Española de Protección de Datos será preciso que las normas o reglas resulten vinculantes para las empresas del Grupo y exigibles conforme al ordenamiento jurídico español. Esta autorización implicará la exigibilidad de lo previsto en las normas o reglas internas tanto por la Agencia como por los afectados cuyos datos hubieran sido objeto de tratamiento. En este sentido, el artículo 70.4 del RLOPD pretende dejar, en el ámbito de las reglas corporativas vinculantes, sin efecto el contenido del artículo 1089 del Código Civil. En éste se estipula que "las obligaciones nacen de la ley, de los contratos y cuasi contratos, y de los actos y omisiones ilícitos o en que intervenga cualquier género de culpa o

[182] Hemos de tener en cuenta que la LOPD fue aprobada a finales de 1999.

negligencia". Por lo tanto, la declaración unilateral de voluntad, por regla general, no es fuente de obligaciones.

El RLOPD no da mayor concreción a las reglas corporativas vinculantes ni informa de los detalles que se exigirán por parte de la AEPD. Sus requisitos y contenido lo deberemos extraer de los Documentos elaborados por el Grupo de Trabajo que ya hemos visto anteriormente[183].

Como pone de manifiesto Álvarez Rigaudias, la autoridad de protección de datos del Reino Unido, el Information Commissioner, emitió dos documentos en septiembre de 2003 y en febrero de 2004 en los cuales clarificaba los requisitos que esta autoridad exige a aquellos grupos que deseen solicitar la autorización de reglas corporativas vinculantes desde el Reino Unido. "Sería pues deseable que la AEPD, siguiendo el ejemplo de su homóloga inglesa, estableciera una primera guía orientativa al respecto"[184].

En relación a este tema es muy interesante la consulta de la "Resolución de Autorización de Transferencias Internacionales de Datos" por parte de la AEPD,

[183] Así lo deja bien claro la AEPD en su *Informe sobre Transferencias Internacionales de Datos. Inspección sectorial de oficio España-Colombia en Centros de atención al Cliente. Julio de 2007*: "Un modelo alternativo para cumplir con los requisitos que permiten autorizar las transferencias internacionales consiste en la fijación de reglas corporativas vinculantes o BCR (Binding Corporate Rules). Este modelo suele plantearse en el caso de grupos de compañías internacionales y posee una cierta complejidad en su tramitación. Cuando una compañía o grupo de compañías internacionales opte por esta vía, debería previamente evaluar su conveniencia, en base a los documentos de trabajo del Grupo de Trabajo del artículo 29". Pág. 25 del documento. Descargable en la siguiente dirección electrónica: **http://www.agpd.es/portalwebAGPD/jornadas/transferencias_internacionales_datos/common/pdfs/INFORME_TIs.pdf**

[184] ÁLVAREZ RIGAUDIAS, C: "Las Transferencias Internacionales de Datos Personales y el Nivel Equiparable o Adecuado de Protección". Revista Actualidad Jurídica Uría Menéndez / 12-2005. Pág. 30.

referente al expediente TI/000040/2009[185]. Se trataba de una solicitud de autorización de transferencias internacionales de datos en el seno del grupo multinacional General Electric en base a Reglas Corporativas Vinculantes. En la Resolución se aclara "que el análisis de las BCR únicamente será suficiente para justificar las transferencias internacionales de datos sometidas a autorización del Director de la Agencia. En modo alguno podrá considerarse que dichas normas sean sustitutivas de lo establecido por el derecho nacional". Y añade "que los tratamientos de datos llevados a cabo en territorio español quedarán en todo caso sometidos a la LOPD y su normativa de desarrollo, siendo las BCR en lo que se refiere a tales tratamientos meramente complementarias de lo previsto en dicha normativa. De este modo, si las exigencias contenidas en las BCR, aun cuando pudieran ser suficientes para amparar una transferencia internacional de datos, fueran menos estrictas que las previstas en la legislación española, será ésta la que se aplique en lo referente a los tratamientos de datos efectuados dentro del ámbito de aplicación establecido en el artículo 2.1 de la LOPD y 3 del RLOPD".

2.3. ESTADO ACTUAL DEL MECANISMO DE APROBACIÓN DE LAS REGLAS CORPORATIVAS VINCULANTES

En el Documento de la AEPD titulado *Segunda sesión anual abierta de la Agencia Española de Protección de Datos* se informa del acuerdo alcanzado en septiembre y comunicado al Grupo de Trabajo del artículo 29 en octubre de 2008 sobre reconocimiento mutuo de las reglas corporativas vinculantes.

[185] El documento TI/000040/2009 se puede descargar desde la página web de la AEPD. La publicación oficial del Acuerdo de Apertura del Período de Información Pública se llevó a cabo en el BOE de seis de abril de 2009.

El acuerdo supone una mejora del procedimiento de coordinación ya existente[186], al que se le reconoce un defecto esencial que es la lentitud y complejidad para llegar a acuerdos con todas las autoridades participantes. Cuando una empresa solicite autorización para unas reglas corporativas vinculantes ante una de las autoridades participantes (autoridad de referencia), la decisión de ésta será aceptada por las demás autoridades participantes afectadas por tener la empresa actividad en su territorio.

Como señala Frédéric Blas "el reconocimiento mutuo es una obligación política, más que un cambio legal. Se basa en la confianza y en la consideración de que estos sistemas legislativos están basados en la directiva europea"[187].

El mecanismo es un compromiso que no altera la necesidad de iniciar los respectivos procedimientos nacionales y tampoco modifica la necesidad de que las reglas corporativas vinculantes se ajusten a las especificidades de tales legislaciones.

El grupo inicial de autoridades en materia de protección de datos que acordó iniciar el procedimiento de reconocimiento mutuo de las reglas corporativas vinculantes estaba formado por las agencias de protección de datos siguientes: Francia, Reino Unido, Irlanda, Alemania (Federal y estados), España, Italia, Holanda, Luxemburgo y Letonia. Posteriormente se han añadido nuevas autoridades de otros países[188].

---

[186] Procedimiento de coordinación ya descrito en base al Documento WP 107.

[187] FRÉDÉRIC BLAS: "Transferencias internacionales de datos, perspectiva española de la necesaria búsqueda de estándares globales". Revista Derecho del Estado. Núm. 23 (2009), p. 37-66.

[188] Por el momento, 21 países son parte del procedimiento de reconocimiento mutuo: Austria, Bélgica, Bulgaria, Chipre, República Checa, Estonia, Francia, Alemania, Islandia, Irlanda, Italia, Letonia, Liechtenstein, Luxemburgo, Malta, Países Bajos, Noruega, Eslovaquia, Eslovenia, España y el Reino Unido (relación obtenida en la web de la Comisión Europea a uno de enero de 2013).

La lista de las empresas que tienen cerrado el procedimiento de reglas corporativas vinculantes es la siguiente[189]:

Nombre de la compañía	**Autoridad líder**
GE	ICO (UK)
Atmel	ICO (UK)
Accenture	ICO (UK)
BP	ICO (UK)
e-Bay	Luxemburgo
Hyatt	ICO (UK)
Sanofi Aventis	CNIL (FR)
Michelin	CNIL (FR)
JPMC	ICO (UK)
Safran	CNIL (FR)
Spencer Stuart	ICO (UK)
Care Fusion	ICO (UK)
Hewlett Packard	CNIL (FR)
International SOS	CNIL (FR)
Bristol Myers Squibb	CNIL (FR)
Intel Corporation	Irlanda
Deutsche Post DHL	BfDI, Alemania
IMS Health Incorporated	ICO (UK)
First Data Corporation	ICO (UK)
Novo Nordisk A/S	Dinamarca
Linklaters	ICO (UK)
Schlumberger Ltd.	Dutch DPA
Sara Lee International B.V.	Dutch DPA
Citigroup	ICO (UK)
Shell International B.V.	Dutch DPA
LVMH	CNIL (FR)
CMA-CGM	CNIL (FR)

[189] Lista obtenida en la página de políticas de la Dirección Gral. de Justicia de la Comisión Europea **http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/bcr_cooperation/index_en.htm** (relación expuesta a uno de enero de 2013).

Hermès	CNIL (FR)
NOVARTIS	CNIL (FR)
Royal Philips Electronics	Dutch DPA
American Express	ICO (UK)
ABN AMRO Bank N.V.	Dutch DPA

Como se puede comprobar, las autoridades que han liderado la mayor parte de los procedimientos son la agencia del Reino Unido (ICO) y la de Francia (CNIL).

3. LAS EXCEPCIONES A LA NECESIDAD DE AUTORIZACIÓN

En el diccionario del la Real Academia Española se define la palabra *excepción* como aquella "cosa que se aparta de la regla o condición general de las demás de su especie". En este sentido vamos a estudiar las excepciones recogidas en el artículo 26.1 de la Directiva 95/46/CE y en el artículo 34 de la LOPD.

3.1. EXCEPCIONES DEL ARTÍCULO 26.1 DE LA DIRECTIVA 95/46/CE

El artículo 26.1 de la Directiva enuncia un número limitado de situaciones en las que se puede aplicar una excepción al requisito de *adecuación* de las transferencias a terceros países. En concreto, los Estados miembros dispondrán que pueda efectuarse una transferencia de datos siempre y cuando:

a) el interesado haya dado su consentimiento inequívocamente a la transferencia prevista, o

b) la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales tomadas a petición del interesado, o

c) la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar en interés del interesado, entre el responsable del tratamiento y un tercero, o

d) La transferencia sea necesaria o legalmente exigida para la salvaguardia de un interés público importante, o para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial, o

e) la transferencia sea necesaria para la salvaguardia del interés vital del interesado, o

f) la transferencia tenga lugar desde un registro público que, en virtud de disposiciones legales o reglamentarias, esté concebido para facilitar información al público y esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo, siempre que se cumplan, en cada caso particular, las condiciones que establece la ley para la consulta.

Como indica Sancho Villa, se trata de transferencias que se dirigen a países que carecen de un nivel de protección adecuado, pero que a pesar de ello no se someten a "autorización previa ninguna". Se entiende "que los intereses que recogen cada uno de los supuestos excepcionales lo justifican"[190].

En contra de lo que pueda parecer, este conjunto de excepciones no ha tenido un tratamiento pacífico en los diferentes Estados. Así lo manifiesta el Informe de la Comisión denominado *Primer informe sobre la aplicación de la Directiva sobre protección de datos (95/46/CE)*[191], de 15 de mayo de 2003. En el apartado donde

[190] SANCHO VILLA, D: *Transferencia Internacional de Datos Personales*. Agencia Española de Protección de Datos, Madrid 2003, pág. 156.

[191] COM (2003) 265 final.

analiza las divergencias entre las legislaciones de los Estados miembros, manifiesta que evidentemente, "cuando un Estado miembro ha sobrepasado los límites de la Directiva o no ha cumplido sus requisitos, se crea una divergencia que se ha de solucionar mediante la modificación de la legislación del Estado miembro en cuestión". Como indica Téllez Aguilera, en las legislaciones en materia de protección de datos de los diversos países de la Unión Europea, se observa "una parcial coincidencia en los enunciados y una patente divergencia en los resultados"[192]. En determinadas disposiciones el margen de acción de los Estados miembros es muy reducido o inexistente y pese a ello se han producido divergencias. Tal es el caso de la trasposición del artículo 26.1. La Comisión ha manifestado en repetidas ocasiones su disposición al uso de las competencias otorgadas por el artículo 258[193] del Tratado de Funcionamiento de la UE, a efecto de que se introdujeran las oportunas modificaciones legales en los Estados, pero nunca ha procedido a una actuación formal.

Al analizar en concreto las divergencias encontradas en la transposición y aplicación de los artículos 25 y 26 (la dimensión exterior), la Comisión llega a la conclusión de que son excesivas.

El planteamiento adoptado por algunos Estados miembros, en los que se considera que es el responsable del tratamiento de datos quien tiene que evaluar la adecuación de la protección prestada por el destinatario, con un control muy limitado de los flujos de

[192] TÉLLEZ AGUILERA, A: *La protección de datos en la Unión Europea. Divergencias normativas y anhelos unificadores*. Editorial Edisofer. Madrid 2002, pág. 333.

[193] De acuerdo al artículo 258 del TFUE: "Si la Comisión estimare que un Estado miembro ha incumplido una de las obligaciones que le incumben en virtud de los Tratados, emitirá un dictamen motivado al respecto, después de haber ofrecido a dicho Estado la posibilidad de presentar sus observaciones. Si el Estado de que se trate no se atuviere a este dictamen en el plazo determinado por la Comisión, ésta podrá recurrir al Tribunal de Justicia de la Unión Europea".

datos por parte del Estado o la autoridad nacional de control, no parece, a juicio de la Comisión, cumplir el requisito impuesto a los Estados miembros en el apartado 1 del artículo 25.

El planteamiento adoptado por algunos otros Estados miembros, que someten todas las transferencias a terceros países a una autorización administrativa, también parece incoherente con el capítulo IV de la Directiva, que tiene por objeto garantizar la protección adecuada y al mismo tiempo los flujos de datos personales a terceros países sin obligaciones innecesarias. Con arreglo al artículo 19 de la Directiva 95/46/CE pueden exigirse notificaciones a las autoridades nacionales de control, pero en opinión de la Comisión, las notificaciones no pueden convertirse de hecho en autorizaciones en aquellos casos en los que esté claramente permitida la transferencia a un tercer país, bien porque el destinatario se encuentre en un país que ofrece una protección adecuada confirmada en una decisión vinculante de la Comisión, bien porque haya suscrito las cláusulas contractuales tipo aprobadas por la Comisión, o bien porque el responsable del tratamiento de datos declare que la transferencia se acoge a una de las excepciones previstas en el artículo 26 de la Directiva. Aunque la autoridad de protección de datos puede exigir legítimamente la notificación de dichas transferencias, no es necesario autorizarlas, porque ya están autorizadas por la legislación comunitaria[194].

Entre las iniciativas propuestas por la Comisión en su Informe, encontramos una Acción (la número 7) para la *simplificación de los requisitos para las transferencias internacionales*. En dicha Acción, la Comisión, con la colaboración del Grupo de

[194] En el caso español se incumple claramente la interpretación de la Comisión en el caso de las transferencias internacionales basadas en cláusulas contractuales tipo. No sería necesaria la autorización de la AEPD porque ya están autorizadas por la legislación comunitaria.

Trabajo del artículo 29 y del Comité del artículo 31, espera avanzar en distintos ámbitos. De éstos, podemos destacar el lograr una interpretación más uniforme del apartado 1 del artículo 26 de la Directiva (excepciones autorizadas al requisito de protección adecuada para las transferencias a terceros países) y las disposiciones nacionales que lo aplican.

El Grupo de Trabajo del artículo 29 retomó dicho tema en el Documento de Trabajo WP 114, relativo a una interpretación común del artículo 26, apartado 1, de la Directiva 95/46/CE de 24 de octubre de 1995[195].

En el Documento de Trabajo se ofrece una serie de orientaciones sobre cómo se debería entender y aplicar el artículo 26, apartado 1, de la Directiva 95/46/CE por parte de los responsables del tratamiento que tengan la intención de realizar transferencias de datos a países que no garanticen un nivel de protección adecuado, en el sentido de lo dispuesto en el artículo 25 de la Directiva.

El Grupo pretende despejar las dudas ante las interpretaciones divergentes que se están haciendo en la práctica de las disposiciones del artículo 26.1, que impiden su aplicación uniforme en los diferentes Estados miembros.

El Grupo de Trabajo coincide con el contenido del Informe elaborado por la Comisión Europea en 2003. Ni un planteamiento excesivamente estricto, ni un enfoque demasiado laxo de lo dispuesto en los artículos 25 y 26 (y específicamente en el artículo 26.1) estaría en consonancia con los fines que se pretende alcanzar, que no son otros que lograr un equilibrio justo entre la protección de los individuos cuyos datos se han de transferir a países que no reúnen las condiciones adecuadas y, entre otras, las

[195] Documento de Trabajo adoptado el 25 de noviembre de 2005.

necesidades legítimas del comercio internacional y la realidad de las redes mundiales de telecomunicación.

Las disposiciones incluidas en el artículo 26.1, facilitan sustancialmente la transferencia de datos personales a un tercer país. Conforme a estas disposiciones, el responsable del tratamiento de los datos que da origen a la transferencia no tiene que asegurarse de que el destinatario ofrece la protección adecuada ni necesita, por lo general, obtener ningún tipo de autorización previa de las autoridades competentes para proceder a la transferencia. Además, estas disposiciones no exigen que el destinatario de los datos cumpla los requisitos establecidos en la Directiva por lo que respecta a cualquier tratamiento de datos en su propio país (por ejemplo, los principios de finalidad, seguridad, derecho de acceso, etc.).

Esta permisividad podría atribuirse al reconocimiento de que la expansión del comercio internacional requiere en determinadas ocasiones la flexibilidad de las transferencias internacionales de datos, incluidas las transferencias de información personal. Otra explicación puede radicar en que el artículo 26.1 se concibió para dar respuesta a un reducido número de situaciones en las que se consideraba que estaba justificada una excepción al requisito de adecuación para las transferencias a terceros países[196].

[196] Como el Grupo de trabajo ya había mencionado en el documento WP12, estas excepciones, muy circunscritas, se refieren en su mayoría a casos en los que los riesgos para el interesado son relativamente escasos o en los que otros intereses (intereses públicos o del propio interesado) prevalecen sobre los derechos de intimidad del interesado. Como excepciones a un principio general, deben interpretarse restrictivamente. Además, los Estados miembros pueden estipular en la legislación nacional que las excepciones no se apliquen en determinados casos. Este puede ser el caso, por ejemplo, cuando sea necesario proteger a grupos de personas especialmente vulnerables, como los trabajadores o los pacientes.

En opinión del Grupo de Trabajo, en la práctica, entre los responsables del tratamiento ha habido una tendencia a hacer uso de estas excepciones como primera opción, incluso en los casos en los que no procedía. De acuerdo al Documento WP 12 la interpretación del artículo 26.1 ha de ser necesariamente restrictiva[197], al igual que en la lógica que subyace en el Protocolo Adicional al Convenio 108.

El Grupo de Trabajo recomienda a los responsables del tratamiento que garanticen la protección adecuada en tantas situaciones como sea posible. Cuando se tenga la intención de transferir datos a terceros países, los responsables del tratamiento de datos establecidos en la Unión Europea deben optar por soluciones que ofrezcan a los interesados la garantía de que seguirán beneficiándose de los derechos y las salvaguardias fundamentales a que tienen derecho por lo que se refiere al tratamiento de sus datos en la UE, una vez que tales datos hayan sido transferidos. Si el nivel de protección en el tercer país no es el adecuado, el responsable del tratamiento debería considerar lo dispuesto en el artículo 26.2, es decir, ofrecer las garantías adecuadas mediante, por ejemplo, cláusulas contractuales tipo o reglas corporativas vinculantes. Únicamente en el caso de que ello no resulte verdaderamente práctico o viable, el responsable del tratamiento de los datos debería considerar hacer uso de las excepciones contempladas en el artículo 26.1.

El Grupo de Trabajo consideraría lamentable que una empresa multinacional o una autoridad pública se planteasen llevar a cabo transferencias significativas de datos a un

[197] Como también se indica en el document de la CNIL *Tout sur les exceptions*: "L'application des dispositions doit être limitée à des cas ponctuels et exceptionnels".

Documento disponible en:

http://www.cnil.fr/fileadmin/documents/Vos_responsabilites/Transferts/CNIL-transferts-EXCEPTIONS.pdf

tercer país sin ofrecer un marco adecuado para las mismas, y siempre que dispongan de los medios prácticos para ofrecer esta protección (un contrato o normas corporativas vinculantes). Cuando recurrir a este marco legal sea imposible en la práctica, el Grupo de Trabajo admite que pueda haber transferencias masivas o repetidas de datos en base a lo dispuesto el artículo 26.1 a condición de que los riesgos para el interesado sean pequeños.

En el Documento de Trabajo se ofrecen algunas directrices en cuanto al significado específico de cada una de las excepciones enumeradas en el artículo 26.1. Estas directrices se elaboraron a partir de la experiencia del Grupo de trabajo y de las autoridades nacionales de protección de datos personales en este campo:

Consentimiento (art. 26.1.a)).

El artículo 26.1.a) establece que se podrá realizar una transferencia de datos personales a un país que no garantice un nivel de protección adecuada, siempre y cuando el interesado haya dado su consentimiento inequívocamente a la transferencia prevista. Para que este consentimiento sea válido ha de ser una manifestación de voluntad, libre, específica e informada de los deseos del interesado, como lo define el artículo 2.h) de la Directiva[198].

El consentimiento se ha de dar de forma *clara e inequívoca*. Se excluye cualquier sistema por el que el interesado sólo tuviera derecho a oponerse a la transferencia después de haberse producido. Para que una transferencia pueda llevarse a efecto se ha de exigir el consentimiento específico para la misma. Cualquier duda que surja en

[198] Artículo 2.h) de la Directiva 95/46/CE:

A efectos de la presente Directiva, se entenderá por "consentimiento del interesado": toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernan.

relación con el otorgamiento del consentimiento hará inaplicable esta excepción. Ello puede significar que en muchas situaciones en que el consentimiento se da por sobreentendido la excepción no resulte aplicable.

Cuando el consentimiento del interesado a la realización de una transferencia se solicita por Internet, el Grupo de Trabajo recomienda que se utilicen casillas que han de ser marcadas por el interesado para manifestar su consentimiento previo. La utilización de casillas ya marcadas no cumple la condición de que el consentimiento ha de ser una indicación clara e inequívoca de intenciones[199].

El consentimiento debe darse *libremente*. Cuando un interesado no ha gozado de la oportunidad de hacer una verdadera elección o se ha encontrado frente a un hecho consumado no se puede considerar que el consentimiento sea válido[200].

El Grupo de Trabajo desea llamar la atención sobre el hecho de que pueden plantearse determinadas dificultades a la hora de considerar que un interesado ha dado su consentimiento libremente en un contexto laboral[201], como consecuencia de la relación de subordinación entre el empleador y el empleado. En tales situaciones de dependencia jerárquica, la negativa o las reservas de un empleado en relación con una transferencia podrían sin duda causarle un perjuicio moral o material, que es

[199] Ya se había manifestado el Grupo de Trabajo en los mismos términos en el Dictamen 5/2004 sobre comunicaciones de venta directa no solicitadas de conformidad con el artículo 13 de la Directiva 2002/58/CE, WP 90, de 27 de febrero de 2004, apartado 3.2.

[200] En el Dictamen 6/2002 relativo a la transmisión de listas de pasajeros y otros datos de compañías aéreas a los Estados Unidos, WP 66, de 24 de octubre de 2002, ya se planteó la duda de si el consentimiento podía ser utilizado para transferir los datos de reservas. Está claro que los pasajeros no pueden dar libremente su consentimiento, ya que, si quieren volar, no tienen elección posible.

[201] Véase el Dictamen 8/2001 sobre el tratamiento de datos personales en el contexto laboral, WP 48, de 13 de septiembre de 2001.

completamente contrario a la letra y al espíritu de la normativa europea de protección de datos personales. En los casos que sea preciso que un empresario se base en el consentimiento, el Grupo de trabajo invita a los empresarios, siempre que sea posible, a no basarse exclusivamente en el consentimiento de sus empleados cuando transfieran datos, salvo en aquellos casos en los que no quepa la menor duda de que los empleados no van a sufrir consecuencias de ningún tipo, de no dar su consentimiento a una transferencia, o si han dado su consentimiento pero posteriormente desean retirarlo.

El Grupo de Trabajo sugiere que, en la mayor parte de casos, es improbable que el consentimiento ofrezca un marco adecuado a largo plazo para los responsables del tratamiento en casos de transferencias repetidas o incluso estructurales para el tratamiento de que se trate.

El consentimiento debe ser *específico*. El interesado ha de dar específicamente su consentimiento para una transferencia concreta o una categoría específica de transferencias. Puesto que el consentimiento debe ser específico, a veces resulta imposible obtener el consentimiento previo del interesado para una transferencia futura, si, por ejemplo, las circunstancias específicas de una transferencia no se conocen en el momento en que se solicite el consentimiento, con lo que no se puede evaluar la repercusión en el interesado. No obstante, es posible que una persona pueda dar su consentimiento de forma válida por adelantado a la transferencia de sus datos a un tercer país, cuando los pormenores de la transferencia esté predeterminados, especialmente por lo que se refiere a la finalidad y categorías de los destinatarios.

El consentimiento debe ser *informado*. El interesado ha de ser informado adecuadamente por adelantado de las circunstancias específicas de la transferencia (su finalidad, la identidad y datos pormenorizados de los destinatarios, etc.), con arreglo al

principio general de lealtad. La información que se ofrezca a los interesados deberá incluir también la relativa al riesgo específico derivado del hecho de que sus datos se transferirán a un país que no ofrece un nivel adecuado de protección. Sólo si se le facilita esta información podrá el interesado dar su consentimiento con pleno conocimiento de causa. En caso contrario la excepción no será de aplicación.

Transferencia necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales adoptadas a instancias del interesado (art. 26.1.b))

Una transferencia de datos a un tercer país que no ofrezca la protección adecuada sólo se puede acoger a la excepción contemplada en el artículo 26.1.b)[202], si puede ser considerada *necesaria* para la ejecución del contrato en cuestión o la ejecución de medidas precontractuales adoptadas a petición del interesado. Es decir, se exige una relación estrecha y sustancial entre el interesado y el objeto del contrato.

A ciertos grupos internacionales les gustaría poder acogerse a esta excepción para transferir datos de sus empleados de una filial a la empresa matriz, con objeto, por ejemplo, de descentralizar las funciones de gestión de pagos y recursos humanos del grupo. Estos grupos internacionales están convencidos de que estas transferencias podrían ser consideradas necesarias para la ejecución del contrato de trabajo suscrito entre el empleado y el responsable del tratamiento. El Grupo de Trabajo estima que esta interpretación es excesiva, dado que resulta muy cuestionable que el concepto de un

[202] Véase el Informe Jurídico 0190/2008 de la AEPD. En el Informe se analiza la transmisión de los datos a una compañía ubicada fuera de la UE. La AEPD considera que el caso analizado se encuentra amparado en el artículo 34.f) de la LOPD (similar en contenido al artículo 26.1.b) de la Directiva 95/46/CE). Documento disponible en la dirección electrónica de la AEPD: **https://www.agpd.es/**

contrato laboral pueda ser interpretado de forma tan amplia, ya que no existe un vínculo directo y objetivo entre la ejecución de un contrato laboral y la transferencia de datos.

Por el contrario, esta excepción constituiría un fundamento jurídico aceptable para la transferencia efectuada por agencias de viaje de los datos personales relativos a sus clientes individuales a hoteles u otros socios comerciales que intervengan en la organización de la estancia de dichos clientes.

Por último, esta excepción no puede aplicarse a las transferencias de información adicional que no sean necesarias a efectos de la transferencia, o a las transferencias destinadas a una finalidad distinta de la ejecución del contrato.

Transferencia necesaria para la celebración o ejecución de un contrato celebrado en interés del interesado entre el responsable del tratamiento y un tercero (art. 26.1.c))

No se puede considerar que una transferencia de datos a un tercer país que no garantice la protección se acoge a la excepción contemplada en el artículo 26.1.c), a menos que pueda ser considerada verdaderamente *necesaria* para la celebración o ejecución de un contrato celebrado o por celebrar en interés del interesado, entre el responsable del tratamiento y un tercero. Se exige entonces que exista un vínculo estrecho y sustancial entre el interés del interesado y el objeto del contrato.

El Grupo de Trabajo analiza, por ejemplo, el caso de alguna empresa que ha mostrado su intención de acogerse a esta excepción para poder llevar a efecto transferencias internacionales de datos relativos a sus empleados, a otra empresa establecida fuera de la UE, a la que subcontrata la gestión del pago de sus nóminas. En opinión de dichas empresas, estas transferencias serían necesarias para la ejecución de sus contratos de externalización y serían en interés del interesado, puesto que la

finalidad de la transferencia es la gestión del pago de las nóminas de los empleados. En este caso, sin embargo, el Grupo de trabajo considera que no se ha acreditado el vínculo estrecho sustancial entre el interés del interesado y el objeto del contrato, y que la excepción no es de aplicación.

El Grupo de Trabajo quiere dejar claro que, tanto en el ejemplo mencionado como en cualquier otro caso similar, la interpretación que hace del artículo 26.1.c) no implica en modo alguno que tenga una opinión negativa de la elección por parte de los responsables del tratamiento de recurrir a encargados del tratamiento de datos en terceros países, sino que simplemente desea insistir en la conveniencia de basarse en un instrumento contemplado en el artículo 26.2 (en la práctica, un contrato) para iniciar transferencias de datos en estos casos.

Transferencia necesaria o legalmente exigida para la salvaguardia de un interés público importante, o para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial (art. 26.1.d))

El Grupo de trabajo dio una interpretación restrictiva del concepto de motivos de *interés público importantes* en su Dictamen 6/2002 sobre el PNR de 24 de octubre de 2002. En él rechazó el uso de esta excepción para justificar la transferencia de datos relativos a pasajeros aéreos a las autoridades de EE.UU. por motivos de interés público importantes por dos razones: en primer lugar, no se había acreditado la necesidad de llevar a cabo dicha transferencia, y, en segundo lugar, no parece aceptable que una decisión unilateral adoptada por un tercer país, alegando motivos específicos de interés público importantes, conduzca a efectuar con regularidad transferencias masivas de datos protegidos por la Directiva.

Otra visión distinta es la que aparece en el Documento WP 143[203] del Grupo de Trabajo. Dicho Documento analiza la Directiva 2006/43/CE, relativa a la auditoría legal de las cuentas anuales y de las cuentas consolidadas (8ª Directiva). Esta Directiva establece las condiciones necesarias para desarrollar la actividad de auditoría legal y prevé la supervisión pública independiente de los auditores legales por los Estados miembros. También contiene disposiciones específicas sobre la cooperación entre los organismos públicos de supervisión de los Estados miembros y las autoridades competentes de los terceros países. Esta cooperación debe incluir el intercambio de los documentos de auditoría del auditor y de otros documentos que obran en poder de las sociedades europeas de auditoría, con las autoridades de los terceros países.

El Grupo de Trabajo advierte de la obligación de que las transferencias internacionales se sometan a la regulación de la Directiva 95/46/CE, opinando que el artículo 26.1 letra d), de la Directiva 95/46/CE, puede constituir la base legal de la transferencia a los reguladores públicos de los terceros países, de documentos de trabajo de auditoría que contengan datos personales. No obstante, el Grupo de Trabajo recuerda que dicha excepción al régimen general de la Directiva de protección de datos que se aplica a los flujos transfronterizos de datos debe interpretarse de forma restrictiva por lo que respecta al interés público importante del envío y a la necesidad de garantizar que sólo se envíen los datos personales relevantes y necesarios en función de dicho interés público importante.

[203] Octava Directiva relativa a la auditoría legal. Dictamen 10/2007 del Grupo de Trabajo del artículo 29, WP 143, emitido el 23 de noviembre de 2007.

El Grupo de trabajo subraya que el concepto de *reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial* también ha de estar sujeto a interpretación estricta. Así pues, por ejemplo, la matriz de una multinacional, establecida en un tercer país, podría ser llevada ante los tribunales por un empleado del grupo que ejerza actualmente sus funciones en una de sus filiales europeas. La excepción prevista en el artículo 26.1.d) parece permitir a la empresa que solicite legalmente a la filial europea la transferencia de determinados datos relativos al empleado, si tales datos fuesen necesarios para su defensa.

En sentido contrario, esta excepción no puede utilizarse para justificar la transferencia de todos los ficheros del empleado a la empresa matriz del grupo, alegando la posibilidad de que algún día se empleen en tales procedimientos judiciales.

Transferencia necesaria para proteger los intereses vitales del interesado (art. 26.1.e))

La excepción prevista en el artículo 26.1.e) se aplica obviamente cuando se transfieren datos en caso de urgencia médica, cuando se considere que son directamente necesarios para prestar la asistencia médica requerida. Así por ejemplo, ha de ser posible transferir datos de forma legal si el interesado está inconsciente y necesita asistencia médica urgente. En estos casos no tiene lógica imponer cualquier otro tipo de requisito para poder efectuar la transferencia.

Esta excepción no podrá utilizarse para justificar la transferencia si su finalidad no es la de tratar el caso específico del interesado. En estos casos, habría que cumplir los requisitos alternativos establecidos en el artículo 26.2 de la Directiva.

Es muy interesante el análisis que hace el Grupo de Trabajo en su Documento WP 131[204] en cuanto a la transferencia internacional de historiales médicos. El Grupo admite que la disponibilidad electrónica de datos médicos puede mejorar considerablemente las facilidades de diagnóstico o de tratamiento, permitiendo el recurso a conocimientos médicos disponibles solamente en instituciones médicas extranjeras. Pero esa consulta de expertos extranjeros a efectos de diagnóstico no requiere generalmente que se revele la identidad del paciente. Por tanto, en la medida de lo posible, tales datos deberían transferirse a países fuera de la Unión Europea de forma anónima o al menos utilizando pseudónimos. Si no se cuenta con el consentimiento explícito del interesado para la transferencia de datos personales, esta solución también evitaría la necesidad de obtener permiso para esta transferencia de datos, pues el interesado no es identificable para el receptor de los mismos.

Teniendo en cuenta el elevado riesgo que existe para los datos personales contenidos en un sistema de historiales médicos electrónicos en un medio sin protección adecuada, el Grupo de Trabajo subraya que todo tratamiento de dichos datos deberá realizarse en países que apliquen la Directiva de protección de datos de la UE o un marco jurídico adecuado de protección de datos.

Transferencia realizada desde un registro público (art. 26.1.f))

Esta excepción se refiere a transferencias desde un registro público que, en virtud de disposiciones legales o reglamentarias, esté concebido para facilitar información al público y esté abierto a la consulta por el público en general o por cualquier persona que

[204] Documento de Trabajo sobre el tratamiento de datos personales relativos a la salud en los historiales médicos electrónicos (HME), WP 131, adoptado el 15 de febrero de 2007.

pueda demostrar un interés legítimo, siempre que se cumplan, en cada caso particular, las condiciones que establece la ley para la consulta.

Si un registro de este tipo puede ser consultado por cualquier persona (o por cualquiera que tenga un interés legítimo) en el interior del país, parece lógico que se permita su consulta a cualquier persona establecida en un tercer país. Pero el considerando 58 de la Directiva impone ciertos límites cuando declara que "en tal caso dicha transferencia no debe afectar a la totalidad de los datos o las categorías de datos que contenga el mencionado registro". En caso contrario cabría la posibilidad de que entidades establecidas en terceros países pudieran emplear los datos para fines distintos de aquéllos para los que se concibieron originalmente.

Habíamos indicado que en el Documento de Trabajo WP 114 se pretendía ofrecer directrices para interpretar las excepciones contempladas en el artículo 26.1 de la Directiva 95/46/CE. Entre las interpretaciones específicas se había analizado la excepción basada en el *consentimiento*. Cinco años después, en la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre *un enfoque global de la protección de los datos personales en la Unión Europea*[205], dentro del apartado denominado “reforzar los derechos de las personas” vuelve a insistir en el objetivo de *garantizar un consentimiento informado y libre.* De acuerdo al texto de la Comunicación, cuando se exige un consentimiento informado, las normas vigentes prevén que el consentimiento

[205] COM (2010) 609 final, de 4.11.2010. En este documento se plantea que a pesar de que los principios planteados por la Directiva 95/46/CE siguen siendo válidos, la rapidez de la evolución tecnológica y la globalización han modificado profundamente nuestro medio y han lanzado nuevos retos en materia de protección de los datos personales.

de la persona sobre el tratamiento de sus datos personales debería ser una *manifestación de voluntad, libre, específica e informada* por la que acepta este tratamiento. Sin embargo estas condiciones son objeto de distintas interpretaciones en los Estados miembros, desde la obligación general de obtener un consentimiento escrito hasta la aceptación de un consentimiento implícito.

La Comisión opina que es preciso clarificar las condiciones del consentimiento del interesado, con el fin de garantizar que se concede siempre con conocimiento de causa, y de garantizar que el interesado es plenamente consciente de que da su autorización y respecto a qué tratamiento, de conformidad con lo dispuesto en el artículo 8 de la Carta de los Derechos Fundamentales de la UE.

Por dichos motivos la Comisión se compromete a estudiar los medios de clarificar y reforzar las normas en materia de consentimiento.

El Grupo de Trabajo del artículo 29 en su Dictamen 15/2011, WP 187, sobre la definición del consentimiento, adoptado el 13 de julio de 2011, analiza el concepto de consentimiento tal como figura en la Directiva de protección de datos. El Dictamen se elabora en parte como respuesta a una petición formulada por la Comisión en el marco del proceso de revisión de la Directiva de protección de datos. Contiene por ello recomendaciones a considerar en dicha revisión. Entre estas figuran:

- La aclaración del significado del consentimiento *inequívoco* y la explicación de que sólo el consentimiento basado en manifestaciones o acciones que expresen conformidad constituye un consentimiento válido.
- La exigencia a los responsables del tratamiento de que apliquen mecanismos para comprobar el consentimiento (en el marco de la obligación general de responsabilidad).

- La introducción de un requisito específico relativo a la calidad y accesibilidad de la información, que constituyen la base del consentimiento.
- Una serie de sugerencias sobre los menores y otras personas que carecen de capacidad jurídica.

Entre los objetivos del Dictamen está aclarar ciertas cuestiones acerca del consentimiento a fin de que el marco legal existente sea entendido de forma uniforme en los diferentes países.

En el apartado III.A.4 del Dictamen, dedicado al artículo 26.1.a), establece que el consentimiento inequívoco del interesado es una excepción a la prohibición de transferir datos a terceros países que no ofrezcan garantías. Además de los requisitos de validez del consentimiento, el consentimiento deberá ser pues inequívoco.

El Grupo de Trabajo insiste en la postura adoptada en el Documento WP12 en relación con el significado del consentimiento inequívoco. Cualquier duda sobre su obtención anularía la aplicabilidad de la excepción. Esto podría significar que en muchas situaciones en que el consentimiento se da por sobreentendido la excepción no resultaría aplicable. Por lo tanto quedará más claro que se ha obtenido el consentimiento inequívoco cuando las personas realicen acciones afirmativas para mostrar su acuerdo con la transferencia, como por ejemplo firmar un formulario de consentimiento o realizar otras acciones que no dejen lugar a dudas sobre el consentimiento otorgado.

También vuelve a apoyarse en el documento WP 114 cuando se refiere al uso del consentimiento para las transferencias de datos al insistir en lo improbable de que el consentimiento ofrezca un marco adecuado a largo plazo para los responsables del tratamiento en casos de transferencias repetidas o incluso estructurales para el tratamiento de que se trate.

3.2. LAS EXCEPCIONES DEL ARTÍCULO 34 DE LA LOPD

El artículo 34 de la LOPD relaciona las excepciones a la prohibición de realizar transferencias contenida en el artículo 33 de la propia Ley.

Así dispone que el contenido de dicho artículo 33 no será de aplicación:

"a) Cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España.

b) Cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional.

c) Cuando la transferencia sea necesaria para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamiento médicos o la gestión de servicios sanitarios.

d) Cuando se refiera a transferencias dinerarias conforme a su legislación específica.

e) Cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista.

f) Cuando la transferencia sea necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero o para la adopción de medidas precontractuales adoptadas a petición del afectado.

g) Cuando la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar, en interés del afectado, por el responsable del fichero y un tercero.

h) Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público. Tendrá esta consideración la transferencia solicitada por una Administración fiscal o aduanera para el cumplimiento de sus competencias.

i) Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

j) Cuando la transferencia se efectúe, a petición de persona con interés legítimo, desde un Registro Público y aquélla sea acorde con la finalidad del mismo.

k) Cuando la transferencia tenga como destino un Estado miembro de la Unión Europea, o un Estado respecto del cual la Comisión de las Comunidades Europeas, en el ejercicio de sus competencias, haya declarado que garantiza un nivel de protección adecuado".

Como señala Frédéric Blas[206] "son una lista con 11 epígrafes, sin ningún criterio sistemático ni lógico". Siguiendo su argumentación, los cuatro primeros (letras *a* hasta *d*) son una reproducción prácticamente literal de los motivos de excepción que aparecían en la LORTAD, mientras que los seis siguientes lo son de la lista de excepciones de la Directiva 95/46/CE (letras e hasta j). La letra k es un intento tanto de recoger en el derecho español la libertad de circulación de datos dentro de la Unión Europea como de reconocer una primacía de la Comisión Europea en determinar el nivel de adecuación de terceros países.

Del contenido del artículo 34 debemos entender que el hecho de aplicar alguna de las excepciones dispensa al exportador de la obtención de garantías por parte del importador en cuanto al nivel de protección adecuado.

[206] BLAS, Frédéric: "Transferencias internacionales de datos, perspectiva española de la necesaria búsqueda de estándares globales". Revista Derecho del Estado nº 23, diciembre de 2009, pp. 37 a 66.

El RLOPD en su artículo 66.2.b) se remite a lo indicado en la Ley: se produce la excepción cuando la transferencia se encuentre en uno de los supuestos contemplados en los apartados a) a j) del artículo 34 de la LOPD.

También se remitía al contenido de la LOPD la Instrucción 1/2000, de 1 de diciembre, al regular en el punto 1 de su Norma Quinta, que cuando la transferencia internacional tenga por destinatario una persona física o jurídica, pública o privada, situada en el territorio de un Estado no miembro de la Unión Europea, respecto del que no se haya declarado por la Comisión Europea la existencia de un nivel adecuado de protección o que no pertenezca al Espacio Económico Europeo y el transmitente se funde en alguno de los supuestos comprendidos en los apartados a) a j) del artículo 34 de la LOPD, la Agencia de Protección de Datos podrá requerir al responsable del fichero para que aporte la documentación que justifique su alegación.

A la lista de excepciones de la Directiva 95/46/CE que habíamos señalado anteriormente, vemos que se añaden en la normativa española tres supuestos adicionales: transferencias en aplicación de tratados o convenios en los que sea parte España, transferencias a efectos de prestar o solicitar auxilio judicial internacional y transferencias dinerarias conforme a su legislación específica. Analizaremos cada uno de ellos.

Transferencias en aplicación de tratados o convenios en los que sea parte España

España es parte firmante y ha ratificado el Convenio 108 del Consejo de Europa, así como su Protocolo Adicional[207]. Debe respetar el contenido de los mismos en su integridad, y de forma particular en lo que respecta a las transferencias internacionales de datos[208].

Transferencias a efectos de prestar o solicitar auxilio judicial internacional

En base a esta exención no es necesaria la autorización del Director de la AEPD para proceder a efectuar una transferencia cuyo motivo sea prestar o solicitar auxilio judicial internacional.

Transferencias dinerarias conforme a su legislación específica

Se refiere por una parte a las transferencias efectuadas por establecimientos de cambio de moneda que tienen autorización para la gestión de transferencias dinerarias con el exterior. Estos establecimientos están regulados básicamente por el RD 2660/1998, de 14 de diciembre, sobre el cambio de moneda extranjera en establecimientos abiertos al público distintos de las entidades de crédito, y por la Orden

[207] Véase el Instrumento de Ratificación del Protocolo Adicional al Convenio en el BOE de 20 de septiembre de 2010.

[208] Según el artículo 12.2 del Convenio, una Parte no podrá, con el fin de proteger la vida privada, prohibir o someter a una autorización especial los flujos transfronterizos de datos de carácter personal con destino al territorio de otra Parte. De acuerdo al artículo 2.1 del Protocolo Adicional cada Parte preverá que la transferencia de datos personales a un destinatario sometido a la competencia de un Estado u organización que no es Parte del Convenio se lleve a cabo únicamente si dicho Estado u organización asegura un adecuado nivel de protección.

de 16 de noviembre de 2000 de regulación de determinados aspectos del régimen jurídico de los establecimientos de cambio de moneda y sus agentes.

Por otra parte incluye las transferencias bancarias para la gestión de cobros y pagos de clientes.

En ambos supuestos la exención tiene razón de ser en las transferencias internacionales de datos que se tengan que llevar a cabo para poder efectuar la operación dineraria hacia países que no ofrecen un nivel adecuado de protección.

Al igual que en los casos anteriores, tampoco será necesaria la autorización del Director de la AEPD.

Por último, podríamos citar por su interés una parte del Fundamento de Derecho Tercero de la Sentencia de la Audiencia Nacional (Sala de lo Contencioso-Administrativo, Sección Primera), de 15 de marzo de 2002, en relación con la Instrucción Número 1/2000, de 1 de diciembre: "la existencia de las mencionadas excepciones a la regla general en modo alguno significa, claro es, que en estos supuestos inexigibilidad de la autorización previa el responsable del fichero que promueve la transferencia de datos quede liberado del conjunto de deberes y obligaciones que le impone la Ley Orgánica 15/1999; ni que pueda eludir las responsabilidades derivadas de su actuación. Únicamente queda liberado de la exigencia de autorización previa de la transferencia por el Director de la Agencia, y ello por disponerlo así de manera expresa el mencionado artículo 34".

4. LAS TRANSFERENCIAS A ESTADOS QUE NO PROPORCIONEN UN NIVEL ADECUADO DE PROTECCIÓN EN LA PROPUESTA DE REGLAMENTO DE PROTECCIÓN DE DATOS DE LA UE

En el capítulo anterior se analizaron las transferencias a estados que proporcionen un nivel adecuado de protección en la Propuesta de Reglamento. Ahora se estudiarán las transferencias a estados que no proporcionen un nivel adecuado.

La Propuesta de Reglamento tiene una serie de innovaciones relevantes sobre la normativa actualmente vigente. Quizá la más importante sea el impulso que se quiere dar a las reglas o normas corporativas vinculantes. Esta figura no aparecía en la Directiva 95/46/CE y obtuvo su desarrollo básicamente a través de los documentos de trabajo del Grupo de Trabajo del artículo 29 de la Directiva.

Se considera que las normas corporativas vinculantes son el instrumento más adecuado para regular las transferencias internacionales de datos en los grupos multinacionales. Sin embargo los plazos para su aprobación por las autoridades en materia de protección de datos, la complejidad del proceso y los costes elevados han hecho que muchos grupos no se las planteen como una solución viable.

El Proyecto de Reglamento quiere que las normas corporativas vinculantes se conviertan en el estándar que empleen los grupos multinacionales en el futuro. Para conseguirlo se quiere simplificar y clarificar el procedimiento de aprobación.

Los artículos del Proyecto de Reglamento que regulan las transferencias a estados que no proporcionen un nivel adecuado de protección son los 42, 43 y 44, junto con el

artículo 45 dedicado a la Cooperación internacional en el ámbito de la protección de datos personales.

Según el artículo 42 (que lleva como título *Transferencias mediante garantías apropiadas*), cuando la Comisión no haya adoptado una decisión de adecuación sólo se podrán transferir datos personales a un tercer país o una organización internacional si se ofrecen garantías apropiadas en un instrumento jurídicamente vinculante. Estas garantías se pueden conseguir, en particular, a través de las siguientes cuatro vías:

a) Las normas corporativas vinculantes.

b) Las cláusulas tipo de protección de datos adoptadas por la Comisión.

c) Las cláusulas tipo de protección de datos adoptadas por una autoridad de control.

d) Las cláusulas contractuales entre el responsable o el encargado del tratamiento y el destinatario de los datos autorizadas por una autoridad de control.

Como ya se ha indicado, la primera de las cuatro vías es realmente la novedosa con respecto a la Directiva. Las cláusulas contractuales ya están contempladas en la actual normativa.

En el Considerando 83 de la Propuesta de Reglamento parece que esta relación se amplía, ya que además de las cuatro posibilidades mencionadas también abre la puerta a "otras medidas adecuadas y proporcionadas que se justifiquen a la luz de todas las circunstancias que rodean la operación de transferencia de datos o las operaciones de transferencia de conjuntos de datos y siempre que las autorice una autoridad de control".

También es relevante el contenido del Considerando 84 en cuanto a la flexibilización del uso de las cláusulas tipo: "La posibilidad de que el responsable o el

encargado del tratamiento utilicen cláusulas tipo de protección de datos adoptadas por la Comisión o una autoridad de control no debe impedir que los responsables o encargados del tratamiento incluyan las cláusulas tipo de protección de datos en un contrato más amplio o añadan otras cláusulas, siempre que no contradigan, directa o indirectamente, las cláusulas contractuales tipo adoptadas por la Comisión o por una autoridad de control o perjudiquen a los derechos o las libertades fundamentales de los interesados".

En el artículo 42.5 se contradice lo enunciado anteriormente. Si allí habíamos apuntado la exigencia de ofrecer garantías apropiadas en un instrumento jurídicamente vinculante, en este artículo se regula que "cuando las garantías apropiadas con respecto a la protección de datos personales *no se proporcionen en un instrumento jurídicamente vinculante*, el responsable o el encargado del tratamiento deberán obtener la autorización previa de la transferencia o serie de transferencias, o de las disposiciones que se vayan a insertar en el acuerdo administrativo que constituye la base de dicha transferencia".

El Grupo de Trabajo, en su *Dictamen 01/2012 sobre las propuestas de reforma de la protección de datos*, critica la introducción de la posibilidad de emplear instrumentos no vinculantes para enmarcar las transferencias internacionales que dependen de una autorización de las autoridades de control. El carácter vinculante se ha considerado siempre un requisito importante en los instrumentos que enmarcan las transferencias internacionales y por ello el Grupo de Trabajo propone la eliminación de esta innovación.

El Supervisor Europeo de Protección de Datos en su Dictamen de 7 de marzo de 2012 también manifiesta su desacuerdo con el contenido del artículo 42.5, planteando la

necesidad de “garantizar que la posibilidad de utilizar instrumentos no vinculantes jurídicamente para proporcionar garantías adecuadas debería quedar claramente justificada y limitarse sólo a los casos en que haya quedado demostrado la necesidad de confiar en dichos instrumentos”.

En el artículo 43 de la Propuesta de Reglamento aparece la parte más novedosa con respecto a la actual Directiva. Está dedicado a las *transferencias mediante normas corporativas vinculantes*.

En el artículo 43.1 se regula que una autoridad de control aprobará normas corporativas vinculantes siempre que éstas:

a) sean jurídicamente vinculantes y se apliquen a todos los miembros del grupo de empresas del responsable o del encargado del tratamiento, incluidos sus empleados, que asegurarán su cumplimiento;

b) confieran expresamente a los interesados derechos exigibles;

c) cumplan los requisitos establecidos en el apartado 2 del mismo artículo.

En el artículo 43.2 se especifica el contenido mínimo que han de tener las normas corporativas vinculantes:

a) la estructura y los datos de contacto del grupo de empresas y de sus miembros;

b) las transferencias o serie de transferencias de datos, incluidas las categorías de datos personales, el tipo de tratamientos y sus fines, el tipo de interesados afectados y el nombre del tercer o los terceros países en cuestión;

c) su carácter jurídicamente vinculante, tanto a nivel interno como externo;

d) los principios generales en materia de protección de datos, en particular la limitación de la finalidad, la calidad de los datos, la base jurídica del tratamiento,

el tratamiento de datos personales sensibles, las medidas encaminadas a garantizar la seguridad de los datos y los requisitos en materia de transferencias ulteriores a organizaciones que no estén vinculadas por esas políticas;

e) los derechos de los interesados y los medios para ejercerlos, en particular el derecho a no ser objeto de una medida basada en la elaboración de perfiles de conformidad con lo dispuesto en el artículo 20, el derecho a presentar una reclamación ante la autoridad de control competente y ante los órganos jurisdiccionales competentes de los Estados miembros de conformidad con lo dispuesto en el artículo 75, y el derecho a obtener una reparación, y, cuando proceda, una indemnización por violación de las normas corporativas vinculantes;

f) la aceptación por parte del responsable o del encargado del tratamiento establecidos en el territorio de un Estado miembro de la responsabilidad por cualquier violación de las normas corporativas vinculantes por parte de cualquier miembro del grupo de empresas no establecido en la Unión; el responsable o el encargado del tratamiento solo podrán ser exonerados de esta responsabilidad, total o parcialmente, si prueban que el acto que originó el daño no es imputable a dicho miembro;

g) la forma en que se facilita a los interesados la información sobre las normas corporativas vinculantes, en particular en lo que respecta a las disposiciones contempladas en las letras d), e) y f), de conformidad con lo dispuesto en el artículo 11;

h) las tareas del delegado de protección de datos designado de conformidad con lo dispuesto en el artículo 35, en particular la supervisión, dentro del grupo de

empresas, del cumplimiento de las normas corporativas vinculantes, así como la supervisión de la formación y de la tramitación de las reclamaciones;

i) los mecanismos establecidos dentro del grupo de empresas para garantizar que se verifica el cumplimiento de las normas corporativas vinculantes;

j) los mecanismos establecidos para comunicar y registrar las modificaciones introducidas en las políticas y para notificar esas modificaciones a la autoridad de control;

k) el mecanismo de cooperación con la autoridad de control para garantizar el cumplimiento por parte de todos los miembros del grupo de empresas, en particular poniendo a disposición de la autoridad de control los resultados de las verificaciones de las medidas contempladas en la letra i).

El contenido mínimo que han de tener las normas corporativas vinculantes no difiere en gran manera de la actual exigencia por parte de las autoridades de control en base a la regulación que ha ido asentándose en los distintos documentos adoptados por el Grupo de Trabajo del artículo 29. Pero es importante que esta regulación pase a formar parte de un texto legislativo ya que, como hemos reiterado en ocasiones anteriores, la Directiva 95/46/CE desconoce esta figura.

En el Considerando 85 de la Propuesta de Reglamento parece entenderse la intención de que las normas corporativas vinculantes pasen a ser un instrumento habitual en todos los grupos multinacionales. Según el mismo, “todo grupo de sociedades debe poder hacer uso de normas corporativas vinculantes autorizadas para sus transferencias internacionales de la Unión a organizaciones dentro del mismo grupo de empresas, siempre que tales normas corporativas incluyan principios esenciales y

derechos aplicables con el fin de asegurar las garantías apropiadas para las transferencias o categorías de transferencias de datos de carácter personal".

Además, como se indica en la Comunicación al Comité Económico y Social Europeo y al Comité de las Regiones[209], a partir de la reforma de la protección de datos, dentro de un proceso de simplificación y racionalización:

- las normas corporativas vinculantes serán validadas por una única autoridad responsable de protección de datos, con mecanismos para asegurar la pronta participación de las demás autoridades de protección de datos pertinentes;
- una vez una autoridad haya aprobado una norma corporativa vinculante, esta será válida para toda la UE sin necesidad de autorizaciones adicionales a nivel nacional.

El Supervisor Europeo de Protección de Datos en su Dictamen de 7 de marzo de 2012 opina que debería incluirse la posibilidad de la "participación de los representantes del personal en todos los niveles, nacionales y europeos, en la elaboración de normas corporativas vinculantes".

En el artículo 44, sobre *excepciones*, se relaciona una serie tasada de casos en los que se podrá proceder a una transferencia de datos personales a un tercer país o a una organización internacional en ausencia de una decisión de adecuación o de garantías apropiadas. Se dan estas circunstancias cuando:

---

[209] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. *La protección de la privacidad en un mundo interconectado. Un marco europeo de protección de datos para el siglo XXI*. Bruselas, 25.1.2012 COM(2012) 9 final.

a) el interesado haya dado su consentimiento a la transferencia propuesta, tras haber sido informado de los riesgos que entraña debido a la ausencia de una decisión de adecuación y de garantías apropiadas; o

b) la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la implementación de medidas precontractuales adoptadas a solicitud del interesado; o

c) la transferencia sea necesaria para la celebración o ejecución de un contrato, en interés del interesado, entre el responsable del tratamiento y otra persona física o jurídica; o

d) la transferencia sea necesaria por motivos importantes de interés público; o

e) la transferencia sea necesaria para el reconocimiento, el ejercicio o la defensa de un derecho en un procedimiento judicial; o

f) la transferencia sea necesaria para proteger los intereses vitales del interesado o de otra persona, cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento; o

g) la transferencia se realice desde un registro público que, con arreglo al Derecho de la Unión o de un Estado miembro, tenga por objeto facilitar información al público y esté abierto a la consulta del público en general o de cualquier persona que pueda acreditar un interés legítimo, en la medida en que se cumplan, en cada caso particular, las condiciones que establece el Derecho de la Unión o de un Estado miembro para la consulta; o

h) la transferencia sea necesaria para la satisfacción de los intereses legítimos del responsable o del encargado del tratamiento, que no puedan ser calificados de frecuentes ni de masivos, y el responsable o el encargado hayan evaluado todas

las circunstancias que rodean la operación o la serie de operaciones de transferencia de datos y hayan ofrecido en su caso, sobre la base de dicha evaluación, garantías apropiadas con respecto a la protección de datos personales.

Esta relación difiere muy poco con la que contiene la Directiva 95/46/CE, excepto en la última de las posibilidades mencionadas: la transferencia que se justifique en la necesidad para la satisfacción de los intereses legítimos del responsable o del encargado del tratamiento. El Grupo de Trabajo, en el documento WP 191, critica esta excepción ya que considera que es demasiado amplia y puede ser aplicable a demasiadas situaciones. Además, y siguiendo con sus criterios tradicionales (manifestados en el documento WP 114 entre otros), considera que las excepciones relacionadas en el artículo 44 de la Propuesta de Reglamento únicamente deben aplicarse en la medida en que el tratamiento no sea masivo, repetitivo o estructural.

El Supervisor Europeo de Protección de Datos en su Dictamen de 7 de marzo de 2012 opina que en el artículo 44 (y en el Considerando 87) se debería "añadir que la posibilidad de transferir datos debería afectar únicamente a las transferencias ocasionales y que debería estar basada en una evaluación cuidadosa, caso por caso, de todas las circunstancias de la transferencia". También cree oportuno "sustituir o aclarar la referencia a las «garantías adecuadas» del artículo 44, apartado 1, letra h)".

Por último mencionar el contenido del Considerando 89 de la Propuesta de Reglamento para cualquier caso de transferencia internacional (incluido aquellas justificadas por alguna excepción) cuando la Comisión no haya tomado ninguna decisión sobre el nivel adecuado de protección de los datos en un tercer país. El

responsable o el encargado del tratamiento deberán arbitrar soluciones que garanticen a los interesados que seguirán beneficiándose de los derechos fundamentales y garantías en lo que se refiere al tratamiento de sus datos en la Unión, una vez que tales datos hayan sido transferidos.

El artículo 45 de la Propuesta de Reglamento "establece explícitamente mecanismos de cooperación internacional para la protección de los datos de carácter personal entre la Comisión y las autoridades de control de terceros países, especialmente aquellas que se considera que ofrecen un nivel de protección adecuado, teniendo en cuenta la Recomendación de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) para la cooperación transfronteriza en la ejecución de leyes que protegen la privacidad, de 12 de junio de 2007". La Comisión y las autoridades de control tomarán medidas apropiadas para:

a) crear mecanismos de cooperación internacional eficaces que faciliten la aplicación de la legislación relativa a la protección de datos personales;

b) prestarse mutuamente asistencia a escala internacional en la aplicación de la legislación relativa a la protección de datos personales, en particular mediante la notificación, la remisión de reclamaciones, la asistencia en las investigaciones y el intercambio de información, a reserva de las garantías apropiadas para la protección de los datos personales y otros derechos y libertades fundamentales;

c) procurar la participación de las partes interesadas pertinentes en los debates y actividades destinados a reforzar la cooperación internacional en la aplicación de la legislación relativa a la protección de datos personales;

d) promover el intercambio y la documentación de la legislación y las prácticas en materia de protección de datos personales.

Como se señala en el documento COM(2012) 9 final, los retos que plantea la globalización requieren herramientas y mecanismos flexibles, especialmente para las empresas activas en todo el mundo, que garanticen al mismo tiempo la protección sin fisuras jurídicas de los datos personales. La Comisión propone entre otras medidas la "apertura de un diálogo y, cuando así proceda, negociaciones con terceros países –especialmente los socios estratégicos de la UE y los países de la Política Europea de Vecindad– y con las organizaciones internacionales pertinentes (como el Consejo de Europa, la Organización para la Cooperación y el Desarrollo Económico y las Naciones Unidas) a fin de promover la adopción de unas normas de protección de datos exigentes e interoperables en todo el mundo".

CAPÍTULO IV

PROCEDIMIENTOS RELACIONADOS CON LAS TRANSFERENCIAS INTERNACIONALES DE DATOS

El título IX del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, está dedicado a los procedimientos tramitados por la AEPD. El capítulo V del título IX regula en concreto los procedimientos relacionados con las transferencias internacionales de datos.

El capítulo V se subdivide a su vez en dos secciones:

- Sección 1.ª Procedimiento de autorización de transferencias internacionales de datos. Incluye los artículos 137 a 140 del Reglamento.

- Sección 2.ª Procedimiento de suspensión temporal de transferencias internacionales de datos. Incluye los artículos 141 a 144 del Reglamento.

1. PROCEDIMIENTO DE AUTORIZACIÓN DE TRANSFERENCIAS INTERNACIONALES DE DATOS

Como hemos señalado en los capítulos anteriores, las transferencias internacionales de datos se regulan básicamente en el Capítulo IV de la Directiva 95/46/CE (artículos 25 y 26), en el Título V de la LOPD (artículos 33 y 34) y en el Título VI del RLOPD (artículos 65 a 70).

De acuerdo al artículo 25.1 de la Directiva 95/46/CE, los Estados miembros dispondrán que la transferencia a un país tercero de datos personales únicamente pueda efectuarse cuando el país tercero de que se trate garantice un nivel de protección adecuado.

Habíamos analizado en apartados anteriores el artículo 26.1 de la Directiva 95/46/CE, que regula una serie de excepciones bajo las que se puede efectuar una transferencia de datos personales a un país tercero que no garantice un nivel de protección adecuado, sin necesidad de obtener autorización del organismo correspondiente.

La transposición de las excepciones del artículo 26.1 de la Directiva se efectuó a través del artículo 34 de la LOPD (si bien, como ya se comentó en su momento, con una redacción diferente a la que aparece en la Directiva).

Dejando aparte las excepciones, tal como indica el artículo 26.2, los Estados miembros podrán autorizar una transferencia o una serie de transferencias de datos personales a un tercer país que no garantice un nivel de protección adecuado cuando el responsable del tratamiento ofrezca garantías suficientes respecto de la protección de la vida privada, de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los respectivos derechos; dichas garantías podrán derivarse, en particular, de cláusulas contractuales apropiadas.

La transposición de estos artículos en la LOPD la encontramos en el artículo 33.1, donde se regula que no podrán realizarse transferencias temporales ni definitivas de datos de carácter personal con destino a países que no proporcionen un nivel de protección equiparable, salvo que se obtenga autorización previa del Director de la Agencia Española de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas.

De acuerdo al artículo 66.1 del RLOPD, para que la transferencia internacional de datos pueda considerarse conforme a lo dispuesto en la LOPD, y en el propio

Reglamento, será necesaria la autorización del Director de la Agencia Española de Protección de Datos, que se otorgará en caso de que el exportador aporte las garantías a las que se refiere el artículo 70 del mismo reglamento. Según este artículo, la autorización podrá ser otorgada en caso de que el responsable del fichero o tratamiento aporte un contrato escrito, celebrado entre el exportador y el importador, en el que consten las necesarias garantías de respeto a la protección de la vida privada de los afectados y a sus derechos y libertades fundamentales y se garantice el ejercicio de sus respectivos derechos. A tal efecto, se considerará que establecen las adecuadas garantías los contratos que se celebren de acuerdo con lo previsto en las Decisiones de la Comisión Europea que den cumplimiento a lo establecido en el artículo 26.4 de la Directiva 95/46/CE. También podrá otorgarse la autorización para la transferencia internacional de datos en el seno de grupos multinacionales de empresas cuando hubiesen sido adoptados por los mismos normas o reglas internas en que consten las necesarias garantías de respeto a la protección de la vida privada y el derecho fundamental a la protección de datos de los afectados y se garantice asimismo el cumplimiento de los principios y el ejercicio de los derechos reconocidos en la LOPD y el propio reglamento.

1.1. INICIACIÓN DEL PROCEDIMIENTO

La iniciación del procedimiento para la obtención de la autorización de las transferencias internacionales de datos a países terceros a las que se refieren el artículo 33 de la LOPD y el 70 del RLOPD viene regulada en el artículo 137 del RLOPD[210].

[210] Como señala el artículo 115.1 del RLOPD, los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el Título IX del mismo Reglamento, y

Según se indica en este artículo, la tramitación se iniciará siempre a solicitud del exportador[211] que pretenda llevar a cabo la transferencia (el importador no jugará ningún papel en el procedimiento)[212].

En su solicitud, además de los requisitos legalmente exigidos, el exportador deberá consignar, en todo caso:

a) La identificación del fichero o ficheros a cuyos datos se refiera la transferencia internacional, con indicación de su denominación y código de inscripción del fichero[213] en el Registro General de Protección de Datos.

b) La transferencia o transferencias respecto de las que se solicita la autorización, con indicación de la finalidad que la justifica.

c) La documentación que incorpore las garantías exigibles para la obtención de la autorización[214] así como el cumplimiento de los requisitos legales necesarios para la realización de la transferencia, en su caso[215].

---

supletoriamente, por la LRJAP. En el mismo sentido se pronuncia el artículo 35.2 de la LOPD cuando manifiesta que "en el ejercicio de sus funciones públicas, y en defecto de lo que disponga la presente Ley y sus disposiciones de desarrollo, la Agencia Española de Protección de Datos actuará de conformidad con la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común**".**

[211] En el artículo 5 del RLOPD, sobre definiciones, se define al exportador de datos personales como la persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español que realice, conforme a lo dispuesto en el Reglamento, una transferencia de datos de carácter personal a un país tercero.

[212] En este sentido, el Reglamento obliga a algo que la LOPD no había concretado. En el artículo 33.1 de la Ley solamente se exige que *se obtenga* autorización previa del Director de la Agencia Española de Protección de Datos, pero no hace mención de quien es el obligado a efectuar la solicitud.

[213] Este apartado tiene su razón de ser en el caso de que se solicite una transferencia internacional sobre los datos contenidos en un fichero ya inscrito anteriormente. Si el fichero todavía no está inscrito lógicamente no se podrán aportar estos datos.

Cuando la autorización se fundamente en la existencia de un contrato entre el exportador y el importador de los datos, deberá aportarse copia del mismo, acreditándose asimismo la concurrencia de poder suficiente en sus otorgantes. Tal como indica el artículo 70.2 del RLOPD, se considerará que establecen las adecuadas garantías los contratos que se celebren de acuerdo con lo previsto en las Decisiones de

[214] Según el artículo 70.2 del RLOPD la autorización podrá ser otorgada en caso de que el responsable del fichero o tratamiento aporte un contrato escrito, celebrado entre el exportador y el importador, en el que consten las necesarias garantías de respeto a la protección de la vida privada de los afectados y a sus derechos y libertades fundamentales y se garantice el ejercicio de sus respectivos derechos.

El artículo 70.4 del RLOPD indica que también podrá otorgarse la autorización para la transferencia internacional de datos en el seno de grupos multinacionales de empresas cuando hubiesen sido adoptados por los mismos normas o reglas internas en que consten las necesarias garantías de respeto a la protección de la vida privada y el derecho fundamental a la protección de datos de los afectados y se garantice asimismo el cumplimiento de los principios y el ejercicio de los derechos reconocidos en la Ley Orgánica 15/1999, de 13 de diciembre, y el propio Reglamento.

[215] Según queda de manifiesto en el artículo 65 del RLOPD, la transferencia internacional de datos no excluye en ningún caso la aplicación de las disposiciones contenidas en la Ley Orgánica 15/1999 y en el propio Reglamento (entre otras podemos citar la notificación del fichero, las obligaciones de información y las medidas de seguridad). Cuestión distinta es la interpretación extensiva que ha dado la AEPD al cumplimiento de los requisitos legales necesarios para la realización de la transferencia. En el documento de la Agencia, disponible en su página web, titulado "Informe sobre transferencias internacionales de datos. Inspección sectorial de oficio España-Colombia en centros de atención al cliente. Julio 2007", en el apartado de "Novedades procedimentales" da su punto de vista a lo que entiende por cumplimiento de las obligaciones legales: "Como condición previa a la realización de una transferencia internacional de datos el exportador de los datos debe cumplir con el resto de obligaciones que establece la normativa de protección de datos, y cualquiera otra que pudiera resultar de aplicación. Un caso paradigmático se da cuando la transferencia de datos puede afectar a otros derechos de los trabajadores. En este caso se deberá tener en cuenta el cumplimiento de las obligaciones relacionadas con el derecho laboral y, en particular, la obligación de informar al comité de empresa de acuerdo con el art. 42.4 del Estatuto de los Trabajadores (RDL 1/1995, de 24 de marzo) en relación con la transposición de la Directiva 2002/14/CE, por la que se establece un marco general relativo a la información y a la consulta de los trabajadores en la Comunidad Europea".

la Comisión Europea 2001/497/CE, de 15 de Junio de 2001, 2002/16/CE[216], de 27 de diciembre de 2001, y 2004/915/CE, de 27 de diciembre de 2004 o de lo que dispongan las Decisiones de la Comisión que den cumplimiento a lo establecido en el artículo 26.4 de la Directiva 95/46/CE.

Si la autorización se pretendiera fundar en lo dispuesto en el apartado 4 del artículo 70 del RLOPD, deberán aportarse las normas o reglas adoptadas en relación con el tratamiento de los datos en el seno del grupo, así como la documentación que acredite su carácter vinculante y su eficacia dentro del grupo. Igualmente deberá aportarse la documentación que acredite la posibilidad de que el afectado o la Agencia Española de Protección de Datos puedan exigir la responsabilidad que corresponda en caso de perjuicio del afectado o vulneración de las normas de protección de datos por parte de cualquier empresa importadora.

1.2. INSTRUCCIÓN DEL PROCEDIMIENTO Y DURACIÓN DEL MISMO

De acuerdo al artículo 26.2.b del Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos, corresponde al Registro General de Protección de Datos la instrucción de los expedientes de autorización de las transferencias internacionales de datos.

La instrucción del procedimiento viene regulada en el artículo 138 del RLOPD. Según se indica en este artículo, cuando el Director de la Agencia Española de

[216] A fecha de hoy debemos incluir la Decisión de la Comisión 2010/87/UE, que deroga la previa Decisión 2002/16/CE.

Protección de Datos acuerde, conforme a lo dispuesto en el artículo 86.1[217] de la LRJAP, la apertura de un período de información pública, el plazo para la formulación de alegaciones será de diez días a contar desde la publicación en el Boletín Oficial del Estado del anuncio previsto en dicha Ley.

El plazo de diez días para la formulación de alegaciones es más reducido que el que establece con carácter general la LRJAP[218]. De acuerdo a su artículo 86.2, "se anunciará en el Boletín Oficial del Estado, de la Comunidad Autónoma, o en el de la Provincia respectiva, a fin de que cualquier persona física o jurídica pueda examinar el procedimiento, o la parte del mismo que se acuerde. El anuncio señalará el lugar de exhibición y determinará el plazo para formular alegaciones, que en ningún caso podrá ser inferior a *veinte días*".

Según el artículo 37.5 de la LRJAP, "el derecho de acceso no podrá ser ejercido respecto a los siguientes expedientes:

A) Los que contengan información sobre las actuaciones del Gobierno del Estado o de las Comunidades Autónomas, en el ejercicio de sus competencias constitucionales no sujetas a Derecho Administrativo.

[217] El artículo 86.1 de la LRJAP, regula que "el órgano al que corresponda la resolución del procedimiento, cuando la naturaleza de éste lo requiera, podrá acordar un período de información pública".

[218] En el documento de la Agencia, disponible en su página web, titulado "Informe sobre transferencias internacionales de datos. Inspección sectorial de oficio España-Colombia en centros de atención al cliente. Julio 2007", se hace constar que, "dado que el plazo de información pública que establece el art. 86.1 de la LRJAP es de 20 días, lo que dificulta a la Agencia la tramitación del expediente en el plazo legalmente establecido, se ha propuesto la introducción en el Proyecto de Reglamento de desarrollo de la LOPD que está tramitando el Ministerio de Justicia, la aplicación del art. 86.4 para reducir el plazo de información pública a 10 días".

B) Los que contengan información sobre la Defensa Nacional o la Seguridad del Estado.

C) Los tramitados para la investigación de los delitos cuando pudiera ponerse en peligro la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando.

D) Los relativos a las materias protegidas por el secreto comercial o industrial.

E) Los relativos a actuaciones administrativas derivadas de la política monetaria".

Transcurrido el plazo de diez días antes mencionado, en caso de que se hubieran formulado alegaciones, se dará traslado de las mismas al solicitante de la autorización, a fin de que en el plazo de diez días alegue lo que estime procedente.

La autorización puede ser denegada por el Director de la AEPD en base al artículo 70.3 del RLOPD, es decir cuando concurra alguna de las circunstancias siguientes:

"a) Que la situación de protección de los derechos fundamentales y libertades públicas en el país de destino o su legislación impidan garantizar el íntegro cumplimiento del contrato y el ejercicio por los afectados de los derechos que el contrato garantiza.

b) Que la entidad destinataria haya incumplido previamente las garantías establecidas en cláusulas contractuales de este tipo.

c) Que existan indicios racionales de que las garantías ofrecidas por el contrato no están siendo o no serán respetadas por el importador.

d) Que existan indicios racionales de que los mecanismos de aplicación del contrato no son o no serán efectivos.

e) Que la transferencia, o su continuación, en caso de haberse iniciado, pudiera crear una situación de riesgo de daño efectivo a los afectados".

Tal como indica el artículo 140 del RLOPD, el plazo máximo para dictar y notificar resolución será de tres meses[219], a contar desde la fecha de entrada en la Agencia Española de Protección de Datos de la solicitud. Si en dicho plazo no se hubiese dictado y notificado resolución expresa, se entenderá autorizada la transferencia internacional de datos.

Nos encontramos en este caso ante un silencio administrativo positivo. Como dispone el artículo 43.3.a) de la LRJAP, en los casos de estimación por silencio administrativo, la resolución expresa posterior a la producción del acto sólo podrá dictarse de ser confirmatoria del mismo.

Por otra parte, y como regula el artículo 43.4 de la LRJAP, "los actos administrativos producidos por silencio administrativo se podrán hacer valer tanto ante la Administración como ante cualquier persona física o jurídica, pública o privada. Los mismos producen efectos desde el vencimiento del plazo máximo en el que debe dictarse y notificarse la resolución expresa sin que la misma se haya producido, y su existencia puede ser acreditada por cualquier medio de prueba admitido en Derecho, incluido el certificado acreditativo del silencio producido que pudiera solicitarse del órgano competente para resolver. Solicitado el certificado, éste deberá emitirse en el plazo máximo de quince días".

[219] Plazo que coincide con el regulado en el artículo 42.3 del la LRJAP para el caso en que las normas reguladoras de los procedimientos no fijen un plazo máximo.

1.3. ACTOS POSTERIORES A LA RESOLUCIÓN

La autorización o denegación de la transferencia internacional de datos deberá notificarse al solicitante de la autorización. Tal como indica el artículo 139 del RLOPD, cuando el Director de la Agencia Española de Protección de Datos resuelva autorizar la transferencia internacional de datos, se dará traslado de la resolución de autorización al Registro General de Protección de Datos, a fin de proceder a su inscripción[220].

El Registro General de Protección de Datos inscribirá de oficio la autorización de transferencia internacional y se dará traslado de la resolución de autorización o denegación de la autorización de la transferencia internacional de datos al Ministerio de Justicia, al efecto de que se proceda a su notificación a la Comisión Europea y a los demás Estados miembros de la Unión Europea de acuerdo a lo previsto en el artículo 26.3 de la Directiva 95/46/CE[221].

Como dispone el artículo 37.2 de la LOPD, las resoluciones de la Agencia Española de Protección de Datos se harán públicas, una vez hayan sido notificadas a los

[220] Tal como indica el artículo 25 del Real Decreto 428/1993, que versa sobre actos y documentos inscribibles, se inscribirán en el Registro General de Protección de Datos las autorizaciones de transferencia de datos personales a otros países, en los casos en que, a tenor de lo dispuesto en el artículo 32 de la Ley Orgánica 5/1992, de 29 de octubre, sea preceptiva para la transferencia la autorización previa del Director. Se regula la materia en el mismo sentido en el artículo 39.2 de la LOPD, según el cual serán objeto de inscripción en el Registro General de Protección de Datos las autorizaciones a que se refiere la propia Ley.

[221] El artículo 26.3 de la Directiva 95/46/CE obliga a los Estados miembros a informar a la Comisión y a los demás Estados miembros acerca de las autorizaciones que concedan. En el supuesto de que otro Estado miembro o la Comisión expresaren su oposición y la justificaren debidamente por motivos derivados de la protección de la vida privada y de los derechos y libertades fundamentales de las personas, la Comisión adoptará las medidas adecuadas con arreglo al procedimiento establecido en el apartado 2 del artículo 31 de la Directiva.

interesados. La publicación se realizará preferentemente a través de medios informáticos o telemáticos. En el artículo 116 del RLOPD se desarrolla el contenido del anterior artículo de la Ley en los siguientes términos: "la publicación de estas resoluciones se realizará preferentemente mediante su inserción en el sitio web de la Agencia Española de Protección de Datos, dentro del plazo de un mes a contar desde la fecha de su notificación a los interesados. En la notificación de las resoluciones se informará expresamente a los interesados de la publicidad prevista en el artículo 37.2 de la Ley Orgánica 15/1999, de 13 de diciembre".

A este tipo de procedimiento le pueden quedar los días contados. De acuerdo a la propuesta de Reglamento de protección de datos de la UE, una transferencia efectuada en virtud de cláusulas tipo de protección de datos (ya hayan sido adoptadas por la Comisión o bien por una autoridad de control), no requerirá nuevas autorizaciones. Sólo en el caso de cláusulas contractuales entre el responsable o el encargado del tratamiento y el destinatario de los datos, que no se correspondan a los modelos anteriores, deberían ser autorizadas por una autoridad de control (art. 42.2 y 42.3).

2. PROCEDIMIENTO DE SUSPENSIÓN TEMPORAL DE TRANSFERENCIAS INTERNACIONALES DE DATOS

De acuerdo al artículo 69 del RLOPD, el Director de la Agencia Española de Protección de Datos, en uso de la potestad que le otorgan el artículo 37.1 f)[222] de la

[222] El artículo 37.1 f) de la LOPD expone que una de las funciones de la Agencia Española de Protección de Datos es la de requerir a los responsables y los encargados de los tratamientos, previa audiencia de éstos, la adopción de las medidas necesarias para la adecuación del tratamiento de datos a las disposiciones de la LOPD y, en su caso, ordenar la cesación de los tratamientos y la cancelación de los ficheros, cuando no se ajuste a sus disposiciones.

LOPD y el artículo 28.3[223] de la Directiva 95/46/CE, podrá acordar, previa audiencia del exportador, la suspensión temporal de la transferencia de datos hacia un importador ubicado en un tercer Estado del que se haya declarado la existencia de un nivel adecuado de protección, cuando concurra alguna de las circunstancias siguientes[224]:

"a) Que las autoridades de Protección de Datos del Estado importador o cualquier otra competente, en caso de no existir las primeras, resuelvan que el importador ha vulnerado las normas de protección de datos establecidas en su derecho interno.

[223] El artículo 28.3 de la Directiva 95/46/CE otorga poderes efectivos de intervención a la autoridad de control, como, por ejemplo, el de formular dictámenes antes de realizar los tratamientos, con arreglo al artículo 20, y garantizar una publicación adecuada de dichos dictámenes, o el de ordenar el bloqueo, la supresión o la destrucción de datos, o incluso prohibir provisional o definitivamente un tratamiento, o el de dirigir una advertencia o amonestación al responsable del tratamiento o el de someter la cuestión a los parlamentos u otras instituciones políticas nacionales.

[224] Esta redacción es muy similar a la usada en el punto 2 de la Norma Cuarta de la Instrucción 1/2000: "Sin perjuicio de lo dispuesto en la Norma Segunda, el Director de la Agencia de Protección de Datos, en uso de la potestad que le otorga el artículo 37 f) de la Ley Orgánica 15/1999, podrá acordar, previa audiencia del transmitente, la suspensión temporal de la transferencia de datos hacia un receptor ubicado en un tercer Estado del que se haya declarado la existencia de un nivel adecuado de protección, cuando concurra alguna de las circunstancias siguientes, previstas en las Decisiones de la Comisión de las Comunidades Europeas:

* Que las Autoridades de Protección de Datos del Estado destinatario o cualquier otra, en caso de no existir las primeras, resuelvan que el destinatario ha vulnerado las normas de protección de datos de su derecho interno.

* Que existan indicios racionales de que se estén vulnerando las normas o, en su caso, los principios de protección de datos por la entidad destinataria de la transferencia y que las autoridades competentes en el Estado en que se encuentre el destinatario no han adoptado o no van a adoptar en el futuro las medidas oportunas para resolver el caso en cuestión, habiendo sido advertidas de la situación por la Agencia de Protección de Datos. En este caso se podrá suspender la transferencia cuando su continuación pudiera generar un riesgo inminente de grave perjuicio a los afectados.

En estos casos, la decisión del Director de la Agencia de Protección de Datos será notificada a la Comisión de las Comunidades Europeas".

b) Que existan indicios racionales de que se estén vulnerando las normas o, en su caso, los principios de protección de datos por la entidad importadora de la transferencia y que las autoridades competentes en el Estado en que se encuentre el importador no han adoptado o no van a adoptar en el futuro las medidas oportunas para resolver el caso en cuestión, habiendo sido advertidas de la situación por la Agencia Española de Protección de Datos. En este caso se podrá suspender la transferencia cuando su continuación pudiera generar un riesgo inminente de grave perjuicio a los afectados".

La suspensión se acordará previa la tramitación del procedimiento establecido en la sección segunda del capítulo V del título IX del RLOPD. Cuando se produzca esta circunstancia, la decisión del Director de la AEPD será notificada a la Unión Europea.

En el caso de las transferencias a Estados que no proporcionen un nivel adecuado de protección, el artículo 70.3 del RLOPD faculta al Director de la Agencia Española de Protección de Datos para denegar o, en uso de la potestad que le otorgan el artículo 37.1 f) de la LOPD y el artículo 28.3 de la Directiva 95/46/CE, suspender temporalmente[225],

[225] Según el artículo 4.1 de la Decisión de la Comisión 2001/497/CE (de redacción casi idéntica al artículo 4.1 de la Decisión de la Comisión 2010/87/UE**),** sobre cláusulas contractuales tipo, las autoridades competentes de los Estados miembros, sin perjuicio de su facultad para iniciar acciones destinadas a garantizar el cumplimiento de las disposiciones Derecho nacional adoptadas con arreglo a los capítulos II, III, V y VI de la Directiva 95/46/CE, podrán ejercer sus facultades para prohibir o suspender los flujos de datos hacia terceros países con objeto de proteger a las personas físicas relación con el tratamiento de sus datos personales en los siguientes casos:

a) si se determina que la legislación a la que está sujeto el importador de datos le impone desviaciones de las normas correspondientes sobre protección de datos que vayan más allá de las restricciones necesarias en una sociedad democrática, como establece el artículo 13 de la Directiva 95/46/CE, cuando tales exigencias puedan tener un importante efecto negativo sobre las garantías proporcionadas por las cláusulas contractuales tipo; o

b) si una autoridad competente decide que el importador de datos no ha respetado las cláusulas contractuales; o

previa audiencia del exportador, la transferencia, cuando concurra alguna de las circunstancias siguientes[226]:

"a) Que la situación de protección de los derechos fundamentales y libertades públicas en el país de destino o su legislación impidan garantizar el íntegro cumplimiento del contrato y el ejercicio por los afectados de los derechos que el contrato garantiza.

b) Que la entidad destinataria haya incumplido previamente las garantías establecidas en cláusulas contractuales de este tipo.

c) Que existan indicios racionales de que las garantías ofrecidas por el contrato no están siendo o no serán respetadas por el importador.

d) Que existan indicios racionales de que los mecanismos de aplicación del contrato no son o no serán efectivos.

e) Que la transferencia, o su continuación, en caso de haberse iniciado, pudiera crear una situación de riesgo de daño efectivo a los afectados".

La suspensión se acordará previa la tramitación del procedimiento establecido en la sección segunda del capítulo V del título IX del RLOPD. Las resoluciones del Director de la AEPD por las que se deniegue o suspenda una transferencia internacional de datos en virtud de las causas arriba mencionadas serán notificadas a la Comisión de las Unión Europea cuando así sea exigible.

---

c) si existe la probabilidad sustancial de que las cláusulas contractuales tipo contenidas en el anexo no se estén respetando, o no se respeten en el futuro, y la continuación de la transferencia provoque un riesgo inminente de daños graves para los interesados.

[226] El contenido del artículo 70.3 del RLOPD es casi idéntico al del punto 7 de la Norma Quinta de la Instrucción 1/2000.

En el artículo 141 del RLOPD se expone la iniciación del procedimiento de suspensión temporal de transferencias internacionales de datos en los supuestos contemplados en el artículo 69 y en el apartado 3 del artículo 70. En tales circunstancias, el Director de la AEPD dictará acuerdo de inicio referido a la suspensión de la transferencia internacional. Dicho acuerdo deberá ser motivado y fundarse en las causas previstas en el propio RLOPD.

El artículo 142 del RLOPD, sobre instrucción y resolución del procedimiento de suspensión temporal, exige se dé "traslado del acuerdo al exportador, a fin de que en el plazo de quince días formule lo que a su derecho convenga". Una vez "recibidas las alegaciones o cumplido el plazo señalado, el Director dictará resolución acordando, en su caso, la suspensión temporal de la transferencia internacional de datos".

No se indica en el artículo 142 el plazo máximo en el que se deberá dictar la resolución, por lo que entrará en juego, como norma de aplicación subsidiaria, la LRJAP. En el artículo 42 de dicha Ley se señala que cuando las normas reguladoras de los procedimientos no fijen el plazo máximo, éste será de tres meses. Este plazo se contará en los procedimientos iniciados de oficio, desde la fecha del acuerdo de iniciación.

Tampoco hace referencia el artículo 142 del RLOPD a la falta de resolución expresa en este procedimiento. Deberemos encontrar de nuevo la respuesta en la LRJAP. En su artículo 44.2 regula que, ante la falta de resolución expresa en procedimientos iniciados de oficio, en que la Administración ejercite potestades sancionadoras o, en general, de intervención, susceptibles de producir efectos

desfavorables o de gravamen, se producirá la caducidad. En estos casos, la resolución que declare la caducidad ordenará el archivo de las actuaciones.

Según el artículo 143 del RLOPD, sobre actos posteriores a la resolución, el Director de la AEPD dará traslado de la resolución al Registro General de Protección de Datos, a fin de que la misma se haga constar en el registro. Éste deberá inscribir de oficio la suspensión temporal de la transferencia internacional. También se dará traslado de la resolución al Ministerio de Justicia, al efecto de que se proceda a su notificación a la Comisión Europea y a los demás Estados miembros de la Unión de acuerdo a lo previsto en el artículo 26.3[227] de la Directiva 95/46/CE.

La obligación de notificar las suspensiones también se regula en las Decisiones de la Comisión 2001/497/CE y 2010/87/UE**,** sobre cláusulas contractuales tipo. Tal como se había indicado anteriormente, en el artículo 4.1 de las dos Decisiones se faculta a las autoridades competentes de los Estados miembros para prohibir o suspender los flujos de datos hacia terceros países. En ambas Decisiones se exige a las autoridades de los Estados miembros a informar a la Comisión de los acuerdos de suspensión. La Comisión por su parte se encargará de informar al resto de los Estados miembros de dichos acuerdos.

[227] El artículo 26.3 de la Directiva obliga a los Estados miembros a informar a la Comisión y a los demás Estados miembros acerca de las autorizaciones que concedan para la realización de una transferencia o una serie de transferencias de datos personales a un tercer país que no garantice un nivel de protección adecuado. Dicho artículo no hace referencia alguna a la obligación de los Estados miembros a informar de las suspensiones temporales de las transferencias internacionales de datos. Sin embargo el RLOPD le ha dado un sentido más amplio que el que literal: si se exige en la Directiva la información sobre las autorizaciones que se concedan, también habrá que informar de aquellos cambios que se produzcan posteriormente que tengan incidencia sobre la autorización inicial que se otorgó.

Sin embargo la obligación de notificar las suspensiones que se regula en las Decisiones de la Comisión sobre cláusulas contractuales tipo debemos entender que sólo afectaría a aquellas transferencias internacionales de datos que se hayan basado en aquellas Decisiones para poderse llevar a cabo. No obligaría por lo tanto a las transferencias internacionales de datos que no hayan hecho uso de las mismas.

En el artículo 144 del RLOPD se contempla el levantamiento de la suspensión temporal de transferencias internacionales de datos: "La suspensión se levantará tan pronto como cesen las causas que la hubieran justificado[228], mediante resolución del Director de la Agencia Española de Protección de Datos, del que se dará traslado al exportador". Y de la misma forma que antes se había actuado para la suspensión se deberá proceder ante el levantamiento de la suspensión: "El Director de la Agencia Española de Protección de Datos dará traslado de la resolución al Registro General de Protección de Datos, a fin de que la misma se haga constar en el Registro. El Registro General de Protección de Datos hará constar de oficio el levantamiento de la suspensión temporal de la transferencia internacional".

La notificación del acuerdo deberá efectuarse tanto al exportador de datos personales como "al Ministerio de Justicia, al efecto de que se proceda a su notificación a la Comisión Europea y a los demás Estados miembros de la Unión Europea de acuerdo a lo previsto en el artículo 26.3 de la Directiva 95/46/CE".

En el artículo 53.1.h) del proyecto de Reglamento de protección de datos de la UE se continúa manteniendo la potestad de las autoridades de control para suspender los

[228] Similar redactado se ha dado en el artículo 4.2 de la Decisión 2001/497/CE y en el mismo artículo de la Decisión 2010/87/UE: La prohibición o suspensión se levantará tan pronto como desaparezcan las razones para dicha prohibición o suspensión.

flujos de datos hacia un destinatario situado en un tercer país o hacia una organización internacional.

3. LAS TRANSFERENCIAS INTERNACIONALES DE DATOS AUTORIZADAS POR LA AEPD

El fenómeno de la globalización combinado con el avance de las tecnologías de la información y especialmente el desarrollo de internet, ha llevado a un incremento muy elevado de los flujos transfronterizos de datos personales. Este incremento en los movimientos internacionales de datos, junto con una concienciación cada vez mayor de las empresas en la necesidad de cumplir con las exigencias de la normativa de protección de datos, ha supuesto un aumento espectacular en el número de transferencias internacionales declaradas. Aún así, hay muchos especialistas que tienen la opinión de que el número de transferencias declaradas es irrisorio[229] sobre el movimiento internacional de datos que se produce en la realidad[230]. Posiblemente

[229] Hay que tener en cuenta que el régimen sancionador penaliza duramente las transferencias ilegales de datos, lo que en principio debería constituir un aliciente al respeto de la legalidad. Según el artículo 44.4.d) de la LOPD es una infracción muy grave la transferencia internacional de datos de carácter personal con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Director de la Agencia Española de Protección de Datos salvo en los supuestos en los que conforme a esta Ley y sus disposiciones de desarrollo dicha autorización no resulta necesaria. Tal como indica el artículo 45.3, las infracciones muy graves serán sancionadas con multa de 300.001 a 600.000 euros.

[230] Es muy interesante el artículo de Jordi Saldaña publicado el dos de marzo de 2012 en el portal jurídico "legaltoday.com". Según la opinión del señor Saldaña cuesta creer que tan solo 100 empresas en el año 2011 realizaran transferencias internacionales de datos. Uno de los motivos por los que cree que se solicitan tan pocas autorizaciones es el régimen jurídico aplicable a las transferencias internacionales a países con un nivel de protección no equiparable. La gran inversión en tiempo y dinero que supone la solicitud produce un efecto disuasorio cuya consecuencia es que el responsable renuncia antes de haberse planteado siquiera empezar con la tramitación.

influyen las causas manifestadas en la Exposición de Motivos de la Propuesta de 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 (Reglamento general de protección de datos)[231]: "Se considera que la complejidad de las normas en materia de transferencias internacionales de datos personales constituye un impedimento sustancial a su funcionamiento, ya que se necesita transferir con regularidad datos personales de la UE a otras partes del mundo".

Es también interesante el comentario que se efectúa en la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de la Regiones, titulado "La protección de la privacidad en un mundo interconectado - Un marco europeo de protección de datos para el siglo XXI"[232]: "La circulación legítima de datos a terceros países se facilitará reforzando y simplificando las normas sobre transferencias internacionales de datos a los países no cubiertos por ninguna decisión de adecuación, y sobre todo racionalizando ciertas herramientas (como por ejemplo las normas corporativas vinculantes) y generalizando su uso, de forma que puedan aplicarse a los responsables del tratamiento de datos y dentro de los grupos de sociedades, lo que reflejará mejor el número de empresas que llevan a cabo actividades de tratamiento de datos, especialmente mediante computación en nube".

[231] Bruselas, 25.1.2012 COM(2012) 11 final.

[232] Bruselas, 25.1.2012 COM(2012) 9 final.

Si volvemos al marco nacional, en las notificaciones de ficheros que son inscritos en el Registro General de Protección de Datos se han declarado las siguientes transferencias internacionales de datos (cifras presentadas de forma acumulativa)[233]:

Hasta 31.12.2002	2.614 transferencias
Hasta 31.12.2003	3.493 transferencias
Hasta 31.12.2004	5.124 transferencias
Hasta 31.12.2005	6.945 transferencias
Hasta 31.12.2006	8.311 transferencias
Hasta 01.07.2007	8.483 transferencias

Tal como hace constar la AEPD, en las cifras indicadas se incluyen las comunicaciones de datos notificadas al Registro que tienen como destino los países del Acuerdo sobre el Espacio Económico Europeo, y los que han sido considerados por la Comisión Europea con un nivel adecuado de protección en aplicación de la Directiva 95/46/CE. Comprenden también las que no teniendo como destino un país con nivel adecuado de protección, se encuentran amparadas en las excepciones previstas en el artículo 34 de la LOPD. Se incluyen, por último, las que han requerido la Autorización del Director de la Agencia, que a uno de julio de 2007 ascendían a 148 transferencias.

Si nos centramos en las transferencias que han requerido la autorización del Director de la AEPD, las finalidades para las que mayoritariamente se realizan son las dos siguientes[234]:

[233] Agencia Española de Protección de Datos. Informe sobre transferencias internacionales de datos. Inspección sectorial de oficio España-Colombia en centros de atención al cliente. Julio 2007. Pág. 5.

[234] Finalidades recogidas en el documento: Agencia Española de Protección de Datos. Informe sobre transferencias internacionales de datos. Inspección sectorial de oficio España-Colombia en centros de atención al cliente. Julio 2007. Pág. 6 y 7. Dichas finalidades principales se clasifican de forma diferente

- Fines relacionados con necesidades propias de la gestión empresarial en un contexto global. Las empresas multinacionales requieren la realización de transferencias internacionales de datos para finalidades tales como la gestión, mantenimiento y soporte técnico de los sistemas de información. Por otra parte se solicitan estas autorizaciones en relación con la gestión eficiente de los recursos humanos, los clientes y los proveedores, así como la prestación de servicios de apoyo administrativo en relación con estos. En esta categoría de transferencias internacionales se encuentra más de la mitad de las autorizaciones otorgadas por la Agencia, que están relacionadas con grupos multinacionales que tienen su empresa matriz fuera de España, principalmente en los Estados Unidos de América, y su actividad empresarial distribuida por diferentes países. A modo de ejemplo, se puede citar la gestión global de personal en compañías internacionales.

- La atención telefónica a los clientes, y otras acciones de marketing telefónico dirigidas a mejorar el grado de satisfacción de los mismos, como la gestión centralizada de los servicios de atención al cliente.

---

en el documento de la AEPD "El Procedimiento de Autorización de Transferencias. Jornada sobre transferencias internacionales de datos. Madrid, 18 de julio de 2007":

- Atención telefónica a los clientes.
- Acciones de marketing telefónico dirigidas a la medición del grado de satisfacción de los clientes.
- Centralización de la gestión de recursos humanos y de proyectos internacionales en el marco de una compañía multinacional.
- Gestión, mantenimiento y soporte técnico de las bases de datos de clientes y proveedores y como parte de una política global del Grupo.
- Prestación de servicios de apoyo administrativo a efectos de beneficiarse de economías de escala, así como de una creciente calidad del servicio, oportunidad y exactitud en virtud de una iniciativa global.

Si diferenciamos las transferencias internacionales de datos en función del modelo de cláusulas contractuales empleado, las 137 autorizaciones de transferencia internacional se repartieron de la forma siguiente[235]:

MODELO	2002	2003	2004	2005	2006	2007	TOTAL
Responsable-Encargado	4	3	27	13	43	15	105
Responsable-Responsable	-	3	20	3	3	3	32

Si atendemos a cifras más recientes, en la Memoria de 2011 de la AEPD se informa del total de transferencias autorizadas hasta el final de dicho ejercicio: 735. La distribución anual de dichas autorizaciones es la siguiente:

2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011
2	9	2	6	47	19	46	43	103	128	155	175

Se puede observar con facilidad que el número de transferencias autorizadas se ha incrementado especialmente desde 2008. A 31-12-2010 los países destinatarios de las transferencias de datos son clasificados por la AEPD de la forma siguiente:

[235] Documento de la AEPD: El Procedimiento de Autorización de Transferencias. Jornada sobre transferencias internacionales de datos. Madrid, 18 de julio de 2007.

Destino	Autorizaciones
Estados Unidos	177
India	81
Latinoamérica	220
Otros países	110

Centrándonos en Latinoamérica, los países de destino con mayor número de transferencias autorizadas a 31-12-2010 son los siguientes:

Destino	Autorizaciones
Colombia	52
Chile	35
México	31
Paraguay	11
Perú	52
Uruguay	23

Como hace constar la AEPD en su Memoria anual de 2010, además de observarse un crecimiento elevado en el número de transferencias en los últimos años, se está

produciendo un desplazamiento rápido de dichas transferencias hacia países emergentes, lo que está determinando una diversificación geográfica de los destinatarios de transferencias internacionales de datos.

Dentro de esa tendencia, en el año 2010 se efectuaron 88 solicitudes de exportación de datos hacia Latinoamérica, mientras que hacia Estados Unidos hubo 25 solicitudes y con destino a Asia fueron 23. Los países latinoamericanos se están consolidando como el principal foco de flujos internacionales de datos desde España. Hasta 31-12-2010 contaban con un total de 220 autorizaciones.

Si se añaden a las aún mayores (377) realizadas a la República Argentina, país en el que, al estar calificado como de nivel adecuado de protección por la Comisión Europea, no es necesaria la autorización, sino sólo la notificación al RGPD, observamos que la concentración de las transferencias en los países latinoamericanos es creciente.

Dentro de los países latinoamericanos ocupan un papel destacado Colombia, Chile, México, Perú y Uruguay. Estos países han aprobado ya o están en proceso de hacerlo leyes específicas sobre protección de datos personales.

En el caso de Uruguay ha obtenido la Decisión de Adecuación de la Comisión Europea 2012/484/UE, de 21 de agosto de 2012 (DOUE L 227 de 23 de agosto de 2012).

Podríamos verificar la distribución de las transferencias internacionales en los últimos años en función del tipo de contrato empleado (responsable-responsable o responsable-encargado). Para ello analizaremos la información que aparece en el

documento titulado "Transferencias internacionales de datos", del señor Jesús Rubí Navarrete, Adjunto al Director de la AEPD[236] (datos acumulativos):

MODELO	31-12-2008	31-12-2009	31-12-2010	31-03-2011
Responsable-Encargado	216	328	475	526
Responsable-Responsable	50	66	80	82

Si pasamos al estudio de un documento más reciente de la AEPD, "El régimen de transferencias internacionales de datos a encargados de tratamiento[237]", se informa de que a 31-12-2011 el volumen de transferencias autorizadas ya asciende a 735. De ese total, 619 autorizaciones corresponden a transferencias de responsables de fichero a encargado de tratamiento (es decir un 84'2% del total). Llama la atención de que solamente el 68'8% de estas últimas autorizaciones están basadas en la Decisión 2002/16/CE, mientras que el 31'1% de las mismas se basan ya en la Decisión 2010/87/UE, a pesar de que ha entrado en vigor en fecha muy reciente.

4. SISTEMAS DE DENUNCIAS INTERNAS EN LAS EMPRESAS

En lo que resta de este apartado vamos a analizar cuatro casos de conflicto con el debido respeto a la regulación de las transferencias internacionales de datos de la

[236] Documento elaborado en el marco del seminario "El impacto de las trasferencias internacionales de datos en América Latina. Las políticas preventivas y la autorregulación en la implantación de la normativa de protección de datos" celebrado los días 14 al 16 de junio del 2011, en Cartagena de Indias.

[237] Documento elaborado por doña María José Blanco Antón, Subdirectora General del Registro General de Protección de Datos, para la "Cuarta sesión anual abierta de la AEPD", celebrada en Madrid el 27 de enero de 2012.

Directiva 95/46/CE y las normas nacionales que la transponen. El primer caso de conflicto que estudiaremos lo encontramos en los sistemas de denuncias internas en las empresas.

La ley Sarbanes-Oxley (SOX) fue adoptada por el Congreso de los Estados Unidos en 2002 a raíz de diversos escándalos financieros protagonizados por empresas.

La SOX exige que las empresas públicas de los EE.UU. y sus filiales en la UE, así como las empresas no estadounidenses que cotizan en bolsa en los EE.UU., establezcan, en su comité de auditoría, "procedimientos para la recepción, conservación y tramitación de las denuncias recibidas por el emisor relativas a la contabilidad, las auditorías internas o las cuestiones de auditoría; así como para la presentación confidencial y anónima por parte de los empleados del emisor de situaciones relativas a cuestiones de contabilidad o auditoría cuestionables". Además, el artículo 806 de la SOX establece una disposición dirigida a garantizar la protección de los empleados de empresas que cotizan en bolsa que proporcionen pruebas de fraude frente a las represalias que pudieran tomarse contra ellos por hacer uso del sistema de denuncia.

Las empresas que no cumplen con estos requisitos de denuncia de irregularidades están sujetas a fuertes sanciones y multas en Estados Unidos. Pero si estas denuncias incumplen las normas sobre protección de datos de la UE, las empresas afectadas se enfrentan al riesgo de ser sancionadas por las autoridades de protección de datos de la UE.

Debido al problema a que se enfrentaban las empresas de la UE, el Grupo de Trabajo, en su WP 117[238] llevó a cabo un análisis del tema que contribuyese a la seguridad jurídica de las empresas que están sujetas tanto a las normas de protección de datos de la UE como a la SOX.

El Grupo de Trabajo opina que la correcta aplicación de las normas sobre protección de datos a los sistemas de denuncia de irregularidades contribuirá a paliar los riesgos mencionados. También considera que, lejos de impedir que estos sistemas funcionen de acuerdo con el objeto previsto, la aplicación de estas normas contribuirá en general al correcto funcionamiento de los sistemas de denuncia de irregularidades.

La aplicación de las normas sobre protección de datos a los sistemas de denuncia de irregularidades implica abordar: la cuestión de la legitimidad de los sistemas de denuncia de irregularidades, la aplicación de los principios de proporcionalidad y calidad de los datos, la información clara y completa sobre el sistema, los derechos de la persona incriminada, la seguridad de las operaciones de tratamiento, la gestión de los sistemas internos de denuncia de irregularidades, los problemas relacionados con las transferencias internacionales de datos y la notificación y los requisitos de comprobación previos.

El Grupo de Trabajo analiza con detenimiento cada uno de los puntos mencionados, pero por la materia que nos afecta en el presente trabajo, nos centraremos en el apartado de las transferencias internacionales. Con respecto a ellas, el Grupo indica que los

[238] Dictamen 1/2006 relativo a la aplicación de las normas sobre protección de datos de la UE a los sistemas internos de denuncia de irregularidades en los ámbitos de la contabilidad, controles de auditoría internos, cuestiones de auditoría, lucha contra la corrupción y delitos financieros y bancarios. Adoptado el 1 de febrero de 2006.

artículos 25 y 26 de la Directiva 95/46/CE se aplicarán cuando los datos personales se transfieran a un país tercero.

La aplicación de las disposiciones de los artículos 25 y 26 será pertinente cuando la empresa haya confiado parte de la gestión del sistema de denuncia de irregularidades a un proveedor establecido fuera de la UE, o cuando los datos recogidos en las denuncias se distribuyan dentro del grupo, alcanzando por tanto a empresas que se encuentren fuera de la UE.

En los casos en que el tercer país al que se envíen los datos no garantice un nivel de protección adecuado, según lo exigido por el artículo 25 de la Directiva 95/46/CE, los datos podrán transferirse siempre y cuando se cumpla alguna de estas condiciones:

- El receptor de los datos personales sea una entidad establecida en los Estados Unidos que haya suscrito el sistema de seguridad Safe Harbor.
- El receptor haya firmado un contrato de transferencia con la empresa de la UE que transfiera los datos, en virtud del cual esta última establezca salvaguardias adecuadas, por ejemplo basándose en cláusulas contractuales estándar publicadas por la Comisión Europea en sus Decisiones de 15 de junio de 2001 o 27 de diciembre de 2004.
- El receptor cuente con un conjunto de normas empresariales obligatorias debidamente aprobadas por las autoridades competentes en materia de protección de datos.

La AEPD también ha analizado el tema en su Informe Jurídico 128/2007: "Creación de sistemas de denuncias internas en las empresas (mecanismos de *whistleblowing*)".

En el Informe se recuerda que la transferencia internacional de datos no excluye de la aplicación de las disposiciones contenidas en la LOPD, conforme a su ámbito de aplicación, correspondiendo a la Agencia Española de Protección de Datos la competencia para verificar su cumplimiento: "Ello implica que, al margen de la necesaria aportación de las garantías exigidas por el artículo 33 de la Ley Orgánica 15/1999, que se materializarían en el caso de la transferencia a Japón en la aportación de las cláusulas contractuales adoptadas por la Comisión Europea, que en este caso deberá ser las que rigen la transferencia de datos entre responsables del tratamiento, será necesario que la cesión implícita a la mencionada transferencia, así como el tratamiento de los datos en España, cumpla con lo dispuesto en la propia Ley Orgánica 15/1999".

Y señala más adelante que "será preciso que se proceda a notificar el tratamiento a fin de obtener su inscripción en el Registro General de Protección de Datos, así como solicitar, en su caso, la autorización para la transferencia internacional de datos que pretende realizarse a Japón, país que no ofrece un nivel adecuado de protección de datos, conforme a lo exigido por el artículo 33.1 de la Ley Orgánica 15/1999".

5. PROTECCIÓN DE LA INTIMIDAD Y LOS DATOS PERSONALES DE LA AGENCIA MUNDIAL ANTIDOPAJE (AMA)

El segundo caso de conflicto con la regulación de las transferencias internacionales de datos que vamos a analizar es el de la protección de la intimidad y los datos personales de la Agencia Mundial Antidopaje.

La Agencia Mundial Antidopaje es una fundación de derecho suizo creada para promover y coordinar, a nivel internacional, la lucha contra el dopaje en el deporte en todas sus formas y, en aras de este objetivo, para cooperar con organizaciones

intergubernamentales, gobiernos, poderes públicos y otros organismos públicos y privados que luchan contra el dopaje en el deporte. Ha adoptado el Código AMA, vigente desde uno de enero de 2009, del que forman parte varias normas, incluida la de protección de la intimidad. La finalidad del Código es garantizar unos programas antidopaje armonizados, coordinados y efectivos a los niveles internacional y nacional por lo que se refiere a la detección, disuasión y prevención del dopaje. El Código ha sido aceptado por las federaciones internacionales de los deportes practicados en la UE y por las organizaciones nacionales antidopaje (ONAD) de todos los Estados miembros de la UE.

El Código AMA obliga, entre otras cosas, a las organizaciones antidopaje (OAD) a seleccionar deportistas para su inclusión en un Grupo registrado para controles y también a obtener de ellos información sobre su paradero. La AMA ha desarrollado y controla una base de datos en internet denominada *Anti-Doping Administration and Management System* (Sistema de administración y gestión antidopaje «ADAMS»), situada en Montreal, Canadá, por medio de la cual actúa como centro de información en cuanto al control antidopaje. ADAMS puede usarse como instrumento de intercambio de datos por las OAD que deseen hacerlo, aunque parece ser que la AMA pretende en último término hacer obligatorio el uso de ADAMS.

El Grupo de Trabajo adoptó el seis de abril de 2009 el Documento WP 162, sobre el Código AMA[239].

[239] Segundo dictamen 4/2009 sobre la Norma internacional para la protección de la intimidad y los datos personales de la Agencia Mundial Antidopaje (AMA), sobre disposiciones relacionadas del Código AMA y sobre otros aspectos relacionados con la intimidad en el contexto de la lucha contra el dopaje en el deporte por parte de la AMA y de las organizaciones nacionales antidopaje.

Después de analizar una serie de puntos problemáticos en el contexto de los requisitos europeos en materia de protección de la intimidad y los datos personales, se centra en las transferencias internacionales de datos a la base de datos ADAMS en Canadá y a otros países fuera de la UE.

En primer lugar se plantea la cuestión de si efectivamente los datos personales pueden transmitirse libremente de la UE a la base de datos ADAMS en Canadá sin salvaguardias adicionales. A este respecto, no hay ninguna decisión de la Comisión sobre Canadá de carácter general. Sólo hay una decisión sobre la adecuación de la protección de los datos personales conferida por la ley canadiense *Personal Information and Electronic Documents Act* (PIPEDA), que solamente se aplica a las entidades privadas que recojan, utilicen o divulguen datos personales en sus actividades comerciales.

Como el acuerdo ADAMS describe, la Agencia Mundial Antidopaje es una organización sin ánimo de lucro. Entonces la Decisión sobre el carácter adecuado de la protección de la PIPEDA no se aplica a la AMA, dado que sus actividades no son de carácter comercial.

Cuando el tercer país al que se realiza una transferencia no garantice un nivel adecuado de protección, la transferencia desde la UE debe basarse en las excepciones del artículo 26.1 de la Directiva 95/46/CE o ir acompañada por las garantías adicionales reglamentadas en el artículo 26.2.

El Grupo de Trabajo entiende que las excepciones a la regla de adecuación del artículo 26.1 de la Directiva se refieren en general a los casos en los que los riesgos para los interesados son relativamente pequeños, o a cuando otros intereses prevalecen sobre

el derecho a la intimidad del interesado y sobre otros derechos fundamentales. Por lo tanto, deben interpretarse restrictivamente de modo que la excepción no se convierta en regla. En base a esta interpretación estudia la posible aplicación de alguna de las excepciones:

- El consentimiento (letra a del art. 26.1) como fundamento de las transferencias de datos de los deportistas no cumple con los requisitos del artículo 2.h) de la Directiva[240]. Aunque se satisfacen muchos de los requisitos en cuanto a la información que debe dar un responsable de los datos a un interesado, no se puede entender que el consentimiento aportado pueda amparar la transferencia internacional.

- La transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales tomadas a petición del interesado (letra b del art. 26.1). En el caso en que, por ejemplo, exista un contrato entre un deportista que compite a nivel internacional y una organización antidopaje que se ocupa del entrenamiento y las competiciones, esto podría proporcionar un fundamento para la transferencia a partes implicadas específicas de terceros países de los datos personales que sean necesarios para competir y entrenarse a escala internacional, incluida la información sobre el paradero. Sin embargo, la exención debe interpretarse restrictivamente. No se deben intercambiar más datos personales de los estrictamente necesarios a efectos del contrato y, salvo las partes

[240] En el artículo 2.h) se define el *consentimiento del interesado* como toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernan. En este sentido el Grupo de Trabajo en su Documento WP 114 se refiere al uso del consentimiento para las transferencias de datos en los siguientes términos: "es improbable que el consentimiento ofrezca un marco adecuado a largo plazo para los responsables del tratamiento en casos de transferencias repetidas o incluso estructurales para el tratamiento de que se trate".

directamente implicadas, nadie más debe recibir esos datos. Esta *prueba de necesidad* exige una relación estrecha y sustancial entre el interesado y el objeto del contrato. Por estas razones, en el ejemplo dado, la transmisión a la AMA en su condición de centro de información en cuanto al control antidopaje y el uso de ADAMS no se considerarían necesarios para cumplir el contrato entre el deportista y la OAD.

- La transferencia sea necesaria o legalmente exigida para la salvaguardia de un interés público importante (letra d del art. 26.1). La mera justificación de un interés público no bastaría. Debe ser una cuestión de interés público importante. Este interés público importante debe ser identificado como tal por la legislación nacional aplicable a los responsables de los datos establecidos en la UE.

Ninguna de las tres posibles excepciones puede usarse como justificación para las transferencias internacionales de datos. Además, el Grupo de Trabajo recomienda que las transferencias de datos personales que puedan calificarse como masivas, repetidas o estructurales no se basen en las excepciones. Por lo tanto las organizaciones antidopaje deberían hacer uso de garantías adicionales tales como las cláusulas contractuales, tal como establece el artículo 26.2, en cuyo caso es necesaria la autorización del Estado miembro.

6. EL TRATAMIENTO DE DATOS PERSONALES POR PARTE DE SWIFT

Antes de proceder en el próximo punto al análisis de los servicios de *Cloud Computing*, nos puede servir de introducción, por sus múltiples conexiones, un caso de transferencia masiva de datos desde un país de la UE a otro país tercero que no proporciona un nivel adecuado de protección, y además sin cumplir los requisitos legales para poder llevarla a cabo.

Hablamos del tratamiento de datos personales por parte de la Sociedad de Telecomunicaciones Financieras Interbancarias Mundiales (*Worlwide Interbank Financial Telecommunication* - SWIFT). El Grupo de Trabajo emitió el Dictamen 10/2006[241], en donde se evalúa el cumplimiento por parte de dicha Sociedad de la normativa sobre protección de datos.

SWIFT es un servicio de mensajería financiera mundial que facilita transferencias internacionales de dinero. Esta sociedad almacena todos los mensajes durante un período de 124 días en dos centros de operaciones, uno en la UE y otro en EE.UU. (se almacena la información por duplicado en *servidores espejos*). Los mensajes contienen datos personales tales como los nombres del ordenante y del beneficiario.

SWIFT es una cooperativa propiedad del sector que ofrece servicios de mensajería y programas informáticos de interfaz seguros y normalizados a más de 7.800 entidades financieras de todo el mundo. Procesa una media de 12 millones de mensajes a diario. El volumen total de mensajes procesados ascendió, por ejemplo, en el año 2005, a 2.500 millones, de los cuales 1.600 millones correspondían a Europa y 467 millones al continente americano. La información procesada por SWIFT afecta entonces a cientos de miles de ciudadanos de la UE ya que las entidades financieras europeas utilizan sus servicios para el envío a todo el mundo de mensajes relacionados con transferencias de dinero entre entidades financieras. Este envío se produce independientemente de si los mensajes se procesan en la Unión Europea y el Espacio Económico Europeo o en un tercer país.

[241] Dictamen 10/2006 sobre el tratamiento de datos personales por parte de la Sociedad de Telecomunicaciones Financieras Interbancarias Mundiales (Worlwide Interbank Financial Telecommunication - SWIFT), WP 128, adoptado el 22 de noviembre de 2006.

Tras los atentados terroristas de septiembre de 2001, el Departamento del Tesoro de los EE.UU. emitió citaciones en las que requería que SWIFT facilitara acceso a la información contenida en mensajes y conservada en los Estados Unidos. SWIFT dio cumplimiento a las citaciones, aunque se negociaron algunas limitaciones al acceso por parte de dicho organismo. El asunto se hizo público a raíz de la cobertura de la prensa a finales de junio y principios de julio de 2006.

Como cooperativa domiciliada en Bélgica y ser considerada como responsable del tratamiento, SWIFT está sujeta a la legislación belga sobre protección de datos por la que se aplica la Directiva 95/46/CE. Por otra parte, las entidades financieras de la UE que utilizan el servicio SWIFT también pueden ser consideradas como responsables del tratamiento, motivo por el cual están sujetas a la legislación nacional sobre protección de datos por la que se aplica la Directiva en el Estado miembro en que están domiciliadas.

Para evaluar la compatibilidad del tratamiento efectuado por SWIFT con las normas de protección de datos, el Grupo de Trabajo analiza los siguientes puntos:

- Aplicación de los principios de calidad de los datos y de proporcionalidad (art. 6 de la Directiva). No se respetan los principios de limitación y compatibilidad de los fines, proporcionalidad y necesidad de los datos personales tratados.
- Legitimidad. Para que cualquier tratamiento de los datos personales sea legal debe ser legítimo y cumplir uno de los motivos enumerados en el artículo 7 de la Directiva. Se estudia si es necesario para la ejecución de un contrato (letra b), si lo es para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento (letra c) o si lo es a efectos del interés legítimo

perseguido por el responsable del tratamiento (letra f). Se considera que no puede utilizarse ninguno de los tres casos para justificar el tratamiento.

- Provisión de información clara y completa sobre el sistema (art. 10 y 11 de la Directiva). El responsable del tratamiento está obligado a informar a los interesados sobre la existencia, el fin y el funcionamiento de su procesamiento de los datos, los destinatarios de los datos personales y el derecho de acceso, rectificación y supresión por el interesado. En el caso de SWIFT esta información referente al tratamiento no fue facilitada.
- Cumplimiento de los requisitos de notificación (art. 18 a 20 de la Directiva). SWIFT notificó algunos tipos de tratamiento a la Agencia de Protección de Datos belga pero no notificó el tratamiento y almacenamiento por duplicado en el centro de operaciones de Estados Unidos para la ejecución de órdenes de pago internacionales ni el fin subsiguiente.
- Mecanismos de supervisión. El Grupo de Trabajo condena el hecho de que los mecanismos existentes de control independiente por parte de las autoridades públicas de control responsables del tratamiento de los datos personales no se han respetado para los datos personales tratados a través del servicio de SWIFT.

Por ser nuestro tema de estudio, reservamos para el final la evaluación efectuada en el marco de los flujos transfronterizos de datos. Los artículos 25 y 26 de la Directiva son aplicables cuando los datos personales se envían a un tercer país. Cualquier envío de datos generado dentro del territorio de la UE que deba utilizarse fuera del territorio de la UE tiene que estar supeditado a una evaluación de adecuación de conformidad con la Directiva.

Para que SWIFT trate y almacene como duplicado datos personales en los Estados Unidos tiene primero que transferir estos datos desde la UE de conformidad con la legislación belga adoptada con la Directiva sobre la transferencia de datos personales a terceros países. Para el Grupo de Trabajo se han de tener en cuenta dos elementos: en primer lugar, el tratamiento comercial y el almacenamiento por duplicado de los datos personales por SWIFT Bélgica en su centro de operaciones en los Estados Unidos, y en segundo lugar el tratamiento de los datos para el fin posterior por parte del Departamento del Tesoro de los EE.UU. aceptado por SWIFT.

Para empezar el análisis, se examina la *protección adecuada de los datos* (artículo 25.1 de la Directiva). Teniendo en cuenta la redacción del artículo 25.2 de la Directiva sobre la evaluación del carácter adecuado del nivel de protección que ofrece un país tercero, y aplicando los principios definidos en el Documento WP12, el Grupo de Trabajo concluye que en los Estados Unidos solo quienes están adheridos a los principios de *Puerto Seguro* cuentan con un nivel de protección adecuado. Sin embargo los acuerdos de *Puerto Seguro* no incluyen los servicios financieros. Por lo tanto SWIFT no puede basarse en el artículo 25 de la Directiva para el tratamiento y almacenamiento por duplicado en el centro de operaciones de Estados Unidos.

Continúa el análisis examinando las *garantías suficientes establecidas por el destinatario* (artículo 26.2 de la Directiva). El responsable del tratamiento puede ofrecer garantías suficientes respecto de la protección de la vida privada, de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los respectivos derechos. Tal como indica el artículo 26.2 dichas garantías pueden derivarse, en particular, de cláusulas contractuales apropiadas. Y en el caso de grupos

multinacionales también pueden utilizarse normas corporativas vinculantes. Pero en el caso de SWIFT no se ha hecho uso de ninguna de estas posibilidades para su tratamiento y almacenamiento por duplicado en el centro de operaciones de los Estados Unidos.

Por último se analiza si el envío de datos personales a Estados Unidos ha podido efectuarse en base a alguna de las excepciones contenidas en el artículo 26.1 de la Directiva. Las posibles excepciones en este caso son las siguientes:

- *Consentimiento del interesado* (letra a del art. 26.1). Para invocar esta excepción el interesado debe dar su consentimiento inequívoco al envío propuesto. Pero SWIFT no ha obtenido el consentimiento inequívoco de los interesados para el tratamiento y almacenamiento en Estados Unidos. Por lo tanto no puede basarse en esta excepción.

- *Que la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales tomadas a petición del interesado* (letra b del art. 26.1). Esta excepción significa que los datos enviados deben ser verdaderamente necesarios para el fin de la realización de ese contrato o de esas medidas precontractuales. Por esta razón, el Grupo de Trabajo considera que esta condición no podría aplicarse a los envíos de datos por SWIFT al centro de operaciones de Estados Unidos, pues SWIFT no tiene una relación contractual directa con el individuo. Asimismo, esta excepción no puede aplicarse al envío de información adicional que no sea necesaria para el fin del envío.

- *Que la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar en interés del interesado, entre el responsable del tratamiento y un tercero* (letra c del art. 26.1). Para aplicar esta excepción debería

comprobarse que la transferencia sea realmente necesaria. Esa “prueba de necesidad” exige una conexión cercana e importante entre el interés del interesado y los fines del contrato. Y para el Grupo de Trabajo esa conexión cercana no existe.

- *Que la transferencia sea necesaria o legalmente exigida para la salvaguardia de un interés público importante, o para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial* (letra d del art. 26.1). SWIFT considera que sería aplicable esta excepción ya que su infraestructura y el almacenamiento por duplicado de datos objeto de tratamiento en los centros de operaciones se consideró como elemento crucial en el sistema financiero internacional y que había sido propuesto por los bancos centrales que actúan como supervisores por razones de seguridad y fiabilidad. El Grupo de Trabajo no puede asumir esta interpretación. Aunque se demostrara que la duplicación internacional del tratamiento fuera "necesaria o legalmente exigida para la salvaguardia de un interés público importante", es posible almacenar por duplicado esos datos tratados fuera del EEE en un país que proporcione un nivel adecuado de protección (por ejemplo Argentina o Canadá). El almacenamiento en un país no perteneciente a la UE sin un nivel adecuado de protección de los datos no era necesario ni puede ser justificado por esta excepción.

- *Que la transferencia sea necesaria para la salvaguardia del interés vital del interesado* (letra e del art. 26.1). Esta excepción es aplicable a las transferencias de datos que estén relacionadas con el interés individual del interesado y, cuando se trata de datos sanitarios, deben ser necesarios para un diagnóstico esencial. Por consiguiente, esta excepción no podría utilizarse para justificar la transferencia.

Por todas las razones apuntadas anteriormente, el Grupo de Trabajo considera que el tratamiento y almacenamiento por duplicado en Estados Unidos no se realizaron legalmente ya que no respetan las disposiciones de la Directiva 95/46/CE. Se exige de SWIFT el cese de las infracciones y el retorno al tratamiento legal de datos.

7. EL *CLOUD COMPUTING*

No podemos olvidarnos en este trabajo de un negocio en auge que probablemente cambiará radicalmente la concepción que tenemos sobre la informática. Según International Data Corporation[242] los ingresos mundiales de los servicios *Cloud Computing* alcanzarán los 55.500 millones de dólares en el año 2014, con tasas de crecimiento acumuladas del 27.4%. Este rápido crecimiento es casi cinco veces más elevado que el de los productos tradicionales de tecnología de la información.

El llamado *Cloud Computing* es un modelo de prestación de servicios tecnológicos que permite el acceso bajo demanda y a través de la red a un conjunto de recursos compartidos y configurables que pueden ser rápidamente asignados y liberados con una mínima gestión por parte del proveedor de servicios[243].

Esta nueva filosofía en el almacenamiento y proceso de datos tiene grandes ventajas, pero también aparecen nuevos problemas. Uno de ellos es en cuanto al

[242] Documento *Worldwide and Regional Public IT Cloud Services 2010-2014 Forecast.* Junio de 2010**.** IDC Corporate USA. Web de la compañía: **http://www.idc.com/research**

[243] Definición obtenida del informe *Utilización del Cloud Computing por los despachos de abogados y el derecho a la protección de datos de carácter personal*. Presentado a 18 de junio de 2012 por la AEPD y el Consejo General de la Abogacía Española. Documento descargable de la dirección electrónica de la AEPD.

cumplimiento de la normativa de protección de datos, tanto de la Directiva 95/46/CE como de la LOPD y del RLOPD.

Como señala Marzo Portera, "los modelos comerciales en Internet no encajan fácilmente con lo establecido en la Directiva 95/46/CE"[244]. Servicios como el *Cloud Computing* "requieren de cierta flexibilidad en la aplicación de la Directivas europeas y normas internas de los estados miembros".

Analizaremos las posibilidades de cumplimiento de dichas normas en el caso de que los prestadores de los servicios de *Cloud Computing* se encuentren radicados en terceros países, circunstancia muy habitual en este tipo de servicios.

Según el Instituto Nacional de Estándares y Tecnologías (organismo dependiente del Departamento de Comercio de Estados Unidos), el *Cloud Computing* tiene cinco características esenciales:

1. *Autoservicio bajo demanda*. El usuario puede acceder a capacidades de computación *en la nube* de forma automática conforme las necesita sin necesidad de una interacción humana con su proveedor o sus proveedores de servicios *Cloud*.
2. *Múltiples formas de acceder a la red*. Los recursos son accesibles a través de la red y por medio de mecanismos estándar que son utilizados por una amplia

[244] MARZO PORTERA, A.M: "Privacidad y Cloud Computing, hacia dónde camina Europa". Revista de la Facultad de Ciencias Sociales y Jurídicas del Elche. Volumen 1 – Núm. 8 – Febrero de 2012. Pág. 202-229.

Disponible en la siguiente dirección:

http://revistasocialesyjuridicas.files.wordpress.com/2012/02/08-tm-12.pdf

variedad de dispositivos de usuario, desde teléfonos móviles a ordenadores portátiles o PDAs.

3. *Compartición de recursos*. Los recursos (almacenamiento, memoria, ancho de banda, capacidad de procesamiento, máquinas virtuales, etc.) de los proveedores son compartidos por múltiples usuarios, a los que se van asignando capacidades de forma dinámica según sus peticiones. Los usuarios pueden ignorar el origen y la ubicación de los recursos a los que acceden, aunque sí es posible que sean conscientes de su situación a determinado nivel, como el de CPD o el de país.
4. *Elasticidad*. Los recursos se asignan y liberan rápidamente, muchas veces de forma automática, lo que da al usuario la impresión de que los recursos a su alcance son ilimitados y están siempre disponibles.
5. *Servicio medido*. El proveedor es capaz de medir, a determinado nivel, el servicio efectivamente entregado a cada usuario, de forma que tanto proveedor como usuario tienen acceso transparente al consumo real de los recursos, lo que posibilita el pago por el uso efectivo de los servicios.

El *Cloud Computing* permite a sus usuarios el acceso a una serie de servicios muy variado: correo electrónico, almacenamiento documental, aplicaciones de gestión o de contabilidad, etc. Y todo ello sin precisar de servidores o de software propios. Los datos se encuentran en algún lugar de Internet representado de forma habitual por una nube.

Las ventajas para el usuario son muy claras, ya que los ahorros en equipos, software y personal informático pueden llegar a ser muy cuantiosos.

Pero junto a las ventajas aparecen también cuestiones problemáticas de difícil resolución. Como señala Fernández Aller “el modelo de cloud computing, por su propia

naturaleza, implica en muchos caso el desconocimiento del país preciso en que los datos van a ser tratados y de las entidades (subcontratadas) que van a intervenir en ese tratamiento"[245]. En general los datos en el modelo de *Cloud Computing* pasan a situarse en algún lugar indeterminado y variable, en un servidor radicado en una ubicación física desconocida por el responsable. Como bien señala el Grupo de Trabajo, la información puede encontrarse en un centro de datos a las dos de la tarde y en el otro extremo del mundo dos horas después[246]. En este contexto, los instrumentos legales tradicionales que regulan las transferencias internacionales de datos no proveen de una protección adecuada.

El usuario que contrata servicios de *Cloud Computing* ocupa la posición de responsable del tratamiento (ya que es a él a quien corresponde, entre otras, la decisión sobre la finalidad, el contenido y el uso del tratamiento) mientras que el prestador de servicios de *Cloud Computing* tendrá la naturaleza de encargado del tratamiento (pues su labor es tratar datos personales por cuenta del responsable).

En el marco de la prestación de servicios de tratamiento de datos personales por cuenta de terceros, el usuario de los servicios de *Cloud Computing* (responsable) deberá velar para que el prestador de servicios (encargado) cumpla la normativa española de protección de datos personales (artículo 20.2 del RLOPD). Las partes no pueden pactar la aplicación de una normativa distinta ni excluir la competencia de la AEPD.

---

[245] FENÁNDEZ ALLER, C: "Algunos retos de la protección de datos en la sociedad del conocimiento. Especial detenimiento en la computación en nube (cloud computing)". Revista de Derecho Uned, nº 10 de 2012, pág. 141.

[246] *Opinion 05/2012 on Cloud Computing*, WP 196, adoptado el uno de julio de 2012.

Por otra parte, es muy probable que los datos no se almacenen en territorio español, lo que nos obliga a tener en cuenta que, de acuerdo al artículo 25 de la Directiva 95/46/CE (o sus equivalentes en la regulación española), la transferencia a un país tercero de datos personales únicamente puede efectuarse cuando el país tercero de que se trate garantice un nivel de protección adecuado. En caso contrario solo se podría realizar la transferencia si se obtiene, previa la aportación de garantías adecuadas (cláusulas contractuales tipo de la Decisión 2010/87/UE), la autorización del Director de la AEPD. Incumplir esta exigencia está calificado como infracción muy grave por la LOPD, sancionada con multa de 300.001 a 600.000 euros.

Entonces un aspecto esencial es conocer el lugar al que se ha efectuado la transferencia de datos:

- Si la transferencia se ha efectuado a otro país que forma parte del Espacio Económico Europeo no tendrá la consideración de transferencia internacional de datos, tal como se regula en el artículo 5.1.s) del RLOPD. Por la misma razón no es necesaria la autorización de la AEPD.
- Cuando la transferencia se efectúa a alguno de los países con un nivel de protección que se considera adecuado por Decisión de la Comisión Europea, sí tendrá la calificación de transferencia internacional de datos, pero tampoco se necesita autorización de la AEPD.
- En el caso de transferencias a encargados del tratamiento que estén radicados en Estados Unidos y que se encuentren adheridos al acuerdo de *puerto seguro* nos

encontraríamos en la misma situación que en el caso anterior. Por lo tanto no hace falta autorización de la AEPD[247].

- Si la transferencia de datos se efectúa a un país que no ofrece un nivel adecuado de protección será necesaria la autorización previa del Director de la AEPD. Dicha autorización deberá seguir el procedimiento previsto en los artículos 137 a 140 del RLOPD.

En el último de los cuatro casos, una herramienta que ofrece garantías adecuadas con respecto a la protección de datos de carácter personal son las *cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países*, adoptadas por la Comisión Europea en la Decisión 2010/87/UE.

Otra alternativa es que el proveedor de *Cloud* haya obtenido una autorización previa del Director de la AEPD para realizar transferencias internacionales de datos a subencargados establecidos en terceros países basada en cláusulas contractuales en las que el responsable del tratamiento (la entidad que contrate los servicios de *Cloud*) autorice los servicios susceptibles de subcontratación y pueda conocer en cualquier momento la identidad de las empresas subcontratadas y, en el caso que se encuentren en países que no ofrezcan garantías adecuadas, en que países operan.

[247] Es el caso de la empresa *Dropbox, Inc.*, que ofrece un servicio (en unos casos de forma gratuita y en otros de pago) mediante el cual el usuario dispone de una carpeta en la nube en la que puede guardar y acceder a sus documentos y archivos desde cualquier dispositivo con conexión a Internet, así como compartirlos con otros usuarios. *Dropbox* ha obtenido la certificación el 16 de febrero de 2012, mediante la que se ha adherido al Protocolo "*Safe Harbour*". Las empresas que incorporen datos personales a *Dropbox* ya no necesitan solicitar autorización del Director de la AEPD. Solamente deberán comunicar dicha transferencia internacional en el Registro General de Protección de Datos.

La AEPD ha elaborado unas cláusulas contractuales, cuya aplicación parte de la existencia de un contrato marco entre el responsable del fichero y el encargado del tratamiento donde conste expresamente la autorización para la subcontratación por parte del encargado del tratamiento de conformidad con lo establecido en el artículo 21 del RLOPD. En este caso, el responsable del tratamiento (la empresa que quiere disfrutar de los servicios de *Cloud*) puede contratar con el proveedor de *Cloud*, quien en base a las cláusulas contractuales antes mencionadas, tendrá autorizada la transferencia internacional de datos.

En los servicios de *Cloud* también tenemos que tomar en consideración el contenido de los dos primeros puntos del artículo 9 de la LOPD:

1. El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.
2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

Por otra parte, de acuerdo al artículo 12.2 de la LOPD, la realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato en donde se establecerá expresamente que el encargado del tratamiento únicamente tratará los datos

conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas. En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar.

En el informe *Utilización del Cloud Computing por los despachos de abogados y el derecho a la protección de datos de carácter personal*, la AEPD relaciona los aspectos esenciales a tener en cuenta en materia de seguridad y confidencialidad, y desde un punto de vista técnico a la hora de seleccionar un proveedor de servicios *Cloud*:

- Como cuestión previa, tanto el responsable que contrata como cliente estos servicios como el propio prestador de servicios han de actuar diligentemente solicitando y ofreciendo una información detallada sobre las medidas que vayan a garantizar la seguridad y confidencialidad de la información. A tal efecto deberán intercambiar información sobre la naturaleza de los datos para establecer un nivel de seguridad apropiado.
- El proveedor de servicios *Cloud* ha de garantizar la conservación de los datos, mediante la realización de copias de seguridad periódicas y dotando a su infraestructura de los mayores niveles de seguridad física y lógica.
- El proveedor ha de establecer mecanismos seguros de autenticación para el acceso a la información. Estos mecanismos han de permitir la compartición e intercambio de información sin que por supuesto sea posible que personas no autorizadas accedan a información reservada o confidencial.

- El cifrado de los datos almacenados es una necesaria medida de seguridad. El proveedor ha de dar a conocer el nivel de seguridad ofrecido por las técnicas de cifrado de la información que aplique en sus sistemas.
- Asimismo, es fundamental acordar el procedimiento de recuperación y migración de los datos a la terminación de la relación entre el responsable del fichero y el proveedor; así como el mecanismo de borrado de los datos por parte del proveedor una vez que estos han sido transferidos al responsable del fichero o al nuevo proveedor designado por éste.
- Habida cuenta de que en numerosos casos los ficheros contendrán datos especialmente protegidos es necesario que el encargado del tratamiento establezca un registro de los accesos realizados a los datos.
- En el caso de que no sea posible verificar directamente las medidas de seguridad del prestador de servicios, deben contemplarse garantías alternativas que cumplan el mismo objetivo, tales como la intervención de un tercero independiente de acreditado prestigio que audite las medidas de seguridad implantadas.
- Que, en todo caso, si se producen incidencias de seguridad que afecten a los datos personales de los que es responsable el cliente del servicio de *Cloud Computing*, sean puestos en su conocimiento por el prestador del servicio junto con las medidas adoptadas para corregir los daños producidos y evitar que se reproduzcan dichos incidentes.

Todos estos aspectos técnicos deberán trasladarse al contrato de servicios que deberán formalizar el responsable del fichero y el proveedor de servicios *Cloud*.

El artículo 20.2 del RLOPD además obliga al responsable del tratamiento a velar por que el encargado del tratamiento reúna las garantías para el cumplimiento de lo dispuesto en el propio Reglamento. Entonces se responsabiliza al cliente que demanda estos servicios en la selección de un encargado que cumpla efectivamente los requisitos legalmente establecidos. Responsabilidad que se extiende a la subcontratación de servicios.

El Instituto Nacional de Tecnologías de la Comunicación expone en el documento *Guía para empresas: seguridad y privacidad del Cloud computing*[248] que habitualmente no será posible una inspección de las medidas de seguridad del proveedor del *Cloud* por parte del cliente interesado en contratar sus servicios. Por otra parte, salvo en casos muy específicos, la contratación se realiza a través de condiciones generales. Por ello será fundamental para el cliente cerciorarse de que el proveedor de servicios se compromete a respetar y cumplir las obligaciones contenidas en la LOPD y en la Directiva comunitaria.

Como bien indica Yolanda Adsuar[249], con la contratación de estos servicios en la nube "casi de manera automática, desaparece o se difumina el conocimiento por parte de la empresa sobre la ubicación física exacta de la información, así como de las condiciones de procesamiento, sin ignorar que de esta manera pueden quedar afectadas las garantías de confidencialidad y de seguridad de la información situada en el *Cloud*". Pero hasta que el legislador indique otro camino distinto "corresponde al Responsable

[248] Documento disponible en la siguiente dirección electrónica:
http://www.inteco.es/Seguridad/Observatorio/guias//Guia_Cloud

[249] ADSUAR, Y: "Cloud Computing vs. Protección de Datos de carácter Personal". Revista Actualidad Jurídica Aranzadi, núm 846, 12 de julio de 2012, pág. 5.

del Fichero, en todo caso, dar cumplimiento a aquellos aspectos de la normativa de protección de datos que le sean exigibles conforme a la legislación española y, en particular, la relativa a la formalización de un contrato por escrito y el cumplimiento de las reglas que rigen las Transferencias Internacionales de Datos, de haberlas, habiéndonos, previamente, informado con exactitud de la ubicación de los servidores que contendrán nuestra información".

Cuando el encargado de tratamiento subcontrate alguna actividad, dicha subcontratación habrá de recogerse en el contrato de prestación de servicios entre el responsable y el encargado del tratamiento. Como se indica en el artículo 21 del RLOPD, cuando no se identificase en el contrato la empresa con la que se vaya a subcontratar, será preciso que el encargado del tratamiento comunique al responsable los datos que la identifiquen antes de proceder a la subcontratación.

Una alternativa que se propone en el informe *Utilización del Cloud* antes mencionado, es que el responsable autorice los servicios susceptibles de subcontratación (por ejemplo el *hosting*) y tenga a su disposición de forma permanente una relación actualizada de las entidades subcontratadas y de los países donde operan (información que puede estar por ejemplo en una página web).

Sin embargo, como apunta el Grupo de Trabajo en la nota de prensa de uno de julio de 2012[250], referente a su *Opinion 05/2012 on Cloud Computing*, "la implantación a gran escala de servicios de computación en nube presenta una serie de riesgos, centrados en la falta de control sobre el uso de los datos de carácter personal y la

[250] Disponible en la web de la AEPD:
http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2012/notas_prensa/common/julio/120701_NP_29_Cloud.pdf

ausencia de información suficiente acerca de cómo, dónde y quién realizará el tratamiento de los datos". Y añade que "es posible que no puedan aplicar las medidas técnicas y organizativas necesarias para garantizar, por ejemplo, la disponibilidad y confidencialidad de los datos, de los que el cliente de los servicios en la nube continúa siendo jurídicamente responsable conforme a la legislación de la UE". Por todo ello concluye que las organizaciones que deseen utilizar servicios de computación en nube deberán realizar "un análisis exhaustivo y riguroso de los riesgos".

La Comisión Europea por su parte ha redactado el documento "Liberar el potencial de la computación en nube en Europa"[251]. Para la Comisión la computación en nube abarca una amplia gama de ámbitos estratégicos. Urge a la adopción de iniciativas políticas, como la reforma de la protección de datos y la normativa común de compraventa europea, que se proponen reducir los obstáculos a la aceptación de la computación en nube en la UE. Al mismo tiempo, la Comisión va a intervenir activamente en 2013 respecto a acciones clave, especialmente en lo que respecta a las medidas en materia de normalización y certificación para la computación en nube, el desarrollo de condiciones contractuales seguras y justas y la puesta en marcha de la Asociación Europea de Computación en Nube. Para la Comisión, será en los dos próximos años cuando se sentarán las bases para que Europa se convierta en una potencia mundial de la computación en nube. El avance adecuado en esta fase preparatoria deberá proporcionar una base estable para una fase de despegue rápido,

[251] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Liberar el potencial de la computación en nube en Europa. Bruselas, 27.9.2012 COM(2012) 529 final.

entre 2014 y 2020, durante la cual la utilización de las ofertas de servicios de computación en nube accesibles al público podría alcanzar un índice de crecimiento anual compuesto del 38 %. La Comisión invita a los Estados miembros a aprovechar el potencial de la computación en nube. Los Estados miembros deben desarrollar el uso de la nube por el sector público sobre la base de enfoques comunes que mejoren las características y la confianza, además de reducir los costes. Asimismo, la Comisión invita a las empresas del sector a cooperar estrechamente en el desarrollo y la adopción de normas comunes y de medidas de interoperabilidad.

El Supervisor Europeo de Protección de Datos ha dado respuesta a la Comunicación de la Comisión en un Dictamen de 16 de noviembre de 2012[252]. Para el SEPD la computación en nube puede traer enormes beneficios tanto a los ciudadanos como a las organizaciones. Sin embargo este nuevo entorno debe proporcionar un nivel adecuado de protección datos. En general los clientes de *Cloud computing* tienen poca influencia sobre los términos y condiciones del servicio ofrecido por los proveedores del servicio. Habrá que asegurarse de que los proveedores de servicios *Cloud* no evitan asumir la responsabilidad que les corresponde, ya que la complejidad de la tecnología de la computación en nube no puede justificar la posible reducción de las normas de protección de datos.

En opinión del SEPD, el desequilibrio de poder entre los clientes de *Cloud computing* y los proveedores de servicios podría resolverse mediante el desarrollo de términos y condiciones comerciales estandarizados que respeten los requisitos de

[252] Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe". Bruselas, 16.11.2012.

protección de datos para los contratos comerciales, la contratación pública y las transferencias internacionales de datos.

Por último podríamos señalar una serie de recomendaciones efectuadas por el SEPD con el objetivo de:

- Clarificar y proporcionar orientación sobre la forma de garantizar la eficacia de las medidas de protección de datos en la práctica y apoyar el uso de normas corporativas vinculantes por parte de los proveedores de servicios.
- Promover el desarrollo de las mejores prácticas en temas como la responsabilidad responsable/encargado, la retención de datos en el entorno de la nube, la portabilidad de datos y el ejercicio de los derechos de los interesados.
- Elaborar normas de desarrollo y sistemas de certificación que incorporen plenamente los criterios de protección de datos.
- Definir claramente la noción de transferencia y los criterios bajo los cuales se podría acceder a los datos en la nube por los organismos encargados de hacer cumplir la ley fuera de los países del EEE.

CAPÍTULO V

TRANSFERENCIAS INTERNACIONALES EN EL MARCO DE LA COOPERACIÓN POLICIAL Y JUDICIAL EN MATERIA PENAL

1. LA DECISIÓN MARCO 2008/977/JAI[253]

Las *decisiones marco* del Consejo han tenido por objeto la aproximación de las disposiciones legales y reglamentarias de los Estados miembros de la UE. Tienen una cierta similitud con las *directivas,* ya que son normas de resultado. Las decisiones marco obligan a los Estados miembros en cuanto al resultado que deba conseguirse, dejando, sin embargo, a las autoridades nacionales la elección de la forma y de los medios. Pero al contrario que en las directivas, en las que es posible el efecto directo, en las decisiones marco dicho efecto directo está descartado expresamente en el artículo 34.2.b del TUE (en su redacción vigente hasta uno de enero de 2009). Con ello se impide a los particulares invocar directamente una norma europea ante una jurisdicción nacional o europea aun en el caso de que un estado no adopte las medidas oportunas en el plazo previsto o que las adopte mediante una transposición incorrecta[254].

Antes de la entrada en vigor del Tratado de Lisboa, la legislación relativa a la protección de datos en el espacio de libertad, seguridad y justicia estaba repartida entre el primer pilar (protección de datos con fines privados y comerciales, con la aplicación del método comunitario), el segundo pilar (política exterior y de seguridad común, que estaba regulada en el Título V del TUE) y el tercer pilar (cooperación policial y judicial en materia penal, cubierta por el Título VI del TUE). El proceso decisorio se regía por normas diferentes. Con el Tratado de Lisboa la estructura de pilares ha desaparecido, quedando integrada la cooperación policial y judicial en materia penal dentro del método comunitario.

[253] DOUE L 350 de 30 de diciembre de 2008.

[254] VV. AA: *Principios de Derecho de la Unión Europea*. Colex. Madrid 2000, pág. 377.

Por ser anterior al Tratado de Lisboa, en el artículo 3.2 de la Directiva 95/46/CE se establece que sus disposiciones no se aplicarán al tratamiento de datos personales "efectuado en el ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario, como las previstas por las disposiciones de los títulos V y 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 (incluido el bienestar económico del Estado cuando dicho tratamiento esté relacionado con la seguridad del Estado) y las actividades del Estado en materia penal".

El tratamiento de datos por las autoridades policiales y judiciales en materia penal lo regula esencialmente la Decisión Marco 2008/977/JAI del Consejo, de 27 de noviembre de 2008. Su entrada en vigor se produjo el 19 de enero de 2009. Por lo tanto también es anterior al Tratado de Lisboa.

Por el reparto de competencias en el seno de la Unión, la Comisión Europea carece de facultades para exigir el cumplimiento de las disposiciones de las Decisiones Marco. Esto ha contribuido a su desigual aplicación en los países de la UE. Por otra parte, el ámbito de aplicación de la Decisión Marco, tal como se regula en su artículo 1.2, se limita a los datos personales que son o han sido transmitidos o puestos a disposición entre Estados miembros o intercambiados entre Estados miembros e instituciones u organismos de la UE. Ello significa que el tratamiento de datos personales que no haya sido objeto de intercambio queda fuera del ámbito de aplicación de las disposiciones de la UE que regulan ese tratamiento y salvaguardan el derecho fundamental a la protección de datos.

Además, según el artículo 28 de la Decisión Marco, "cuando algún acto, adoptado en virtud del título VI del Tratado de la Unión Europea antes de la fecha de entrada en vigor de la presente Decisión Marco y que regule el intercambio de datos personales entre los Estados miembros o el acceso de unas autoridades designadas de los Estados miembros a sistemas de información establecidos en virtud del Tratado constitutivo de la Comunidad Europea, establezca condiciones específicas respecto de la utilización de dichos datos por el Estado miembro receptor, estas primarán sobre las disposiciones de la presente Decisión Marco relativas al uso de los datos transmitidos o puestos a disposición por otro Estado miembro".

El Considerando 39 de la Decisión Marco preceptúa que ésta no debe afectar, entre otros, al conjunto completo y coherente de disposiciones de protección de datos que rigen el funcionamiento "de Europol, Eurojust, el Sistema de Información de Schengen (SIS) y el Sistema de Información Aduanero (SIA), ni a los que permiten a las autoridades de los Estados miembros acceder directamente a determinados sistemas de datos de otros Estados miembros. Lo mismo se aplica a las disposiciones de protección de datos que rigen la transferencia automatizada de perfiles de ADN[255], datos dactiloscópicos y datos de los registros nacionales de matriculación de vehículos en virtud de la Decisión 2008/615/JAI del Consejo, de 23 de junio de 2008, sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza".

[255] Un estudio en profundidad sobre esta materia nos lo ofrece Yolanda Gómez Sánchez en su artículo "Los datos genéticos en el Tratado de Prüm". Revista de Derecho Constitucional Europeo nº 7 de 2007.

En el caso de medidas sectoriales que contienen normas de protección de datos de alcance más limitado solo prevalecen sobre la Decisión Marco cuando son más restrictivas que esta última. En los demás casos se aplica la Decisión Marco (tal como se establece en su Considerando 40).

La Decisión Marco dispone sobre la legitimidad del tratamiento de los datos personales a fin de garantizar que toda la información que pueda ser objeto de intercambio sea tratada de forma legítima y de acuerdo con los principios de calidad de los datos. También regula los derechos de los interesados a garantizar la protección de sus datos personales, sin que ello suponga una limitación a los intereses de las investigaciones penales. Con este motivo, los titulares de los datos deben estar informados y tener acceso a sus datos personales.

Las autoridades nacionales de control deberán emitir su dictamen y supervisar las normas que los Estados miembros adopten para incorporar la Decisión Marco a su ordenamiento.

Si nos centramos en el tema de las transferencias internacionales de datos, estas se regulan básicamente en el Considerando 24 y en el artículo 13 de la Decisión Marco.

El Considerando 24 dispone que "cuando los datos personales se transfieren de un Estado miembro a terceros países o a organismos internacionales, tal transferencia, en principio, únicamente debe efectuarse una vez que el Estado miembro del que se hayan obtenido los datos haya dado su consentimiento a la transferencia. Cada Estado miembro debe poder determinar las modalidades de dicho consentimiento, incluso, por

ejemplo, mediante un consentimiento general para categorías de información o terceros Estados concretos".

En el artículo 13.1 se regula que los Estados miembros dispondrán que los datos personales transmitidos o puestos a disposición por la autoridad competente de otro Estado miembro puedan transferirse a terceros Estados u organismos internacionales solo si se cumplen todas las condiciones siguientes:

"a) Que sea necesario para la prevención, la investigación, la detección o el enjuiciamiento de infracciones penales o para la ejecución de sanciones penales.

b) Que la autoridad receptora del tercer Estado o el organismo internacional receptor sea competente para la prevención, la investigación, la detección o el enjuiciamiento de infracciones penales o la ejecución de sanciones penales.

c) Que el Estado miembro que proporcionó los datos haya consentido la transferencia de acuerdo con su Derecho nacional.

d) Que el tercer Estado u organismo internacional de que se trate garantice un nivel adecuado de protección en el tratamiento de datos previsto".

La transferencia de datos sin el consentimiento previsto en el apartado anterior "solo podrá permitirse si es esencial para la prevención de una amenaza inmediata y grave a la seguridad pública de un Estado miembro o de un tercer Estado o a intereses esenciales de un Estado miembro, y si el consentimiento previo no puede obtenerse a tiempo. Se informará sin demora a la autoridad encargada de otorgar el consentimiento" (artículo 13.2).

Aunque el tercer Estado u organismo internacional de que se trate no garantice un nivel adecuado de protección en el tratamiento de datos previsto, podrán transferirse datos personales en cualquiera de los siguientes supuestos (artículo 13.3):

"a) Que así lo disponga el Derecho nacional del Estado miembro que transfiere los datos por alguno de los siguientes motivos:

i) Legítimos intereses específicos del interesado.

ii) Legítimos intereses superiores, en especial importantes intereses públicos.

b) Que el tercer Estado o el organismo internacional receptor ofrezca garantías que el Estado miembro de que se trate considere adecuadas de conformidad con su Derecho nacional".

Para evaluar si el tercer Estado u organismo internacional de que se trate garantiza un nivel adecuado de protección se atenderá "a todas las circunstancias que concurran en una operación de transferencia de datos o en un conjunto de operaciones de transferencia de datos. Se tomará en consideración en particular la naturaleza de los datos, la finalidad y la duración de la operación u operaciones de tratamiento previstas, el Estado de origen y el Estado u organismo internacional de destino final de los datos, la normativa, tanto general como sectorial, vigente en el tercer Estado u organismo internacional de que se trate, y las normas profesionales y medidas de seguridad que sean de aplicación" (artículo 13.4).

Por otra parte, el artículo 26 regula que la Decisión "no afectará a las obligaciones y compromisos contraídos por los Estados miembros o la Unión en virtud de acuerdos bilaterales o multilaterales con terceros Estados que estén vigentes en el momento de la adopción de la Decisión Marco".

En el Tercer Dictamen del Supervisor Europeo de Protección de Datos sobre la propuesta de Decisión Marco del Consejo relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal[256], éste había criticado la regulación del intercambio de datos personales con terceros países.

El Dictamen parte de la regulación de las transferencias a terceros países del Convenio 108. En su Protocolo Adicional relativo a las autoridades de control y los flujos transfronterizos de datos establece el principio general de que se permite la transferencia de datos personales a un país tercero solamente si esa parte garantiza un nivel adecuado de protección para la transferencia considerada.

En la Decisión Marco en caso de transferencia de datos personales a terceros países u organismos internacionales, estos datos deberían, en principio, gozar de un nivel de protección adecuado. Pero de forma alternativa permite que se transfieran datos personales transmitidos de otro Estado miembro a terceros países u organismos internacionales cuando la autoridad que los transmite haya dado su consentimiento a la transferencia de acuerdo con su Derecho nacional.

Por lo tanto, en la Decisión Marco no se establece ninguna necesidad de protección adecuada, ni prevé criterio o mecanismo común alguno para evaluar la adecuación. Esto significa que cada Estado miembro evaluará conforme a su propia discreción el nivel de adecuación previsto por el tercer país o el organismo internacional. Por consiguiente, la

[256] El contenido del Tercer Dictamen del SEPD se encuentra en el DOUE C 139 de 23 de junio de 2007. Antes ya había formulado dos dictámenes sobre la misma materia que se habían publicado en el DOUE C 47 de 25 de febrero de 2006 y en el DOUE C 91 de 26 de abril de 2007.

lista de países y organizaciones internacionales adecuados podrá variar considerablemente de un Estado miembro a otro.

Este marco jurídico también obstaculizaría la cooperación policial y judicial. Las autoridades policiales de un Estado miembro, al decidir sobre una solicitud de un expediente penal determinado presentada por un tercer país, no solamente tendrán que considerar la adecuación de ese país, sino que también habrán de tener en cuenta si cada uno de los demás Estados miembros que han contribuido al expediente ha dado su consentimiento, con arreglo a su propia evaluación de la adecuación del tercer país de que se trate.

El SEPD cree que la Decisión Marco regula las transferencias de datos personales a terceros países y organizaciones internacionales de forma inadecuada para proteger los datos personales e inviable para las autoridades policiales. Sería imprescindible garantizar un nivel adecuado de protección cuando se transfieran datos personales a terceros países u organizaciones internacionales y que se crearan mecanismos que garanticen normas comunes y decisiones coordinadas en relación con las constataciones.

2. PROPUESTA DE DIRECTIVA DE PROTECCIÓN DE DATOS EN EL MARCO DE LA COOPERACIÓN POLICIAL Y JUDICIAL EN MATERIA PENAL

El Tratado de Lisboa ha creado, en virtud del artículo 16 del Tratado de Funcionamiento de la Unión Europea, una nueva base jurídica para un enfoque

modernizado y completo de la protección de datos y de la libre circulación de datos personales, que abarca asimismo la cooperación policial y judicial en materia penal.

La Decisión Marco 2008/977/JAI refleja las especificidades de la estructura de pilares anterior al Tratado de Lisboa y se caracteriza por su limitado ámbito de aplicación y por un conjunto de lagunas que se han convertido en fuente de inseguridad jurídica tanto para los ciudadanos como para las autoridades que han de aplicarla. Otro problema se encuentra en las dificultades encontradas a la hora de transponer la Decisión en los países de la Unión. Y no podemos olvidar que las Decisiones Marco carecen de efecto directo.

Frente a estos problemas, se ha constatado la necesidad de reforzar la coherencia del marco de protección de datos en el ámbito de la cooperación policial y judicial en materia penal, habida cuenta de la entrada en vigor del Tratado de Lisboa.

Ello se ha traducido en la 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[257]. Esta Directiva, que sustituiría a la Decisión Marco 2008/977/JAI, fija las normas sobre la protección de los datos personales tratados con fines de prevención, detección, investigación o persecución de delitos y para las actividades judiciales correspondientes.

[257] Bruselas, 25.1.2012 COM (2012) 10 final.

La propuesta de Directiva aplica los principios generales de la protección de datos a la cooperación policial y judicial en materia penal, siempre en total respeto de la naturaleza específica de cada uno de estos ámbitos. Establece condiciones y criterios mínimos armonizados para toda posible limitación de las reglas generales. Especialmente en cuanto a los derechos de los ciudadanos a ser informados cuando la policía y las autoridades judiciales manejen sus datos o accedan a ellos, ya que esas limitaciones son necesarias para la prevención, investigación, detección o enjuiciamiento efectivos de los delitos. Y establece también normas específicas adaptadas a la naturaleza característica de las actividades de los organismos con funciones coercitivas, incluida una distinción entre las distintas categorías de interesados, cuyos derechos pueden variar (como los testigos y los sospechosos).

Si centramos nuestro análisis en la cuestión de las transferencias internacionales, su regulación se contiene en el Capítulo V de la propuesta de Directiva (artículos 33 a 38), titulado *Transferencia de datos personales a terceros países u organizaciones internacionales*. Además se puede contar con el texto de varios de los Considerandos (los números 45, 46, 48 y 49 especialmente) de la Directiva que pueden clarificar el contenido su Capítulo V.

De acuerdo al Considerando 45, los Estados miembros deben velar por que una transferencia a un tercer país solo se lleve a cabo si es necesaria para la prevención, investigación, detección y enjuiciamiento de infracciones penales o la ejecución de sanciones penales, y si el responsable del tratamiento en el tercer país u organización internacional es una autoridad competente a tenor de la Directiva. Puede llevarse a cabo una transferencia en los casos en que la Comisión haya decidido que el tercer país o la

organización internacional de que se trate garantizan un nivel adecuado de protección, o cuando se hayan ofrecido unas garantías apropiadas.

La Comisión puede determinar, según el Considerando 46, con efectos para toda la Unión, que algunos terceros países, un territorio o un sector del tratamiento en un tercer país, o una organización internacional ofrecen un nivel adecuado de protección de datos, proporcionando así seguridad jurídica y uniformidad en toda la Unión en lo que se refiere a los terceros países u organizaciones internacionales que se considera aportan tal nivel de protección. En estos casos, se pueden realizar transferencias de datos personales a estos países sin tener que obtener ninguna otra autorización.

La Comisión también debe poder reconocer que un tercer país, un territorio, un sector del tratamiento en un tercer país, o una organización internacional no ofrece un nivel adecuado de protección de datos (Considerando 48). En consecuencia, debe prohibirse la transferencia de datos personales a dicho tercer país, salvo cuando se base en un acuerdo internacional, unas garantías apropiadas o una excepción. Deben establecerse los procedimientos para celebrar consultas entre la Comisión y dichos terceros países u organizaciones internacionales. Sin embargo, tal decisión de la Comisión se entenderá sin perjuicio de la posibilidad de llevar a cabo transferencias sobre la base de garantías apropiadas o de una excepción establecida en la Directiva.

El Considerando 49 dispone que las transferencias no basadas en una decisión de adecuación solo deben permitirse cuando se hayan invocado las garantías apropiadas en un instrumento jurídicamente vinculante que garantice la protección de los datos personales o cuando el responsable o encargado del tratamiento haya evaluado todas las circunstancias que rodean la operación de transferencia de datos o el conjunto de

operaciones de transferencia de datos y, basándose en esta evaluación, considere que existen las garantías apropiadas con respecto a la protección de los datos personales.

En los casos en que no existan razones para autorizar una transferencia, deben permitirse excepciones, si fuera necesario, para proteger el interés vital del interesado o de otra persona, o para proteger intereses legítimos del interesado en caso de que la legislación del Estado miembro que transfiere los datos personales así lo disponga, o cuando sea indispensable para prevenir una amenaza inminente y grave para la seguridad pública de un Estado miembro o de un tercer país, o en determinados casos a efectos de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, o en casos específicos para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial.

Centrándonos en el articulado del Capítulo V de la propuesta de Directiva, en el artículo 33, sobre Principios generales de las transferencias de datos personales, se regula que cualquier transferencia de datos personales por las autoridades competentes que sean o vayan a ser objeto de tratamiento tras su transferencia a un tercer país o a una organización internacional, incluidas las transferencias ulteriores a otro tercer país u otra organización internacional, solo podrá realizarse si:

a) la transferencia es necesaria para la prevención, investigación, detección o enjuiciamiento de infracciones penales o para la ejecución de sanciones penales; y
b) el responsable y el encargado del tratamiento cumplen las condiciones establecidas en el presente capítulo.

En el artículo 34 se contemplan las transferencias con una decisión de adecuación. Los Estados miembros dispondrán que una transferencia de datos personales a un tercer país o una organización internacional podrá realizarse cuando la Comisión haya decidido que el tercer país, o un territorio o un sector de tratamiento en ese tercer país, o la organización internacional de que se trate garantizan un nivel de protección adecuado. Dichas transferencias no requerirán nuevas autorizaciones.

Cuando no exista una decisión adoptada, la Comisión evaluará la adecuación del nivel de protección, tomando en consideración los elementos siguientes:

a) El Estado de Derecho, la legislación pertinente en vigor, tanto general como sectorial, en particular en lo que respecta a la seguridad pública, la defensa, la seguridad nacional, el Derecho penal, las medidas de seguridad en vigor en el país de que se trate o aplicables a la organización internacional en cuestión, así como los derechos efectivos y exigibles, incluido el derecho de recurso administrativo y judicial efectivo de los interesados, en particular los residentes en la Unión cuyos datos personales estén siendo transferidos.
b) La existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el tercer país u organización internacional de que se trate, encargadas de garantizar el cumplimiento de las normas en materia de protección de datos, de asistir y asesorar a los interesados en el ejercicio de sus derechos y de cooperar con las autoridades de control de la Unión y de los Estados miembros.
c) Los compromisos internacionales asumidos por el tercer país o la organización internacional de que se trate.

La Comisión podrá decidir que un tercer país, o un territorio o un sector de tratamiento de datos en ese tercer país, o una organización internacional garantizan un nivel de protección adecuado.

El acto de ejecución especificará su ámbito de aplicación geográfica y sectorial, y, cuando proceda, determinará cuál es la autoridad de control.

La Comisión podrá decidir que un tercer país, o un territorio o un sector de tratamiento de datos en ese tercer país, o una organización internacional no garantizan un nivel de protección adecuado, en particular en los casos en que la legislación pertinente, tanto general como sectorial, en vigor en el tercer país o aplicable a la organización internacional en cuestión, no garantice derechos efectivos y exigibles, incluido el derecho de recurso administrativo y judicial efectivo de los interesados, en particular aquellos cuyos datos personales estén siendo transferidos. En este caso los Estados miembros prohibirán toda transferencia de datos personales al tercer país, o a un territorio o un sector de tratamiento de datos en ese tercer país, o a la organización internacional de que se trate. La Comisión entablará consultas, en su debido momento, con el tercer país o la organización internacional con vistas a poner remedio a la situación resultante de la decisión adoptada.

La Comisión publicará en el Diario Oficial de la Unión Europea una lista de los terceros países, territorios y sectores de tratamiento de datos en un tercer país o una organización internacional para los que haya decidido que está o no está garantizado un nivel protección adecuado.

El artículo 35 está dedicado a las transferencias mediante garantías apropiadas. Cuando la Comisión no haya adoptado una decisión con arreglo a lo dispuesto en el

artículo 34, los Estados miembros dispondrán que podrá tener lugar una transferencia de datos personales a un destinatario en un tercer país o una organización internacional cuando se hayan aportado garantías apropiadas con respecto a la protección de datos personales en un instrumento jurídicamente vinculante o el responsable o el encargado del tratamiento hayan evaluado todas las circunstancias que concurren en la transferencia de datos personales y hayan llegado a la conclusión de que existen garantías apropiadas con respecto a la protección de datos personales. La decisión tomada en base a esta evaluación del responsable o del encargado deberá ser adoptada por personal debidamente autorizado. Estas transferencias deberán documentarse y la documentación se pondrá a disposición, previa solicitud, de la autoridad de control.

El artículo 36, inspirándose en el artículo 26 de la Directiva 95/46/CE y el artículo 13 de la Decisión Marco 2008/977/JAI, regula las excepciones. No obstante lo dispuesto en los artículos 34 y 35, los Estados miembros dispondrán que podrá procederse a la transferencia de datos personales a un tercer país o una organización internacional en caso de que concurra alguna de estas circunstancias:

a) La transferencia sea necesaria para proteger los intereses vitales del interesado o de otra persona.
b) La transferencia sea necesaria para salvaguardar intereses legítimos del interesado cuando así lo disponga el Derecho del Estado miembro que transfiere los datos personales.
c) La transferencia de los datos sea esencial para prevenir una amenaza inminente 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 concretos para el reconocimiento, el ejercicio o la defensa de un derecho en un procedimiento judicial relativo a la prevención, investigación, detección o enjuiciamiento de una infracción penal o la ejecución de una sanción penal específica.

De acuerdo al artículo 37, los Estados miembros dispondrán que el responsable del tratamiento informará al destinatario de los datos personales de cualquier limitación al tratamiento y tomará todas las medidas razonables para garantizar que se cumplan dichas limitaciones.

El contenido del último de los artículos del Capítulo, el 38, tiene en cuenta la Recomendación de la OCDE relativa a la cooperación transfronteriza en la aplicación de las legislaciones que protegen la privacidad, de 12 de junio de 2007. Con la intención de que esa cooperación internacional con los terceros países y las organizaciones internacionales sea efectiva, la Comisión y los Estados miembros tomarán medidas apropiadas para:

a) Crear mecanismos de cooperación internacional eficaces que faciliten la aplicación de la legislación relativa a la protección de datos personales.
b) Prestarse mutuamente asistencia a escala internacional en la aplicación de la legislación relativa a la protección de datos personales, en particular mediante la notificación, la remisión de reclamaciones, la asistencia en las investigaciones y

el intercambio de información, a reserva de las garantías apropiadas para la protección de los datos personales y otros derechos y libertades fundamentales.

c) Procurar la participación de las partes interesadas pertinentes en los debates y actividades destinados a reforzar la cooperación internacional en la aplicación de la legislación relativa a la protección de datos personales.

d) Promover el intercambio y la documentación de la legislación y las prácticas en materia de protección de datos personales.

A estos efectos la Comisión tomará medidas apropiadas para impulsar las relaciones con terceros países u organizaciones internacionales y, en particular, sus autoridades de control, cuando haya decidido que garantizan un nivel de protección adecuado.

3. OPINIÓN DEL GRUPO DE TRABAJO SOBRE LA PROPUESTA DE DIRECTIVA

El Grupo de Trabajo ha manifestado sus opiniones sobre la propuesta de Directiva en el Documento WP 191[258]. Las observaciones efectuadas en cuanto a las transferencias internacionales, se centran en cuatro puntos:

a) Principios generales de transferencia y transferencia sucesiva

El artículo 33 contiene disposiciones para las transferencias originales y las transferencias sucesivas de datos personales a terceros países u organizaciones internacionales. Es preciso distinguir claramente entre esas situaciones, posibilitando

[258] Dictamen 01/2012 sobre las propuestas de reforma de la protección de datos, WP 191, adoptado el 23 de marzo de 2012.

restricciones adicionales para las transferencias sucesivas y cuidando, por ejemplo, que haya una relación directa con el objetivo para el que se recogieron originalmente los datos y el consentimiento previo de la autoridad que los remita.

b) Decisiones de adecuación negativas

El Grupo de Trabajo no ve claro qué objeto tienen las decisiones de falta de adecuación ni el modo en que estas pueden funcionar en la práctica. La redacción sugiere que una decisión de falta de adecuación bloquearía todas las transferencias internacionales a un determinado país tercero, organización internacional o sector de tratamiento. Pero del artículo 34 y del artículo 35 puede también interpretarse que se autorizan transferencias a países declarados no adecuados si la autoevaluación de adecuación realizada por el responsable o el encargado del tratamiento arroja un resultado satisfactorio y se han acordado salvaguardias apropiadas. Se insta, pues, al legislador europeo a que adopte disposiciones para aclarar las consecuencias que tendría una tal decisión de no adecuación y lo que significarían en la práctica.

c) Transferencias mediante salvaguardas apropiadas

El artículo 35 de la Directiva prevé la posibilidad de transferir datos personales a terceros países u organizaciones internacionales en situaciones en que la Comisión no haya adoptado una decisión de adecuación. Si dichas transferencias se realizan sobre la base de una autoevaluación, la autoridad competente debe garantizar que se establezcan las salvaguardias apropiadas en un instrumento jurídicamente vinculante. El proceso conducente a la evaluación debe documentarse plenamente y ponerse a disposición de la autoridad de control si ésta lo solicitara.

d) Excepciones

El Grupo de Trabajo ve con inquietud las excepciones establecidas para transferir datos personales sin decisión de adecuación y salvaguardias apropiadas, especialmente las que figuran en las letras c), d) y e) del artículo 36. Esas excepciones pueden dar lugar a muchas transferencias internacionales en casos concretos que simplemente se consideren *necesarias*. Debe quedar claro que a toda excepción deberá dársele una interpretación restrictiva de modo que las transferencias que se realicen por estos conceptos sean la excepción y no la norma. El Grupo de Trabajo considera por ello que la redacción del artículo 36, letras c), d) y e), debe acotar las posibilidades de transferencias internacionales en casos particulares.

Por otra parte, el Grupo de Trabajo hace observar que no se incluye obligación alguna para garantizar la necesidad de documentar las excepciones previstas en el artículo 36. Esto dificultaría, si no lo imposibilitaba, que el supervisor comprobara si el responsable o el encargado del tratamiento habían respetado las condiciones de las excepciones.

4. DICTAMEN DEL SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS SOBRE LA PROPUESTA DE DIRECTIVA

El Supervisor Europeo de Protección de Datos ha manifestado sus opiniones sobre la propuesta de Directiva en su Dictamen de 7 de marzo de 2012 sobre el paquete legislativo de reforma de la protección de datos[259].

[259] Puede encontrarse el Resumen del Dictamen de 7 de marzo del SEPD en el DOUE C 192 de 30 de junio de 2012, o bien su versión íntegra en el sitio web del SEPD **http://www.edps.europa.eu**

Nos centraremos en las cuatro propuestas efectuadas en materia de transferencias a terceros países:

a) En el artículo 33 propone añadir el requisito de que la transferencia sólo puede realizarse si el responsable del tratamiento en el tercer país o la organización internacional es la autoridad competente en el sentido de la Directiva propuesta.

b) En el artículo 35 sugiere la eliminación de que pueda tener lugar una transferencia cuando el responsable o el encargado del tratamiento hayan evaluado todas las circunstancias que concurren en la transferencia de datos personales y hayan llegado a la conclusión de que existen garantías apropiadas con respecto a la protección de datos personales.

Si no se elimina esta opción, como mínimo, incluir el requisito de una autorización previa de la autoridad de control.

c) En cuanto a las excepciones del artículo 36 sugiere aclarar en un considerando que es necesario interpretar de manera restrictiva toda excepción utilizada para justificar una transferencia y que no debe permitirse la transferencia frecuente, masiva y estructural de datos de carácter personal. Deberían añadirse garantías adicionales como la obligación de documentar de manera específica las transferencias.

d) En caso de adoptar una decisión negativa sobre la adecuación, las transferencias deberían estar basadas en la existencia de un acuerdo internacional jurídicamente vinculante que permita las transferencias en condiciones específicas que garanticen una protección adecuada, o en las excepciones contempladas en el artículo 36, letras a) o c), es decir que la transferencia sea necesaria para proteger los intereses vitales del

interesado o de otra persona o que sea esencial para prevenir una amenaza inminente y grave para la seguridad pública de un Estado miembro o de un tercer país.

5. DICTAMEN DEL COMITÉ DE LAS REGIONES SOBRE LA PROPUESTA DE DIRECTIVA

El Comité de las Regiones ha manifestado su opinión crítica sobre la propuesta de Directiva en su Dictamen de 10 de octubre de 2012[260].

Expone sus dudas sobre la conformidad de una reglamentación también del tratamiento de datos de carácter exclusivamente nacional en el marco de la propuesta de Directiva relativa al ámbito judicial y policial respecto de las competencias legislativas de la Unión Europea, así como sobre su idoneidad según el principio de subsidiariedad y el principio de proporcionalidad.

Según su opinión, además de las funciones en la lucha contra el terrorismo, la delincuencia organizada o los delitos cibernéticos, persisten amplios paquetes de datos de la policía y los servicios de seguridad que se tratan tan solo a escala nacional y que, por ello, no exigen reglamentación alguna en el ámbito europeo.

Por otro lado manifiesta su sorpresa por el hecho de que las instituciones y órganos europeos, empezando por Eurojust y Europol, estén excluidos del ámbito de aplicación de la Directiva.

En el ámbito de las transferencias internacionales, el Dictamen muestra su acuerdo en que no conviene limitar o impedir indebidamente los intercambios de datos con

[260] Dictamen del Comité de las Regiones – Paquete sobre la protección de datos. (2012/C 391/13). (DOUE C 391 de 18 de diciembre de 2012).

terceros países. Sin embargo entiende que se han de crear las salvaguardias necesarias para aquellas excepciones relacionadas con transferencias internacionales en casos individuales. Así propone que se añada un párrafo adicional en el artículo 36 con el siguiente contenido: "La utilización de estas excepciones deberá documentarse adecuadamente".

6. OPINIÓN PERSONAL SOBRE LA PROPUESTA DE DIRECTIVA

El Tratado de Maastricht (1992) introdujo una estructura institucional que se ha mantenido hasta la entrada en vigor del Tratado de Lisboa, el uno de diciembre de 2009. Dicha estructura institucional estaba compuesta por tres *pilares*:

- El pilar comunitario, que correspondía a las tres comunidades: la Comunidad Europea, la Comunidad Europea de la Energía Atómica (Euratom) y la antigua Comunidad Europea del Carbón y del Acero (CECA) (primer pilar).
- El pilar correspondiente a la política exterior y de seguridad común, que estaba regulada en el título V del Tratado de la Unión Europea (segundo pilar).
- El pilar correspondiente a la cooperación policial y judicial en materia penal, cubierta por el título VI del Tratado de la Unión Europea (tercer pilar).

Estos tres pilares funcionaban siguiendo procedimientos de decisión diferentes: procedimiento comunitario para el primer pilar y procedimiento intergubernamental para los otros dos.

El Tratado de Lisboa elimina esta estructura de pilares en beneficio de la creación de la Unión Europea (UE). Sin embargo, el método intergubernamental sigue aplicándose a la política exterior y de seguridad común.

El tratamiento de datos por las autoridades policiales y judiciales en materia penal en el ámbito de la Unión Europea está regulado en la actualidad por una norma aprobada antes de la entrada en vigor del Tratado de Lisboa, la Decisión Marco 2008/977/JAI. Como es lógico su aprobación siguió los cauces del procedimiento intergubernamental establecidos para el tercer pilar.

No podemos pasar por alto que todos los Estados miembros de la Unión han ratificado el Convenio 108 del Consejo de Europa (Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal), si bien algunos de ellos no han hecho lo mismo con su Protocolo Adicional[261]. El Convenio 108 es aplicable, sin excepción, a todos los tratamientos de datos, sean de carácter privado o de carácter público. Sin embargo el artículo 9.2 del Convenio posibilita la no aplicación de algunas de sus disposiciones (artículo 5 sobre calidad de los datos, artículo 6 sobre categorías particulares de datos y artículo 8 sobre garantías complementarias para la persona concernida) cuando tal excepción, prevista por la ley de la Parte, constituya una medida necesaria en una sociedad democrática:

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 otras personas.

La entrada en vigor de la Decisión Marco 2008/977/JAI significó un paso adelante en la protección de datos dentro de su campo de acción. Sin embargo se trató de una

[261] No han ratificado el Protocolo Adicional: Bélgica, Dinamarca, Grecia, Italia y Reino Unido.

regulación poco ambiciosa por diferentes razones. En primer lugar podemos criticar su limitado ámbito de aplicación. La Decisión Marco solo se aplica al tratamiento transfronterizo de datos y no a las actividades de tratamiento por parte de las autoridades policiales y judiciales a nivel puramente nacional. Para otorgar mayor complejidad a la materia, podemos encontrar muchos casos en que sea difícil de determinar si nos encontramos ante un tratamiento meramente nacional o bien de tipo transfronterizo. Incluso puede darse el caso de un tratamiento de carácter nacional que posteriormente puede derivar en un intercambio de datos con otro u otros países.

En segundo lugar podemos mencionar el amplio margen de maniobra a los Estados miembros para transponer las disposiciones de la Decisión Marco a su Derecho interno. Esto ha originado unas divergencias de gran calado entre las normas de los diferentes países de la UE.

En tercer lugar podemos mencionar la falta de mecanismos de interpretación común de la Decisión Marco. La Directiva 95/46/CE creó el Grupo de Trabajo de su artículo 29 para, entre otras funciones, efectuar una interpretación común del contenido de la propia Directiva. En la Decisión Marco no existe ningún instrumento similar.

En cuarto lugar podemos criticar el instrumento elegido para efectuar dicha regulación: una Decisión Marco. La Comisión Europea carece de competencias para exigir el cumplimiento de las disposiciones de las Decisiones Marco. En este contexto es evidente que no todos los países miembros han actuado con la misma voluntad a la hora de transponer esta regulación a su normativa interna.

En quinto lugar podemos destacar que la Decisión Marco contiene una excepción demasiado amplia al principio de limitación de la finalidad. Así en el artículo 3.2 se autoriza al tratamiento posterior para otros fines en la medida en que:

a) el tratamiento no sea incompatible con los fines para los que se recogieron los datos;
b) las autoridades competentes estén autorizadas a tratar los datos para tales otros fines con arreglo a la normativa aplicable, y
c) el tratamiento sea necesario para ese otro fin y proporcionado a él.

En sexto lugar podemos citar la ausencia de disposiciones que prevean una diferenciación de las distintas categorías de datos en función de su grado de exactitud o fiabilidad, y en particular una diferenciación de los datos basados en hechos de los basados en opiniones o valoraciones personales, así como una diferenciación de las distintas categorías de interesados (delincuentes, sospechosos, victimas, testigos, etc.).

Las limitaciones mencionadas (y otras a las que no hemos hecho referencia) han exigido una revisión a fondo de la normativa actual a efecto de garantizar un nivel elevado y sistemático de protección de los datos que fomente la confianza mutua entre la policía y las autoridades judiciales de los distintos Estados miembros, contribuyendo con ello a mejorar la libre circulación de datos y la cooperación efectiva entre la policía y las autoridades judiciales.

A la hora de elegir el instrumento legal, la Comisión ha propuesto que el nuevo marco en materia de protección de datos conste de:

- Un Reglamento (que sustituye a la Directiva 95/46/CE) en el que se fija el marco jurídico general de protección de datos de la UE.
- Una Directiva (que sustituye a la Decisión Marco 2008/977/JAI), que fija las normas sobre la protección de los datos personales tratados con fines de prevención, detección, investigación o persecución de delitos y para las actividades judiciales correspondientes.

La adopción de dos regímenes distintos, uno para asuntos civiles, y otro de asuntos penales y orden público ha sido criticada en amplios sectores. El Consejo de la Abogacía Europea ha reclamado a las instituciones europeas la creación de un único régimen de protección de datos[262]. Opina, al igual que el Supervisor Europeo de Protección de Datos, que el procesamiento de datos en el ámbito de la cooperación judicial y policial en asuntos penales requiere al menos tanta protección como la prevista en el Reglamento, en lugar de una protección inferior como la que se ha establecido en la Directiva.

La Comisión entiende que su propuesta asegura un alto nivel de protección de los datos personales por medio de una Directiva que:

- aplique los principios generales de la protección de datos a la cooperación policial y judicial en materia penal, siempre en total respeto de la naturaleza específica de cada uno de estos ámbitos;

[262] Véase el documento "*Prise de position du CCBE concernant le paquet de réformes de la protection des données COM (2012) 11 et COM(2012) 10*" de fecha 07.09.2012. Documento descargable desde la página de la organización: **www.ccbe.eu**

- establezca condiciones y criterios mínimos armonizados para toda posible limitación de las reglas generales; esto se refiere específicamente a los derechos de los ciudadanos a ser informados cuando la policía y las autoridades judiciales manejen sus datos o accedan a ellos; esas limitaciones son necesarias para la prevención, investigación, detección o enjuiciamiento efectivos de los delitos;
- establezca normas específicas adaptadas a la naturaleza característica de las actividades de los organismos con funciones coercitivas, incluida una distinción entre las distintas categorías de interesados, cuyos derechos pueden variar (como los testigos y los sospechosos).

En este punto podemos expresar nuestra visión crítica con respecto a la elección de la Directiva como instrumento normativo. La propia Comisión Europea expresó en multitud de ocasiones su malestar con la transposición de la Directiva 95/46/CE en buena parte de los Estados miembros. Esa incorrecta transposición llevó a una fragmentación de las legislaciones nacionales imposibilitando el establecimiento de un marco armonizado y coherente en materia de protección de datos. Pero ese mal precedente no ha impedido que se elija de nuevo una Directiva para la regulación del tratamiento de datos personales por las autoridades competentes a efectos de la prevención, investigación, detección y enjuiciamiento de infracciones penales o a la ejecución de sanciones penales, y a la libre circulación de estos datos.

Otro punto que puede causar conflicto se encuentra en la dificultad de distinguir el ámbito de aplicación del nuevo Reglamento (como instrumento general de protección de datos personales) y el de la Directiva. Hay una serie de actividades en las que las autoridades de los diferentes Estados miembros tienen objetivos de ejecución legal o

simplemente administrativos (así por ejemplo en materia de aduanas, inmigración o medio ambiente). Ello supondría que la Directiva y el Reglamento pueden aplicarse a la misma institución en Estados distintos, lo que no casa con la pretendida armonización y coherencia.

En cuanto a los principios del tratamiento de datos, la Directiva no incluye elementos importantes sobre retención de datos personales (y periodos de retención), transparencia frente a las personas, actualización de datos personales y garantía de adecuación, pertinencia y suficiencia. También están ausentes las disposiciones sobre responsabilidad que requieran que el responsable del tratamiento demuestre el cumplimiento de las normas.

La Directiva tampoco establece un derecho para oponerse al tratamiento de datos personales. Ello es especialmente importante para el caso de que determinadas personas puedan limitar el tratamiento ulterior de sus datos en el momento en que finalice el proceso legal.

Ya en el campo de las transferencias de datos, el responsable del tratamiento no tiene obligación de informar al interesado para transferir datos personales a terceros países.

Por otro lado nos encontramos con una figura difícil de entender: la decisiones de adecuación negativas del artículo 33.6 de la Directiva. De la lectura de dicho artículo parece entenderse que una decisión de falta de adecuación bloquearía todas las transferencias internacionales a un determinado país tercero, organización internacional o sector del tratamiento. Pero del artículo 34.6 y 35.1 podemos interpretar que se autorizan transferencias a países declarados no adecuados tras una autoevaluación

positiva de adecuación realizada por el responsable o el encargado del tratamiento junto a salvaguardias apropiadas.

También podemos destacar las excepciones del artículo 36 para transferir datos personales sin decisión de adecuación ni salvaguardias apropiadas. A menos que el contenido de este artículo se interprete de forma restrictiva, es posible que se convierta en el instrumento habitual a la hora de efectuarse transferencias internacionales. La excepción puede convertirse en la regla habitual.

Pese a todas las limitaciones que encontramos en la propuesta de Directiva, no seríamos justos si no se reconoce el gran paso adelante que su entrada en vigor supondrá para la protección de datos personales. Todavía estamos a tiempo para que se efectúen modificaciones en el texto de la propuesta de Directiva. Si hay voluntad en las instituciones europeas, muchas de las deficiencias criticadas por el Grupo de Trabajo del art. 29, el SEPD y otras organizaciones pueden ser subsanadas.

Incluso en el caso de que el texto definitivo de la Directiva coincidiera con la propuesta de 25 de enero de 2012, está claro que se podría celebrar como una gran mejora. Partiendo de un punto tan bajo como es la Decisión Marco 2008/977/JAI cualquier otro texto normativo, incluso con grandes carencias, significa un avance importante.

CAPÍTULO VI

CONCLUSIONES

CONCLUSIONES

Para finalizar el presente trabajo de investigación, dedicaremos las últimas páginas a recoger las conclusiones que derivan del estudio acometido. Con ellas se pretende dar una visión global de las diferentes cuestiones que se han abordado a lo largo del trabajo, de los problemas suscitados y, en su caso, de las posibles soluciones que cabría dar a los mismos.

Podríamos haber dado formatos muy diversos a las conclusiones de la tesis doctoral, pero la solución que nos ha parecido más lógica es la agrupación en cinco partes siguiendo el orden de los apartados de la tesis:

- Justificación de la necesidad de estudio de la transferencia internacional de datos.
- Las soluciones normativas, diferenciando ente nivel adecuado y no adecuado de protección.
- Procedimientos.
- Cooperación policial y judicial.
- Valoración personal.

Sin más preámbulo pasamos a analizar cada una de estas partes.

I. La protección de datos de carácter personal es un campo del derecho de nacimiento muy reciente. Su desarrollo ha estado muy ligado a la evolución de la informática. La posibilidad de almacenar cantidades masivas de datos y de gestionarlos de forma automatizada ha obligado a que surgiese un nuevo derecho para la protección de los datos de carácter personal. Además este campo del derecho se ha consolidado en un periodo de tiempo muy breve.

El poco tiempo transcurrido desde que se implantan las primeras normas reguladoras de la protección de datos ha impedido la consolidación de un cuerpo doctrinal suficientemente amplio y de una jurisprudencia que ayuden a clarificar los puntos más complejos de esa regulación legal. En consecuencia, a la hora de interpretar las normas, ya sean de carácter español o europeo, aparecen dudas que en muchos casos no podrán ser resueltas por la ausencia de elementos que otorguen una relativa seguridad en su respuesta. Y si nos centramos en el ámbito de las transferencias internacionales de datos, este problema todavía es mucho más importante.

El gran avance de la tecnología, junto con el fenómeno de la globalización, ha llevado a un aumento muy importante de los flujos transfronterizos de datos. Las empresas multinacionales necesitan que la información pueda fluir entre sus diferentes sedes. Pero también necesitan de la contratación de servicios con empresas de otros países en donde los costes son más reducidos. Para que se puedan prestar estos servicios, en muchos casos hay que efectuar una transferencia de datos personales. Sin embargo no se ha dado una respuesta legislativa adecuada al movimiento internacional de datos.

El Convenio nº 108, la Directiva 95/46/CE y las normas nacionales que han transpuesto a ésta última (LOPD y RLOPD) han establecido límites a las transferencias internacionales para evitar la desprotección de los titulares de los datos. Se quiere evitar que la legislación interna de un país en materia de protección de datos pueda ser burlada mediante la transferencia a otro país en donde la legislación sea menos exigente (o incluso que no exista legislación alguna en este campo).

La normativa europea y la española que regula las transferencias internacionales de datos de datos, podríamos calificarla como insuficiente y poco clara. Además es una gran desconocida, no sólo para la gran mayoría de ciudadanos sino también para muchos de los investigadores en el campo de la protección de datos. Pese a la gran importancia que tiene esta materia son muy pocos los textos que han reservado un espacio para su estudio.

En esta tesis doctoral se ha intentado dar un poco de luz a la regulación actual y a la que previsiblemente será la nueva normativa en un plazo breve, de las transferencias internacionales en sus diferentes vertientes.

Como consecuencia de la falta de manuales referidos a la materia investigada, se ha recurrido fundamentalmente a las fuentes primarias de información, lo cual puede ser más laborioso, pero también más satisfactorio a la hora de elaborar la investigación.

El trabajo analiza a fondo la normativa vigente. Por un lado encontramos la norma fundamental: la Directiva 95/46/CE. Por otro lado tenemos la ley de transposición interna, la LOPD, así como sus normas de desarrollo, esencialmente el RLOPD y la Instrucción 1/2000.

A la vez se tiene en cuenta la propuesta de Reglamento de protección de datos de la UE, que con toda probabilidad se convertirá en la nueva normativa de la Unión en un próximo futuro.

En otro orden, se efectúa el análisis de un gran número de Documentos de Trabajo del Grupo del artículo 29. La excepcional labor de investigación y estudio plasmada en estos Documentos de Trabajo ha permitido un desarrollo progresivo del derecho

fundamental a la protección de datos personales en Europa. Y de forma particular se ha avanzado de forma muy intensa en cuanto a las transferencias internacionales. Incluso herramientas desconocidas por la legislación han sido desarrolladas de forma muy acertada en base a los diferentes Documentos de Trabajo que ha elaborado el Grupo. Así por ejemplo, las normas corporativas vinculantes.

También ha tenido mucha relevancia el estudio de la documentación elaborada por la Agencia Española de Protección de Datos, de otras Agencias europeas (algunas de ellas muy activas como es el caso de la Comisión Nacional de Informática y Libertades francesa o la Oficina del Comisionado de Información Británico) y del Supervisor Europeo de Protección de Datos.

Ha sido esencial el examen de las Decisiones en las que la Comisión ha reconocido el nivel adecuado de protección al grupo de países que forman la llamada “lista blanca”.

Es relevante también la indagación efectuada en los textos de los Acuerdos PNR alcanzados con Estados Unidos, Canadá y Australia, así como la documentación que hace referencia al conflicto entre las diferentes instituciones de la Unión Europea con motivo de esos Acuerdos.

Y no podemos olvidar, por su importancia fundamental, el conjunto de cláusulas contractuales tipo que ha aprobado la Comisión Europea.

Junto a todas las fuentes mencionadas se puede citar también la lectura de un número muy considerable de artículos de revistas y el seguimiento de las noticias relacionadas con el tema investigado que aparecen día a día en la prensa escrita.

II. El RLOPD define como transferencia internacional de datos a aquel tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español. En este tratamiento aparecen dos figuras esenciales:

- Exportador de datos personales: la persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español que realice, conforme a lo dispuesto en el presente Reglamento, una transferencia de datos de carácter personal a un país tercero.
- Importador de datos personales: la persona física o jurídica, pública o privada, u órgano administrativo receptor de los datos en caso de transferencia internacional de los mismos a un tercer país, ya sea responsable del tratamiento, encargada del tratamiento o tercero.

Nos encontraremos ante una cesión o comunicación de datos cuando el importador de los mismos se convierta en responsable de tratamiento, es decir, cuando tenga capacidad de decisión sobre la finalidad, contenido y uso del tratamiento.

Se tratará de la realización de un tratamiento de datos por cuenta del responsable del fichero, cuando el importador trate datos personales por cuenta de aquél como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio.

La transferencia internacional de datos se podrá efectuar a países que proporcionen un nivel adecuado de protección o bien a países que no lo proporcionen. Ante la poca precisión que se obtiene de la Directiva 95/46/CE, de la LOPD y del RLOPD sobre el concepto de protección adecuada hemos tenido que recurrir en la presente investigación a los Documentos de Trabajo elaborados por el Grupo del artículo 29 de la Directiva. Hemos encontrado una respuesta bien elaborada especialmente en el WP 12. En este documento se analizan las circunstancias que podrán determinar si nos encontramos (o no) ante un nivel de protección adecuado (que no equivalente).

La Comisión Europea está facultada por la Directiva 95/46/CE para hacer constar que un país tercero garantiza un nivel de protección adecuado, vinculando sus decisiones al conjunto de países que forman el EEE. El número de países que han obtenido la decisión favorable por parte de la Comisión es muy reducido: Suiza, Estados Unidos (principios de puerto seguro), Canadá (respecto de las entidades sujetas a la ley canadiense de protección de datos), Argentina, Guernesey, Isla de Man, Jersey, Islas Feroe, Andorra, Israel, Uruguay y Nueva Zelanda. No es previsible que esta lista tenga mucho crecimiento en el medio plazo.

A nivel español, la LOPD y el RLOPD reconocen la potestad de la AEPD para reconocer el carácter adecuado del nivel de protección que ofrece un país. Sin embargo desde la entrada en vigor de la LOPD no se ha producido ninguna resolución en dicho sentido por parte del Director de la AEPD.

Las transferencias internacionales de datos a aquellos países que tienen un nivel de protección adecuado a juicio de la Comisión Europea no precisan de la autorización por parte del Director de la AEPD.

El reconocimiento del nivel adecuado de protección por parte de la Comisión puede ser general para un país o bien parcial. Son decisiones de reconocimiento parcial por parte de la Comisión las que afectan a Estados Unidos y a Canadá. En el caso del primer país, la decisión reconoce el nivel adecuado sólo a aquellas entidades adheridas al sistema de puerto seguro. En el caso de Canadá, la decisión reconoce dicho nivel solamente a aquellas que están sujetas a la ley canadiense de protección de datos.

Los Acuerdos de puerto seguro con los Estados Unidos constan de siete principios básicos junto a un conjunto de preguntas más frecuentes. Se entiende que aquellas entidades que aceptan su contenido y se someten a los organismos de control americanos que figuran en los Acuerdos, ofrecen un nivel adecuado de protección.

En la propuesta de Reglamento de protección de datos de la UE encontramos pocos cambios para las transferencias internacionales de datos a países con nivel adecuado de protección. Como señalaremos más adelante, las modificaciones más relevantes se producirán en las transferencias a estados que no proporcionan un nivel adecuado de protección.

Mucho enfrentamiento se ha creado por la transmisión de datos de los pasajeros (PNR) a los Estados Unidos (y en menor medida a Canadá y Australia). El conflicto institucional en la Unión Europea ha durado casi una década. La Comisión Europea adoptó el 14 de mayo de 2004 la Decisión 2004/535/CE, en la que se otorgaba un nivel de protección adecuado al tratamiento que las autoridades de EE.UU. efectuarían con los datos de los pasajeros. Tres días después el Consejo adoptó la Decisión 2004/496/CE por la que se aprobaba la celebración de un Acuerdo entre la Unión Europea y los Estados Unidos.

El Grupo de Trabajo del art. 29, el SEPD y el Parlamento Europeo manifestaron su disconformidad con el Acuerdo alcanzado, presentando éste último dos recursos de anulación ante el Tribunal de Justicia de la Unión Europea. Fruto de este procedimiento se procedió a la anulación de la Decisión 2004/496/CE del Consejo y la Decisión 2004/535/CE de la Comisión.

Desde ese momento continuó la batalla entre la Comisión y el Consejo por una parte y el Parlamento por otra. La solución no llegó hasta que el 13 de diciembre de 2011 el Consejo adoptó un nuevo Acuerdo sobre la transmisión de los registros de nombres de los pasajeros (PNR), el 14 de diciembre de 2011 la UE y los EE.UU. firmaron dicho Acuerdo y el 19 de abril de 2012 el Parlamento Europeo ha dado su aprobación al mismo.

A pesar de las duras críticas por parte del Grupo de Trabajo y del SEPD al Acuerdo alcanzado, éste ha entrado en vigor en julio de 2012. Las transferencias de PNR a Estados Unidos continúan siendo un problema mal resuelto y del que se desconoce el final.

Centrándonos ahora en las transferencias internacionales a países que no proporcionan un nivel adecuado de protección, el artículo 70 del RLOPD exige para poder efectuarlas la autorización del Director de la AEPD. Esta autorización podrá ser otorgada en caso de que el responsable del tratamiento aporte un contrato escrito, celebrado entre el exportador y el importador, en el que consten las necesarias garantías de respeto a la protección de la vida privada de los afectados y a sus derechos y libertades fundamentales y se garantice el ejercicio de sus respectivos derechos. También podrá otorgarse la autorización para la transferencia internacional en el seno

de grupos multinacionales de empresas cuando hubiesen sido adoptados por los mismos normas o reglas internas en que consten las necesarias garantías de respeto a la protección de la vida privada y el derecho fundamental a la protección de datos de los afectados y se garantice asimismo el cumplimiento de los principios y el ejercicio de los derechos reconocidos en la normativa española sobre protección de datos.

La AEPD diseñó una estructura de reglas contractuales en la Instrucción 1/2000, pero tuvieron en la práctica una vida muy efímera. Tan pronto como fueron apareciendo las cláusulas contractuales tipo de la Comisión Europea cesó el uso de las primeras.

La Comisión Europea ha aprobado cláusulas contractuales tipo entre responsables de tratamiento:

• Decisión 2001/497/CE, de 15 de junio de 2001 relativa a cláusulas contractuales tipo para la transferencia de datos personales a un tercer país.

• Decisión 2004/915/CE, de 27 de diciembre de 2004, por la que se modifica la Decisión 2001/497/CE, de 15 de junio de 2001.

Y también para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países:

• Decisión 2002/16/CE, de 27 de diciembre de 2001 relativa a cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países. (Derogada a partir de 15 de mayo de 2010).

• Decisión 2010/87/UE de la Comisión, de 5 de febrero de 2010, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados

del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE.

A estas cláusulas contractuales tipo debemos añadir las recientemente aprobadas por la AEPD para el caso de transferencias internacionales en el caso de subcontratación de servicios entre encargados establecidos en España y subencargados radicados en terceros países. Están basadas en las cláusulas de la Decisión 2010/87/UE, pero éstas sólo contemplaban que el exportador de datos pudiera ser un responsable del tratamiento. En cambio las cláusulas aprobadas por la AEPD están previstas para el caso de que el exportador de datos sea un encargado del tratamiento.

Como solución alternativa para las transferencias internacionales dentro de un mismo grupo multinacional, también se podrán autorizar transferencias entre sus sociedades, cuando hubieran sido adoptadas normas o reglas internas vinculantes para las empresas del grupo y exigibles conforme al ordenamiento jurídico español.

La Directiva 95/46/CE se ha convertido en un problema para el comercio internacional, especialmente en el ámbito de los grupos multinacionales. Ha sido necesario buscar el instrumento que permitiera efectuar transferencias internacionales con mayor flexibilidad que las cláusulas contractuales, en el seno de estos grupos. Las reglas corporativas vinculantes constituyen una alternativa a las cláusulas contractuales tipo, ya que permiten asegurar un nivel de protección suficiente a los datos transferidos fuera de la UE. En este sentido también constituyen una alternativa a los principios de Puerto Seguro para las transferencias a Estados Unidos.

Las reglas corporativas vinculantes no deben considerarse como una panacea en el contexto de las transferencias internacionales, sino sólo como un instrumento adicional

para aquellos casos en que las cláusulas contractuales no responden adecuadamente a la problemática real.

La regulación de las reglas corporativas vinculantes ha sido muy criticada por la gran complejidad de su elaboración y tramitación, el tiempo que se precisa y el enorme desembolso económico que exige el proceso. Por estos motivos es todavía una figura poco usada por los grupos multinacionales (poco más de treinta empresas tienen cerrado el procedimiento de reglas corporativas vinculantes, a fecha de hoy, en toda la UE).

La propuesta de Reglamento de protección de datos considera que son el instrumento más adecuado para regular las transferencias internacionales de datos en los grupos multinacionales. Para conseguirlo quiere simplificar y clarificar el procedimiento de aprobación. Con ello se espera que las normas corporativas vinculantes se conviertan en el estándar que empleen los grupos multinacionales en el futuro.

La propuesta de Reglamento abre una vía adicional a las cláusulas contractuales y a las reglas corporativas vinculantes: garantías apropiadas con respecto a la protección de datos personales que **no** se proporcionen en un instrumento jurídicamente vinculante. Es una figura innovadora que ha creado fuerte polémica por los riesgos de desprotección que puede conllevar.

En la Directiva 95/46/CE y en las normas españolas que la transponen, se enuncian un número limitado de situaciones (así por ejemplo, cuando el afectado haya dado su consentimiento inequívoco) en las que se puede aplicar una excepción al requisito de adecuación de las transferencias a terceros países. En estas situaciones no se hace necesaria la autorización de transferencia a países que no proporcionan un nivel de protección adecuado por parte de la AEPD. El responsable del tratamiento deberá

notificar la transferencia en el Registro de la Agencia, pero no tendrá que solicitar autorización.

Cuando se hace uso de alguna de las excepciones para poder efectuar la transferencia, no se exige que el destinatario de los datos cumpla los requisitos establecidos en la Directiva por lo que respecta a cualquier tratamiento de datos (por ejemplo, los principios de finalidad, seguridad, derecho de acceso, etc.).

En opinión del Grupo de Trabajo, entre los responsables del tratamiento ha habido una tendencia a hacer uso de estas excepciones como primera opción, incluso en los casos en los que no procedía. El uso de dichas excepciones ha de ser necesariamente restrictivo, ya que habría que garantizar la protección adecuada en tantas situaciones como sea posible. El responsable del tratamiento debería ofrecer las garantías adecuadas mediante cláusulas contractuales tipo o reglas corporativas vinculantes. Únicamente en el caso de que ello no resulte verdaderamente práctico o viable, el responsable del tratamiento de los datos debería considerar hacer uso de las excepciones.

En la propuesta de Reglamento de protección de datos la relación de excepciones ha sido aumentada con un nuevo supuesto: cuando la transferencia sea necesaria para la satisfacción de los intereses legítimos del responsable o del encargado del tratamiento. Según cuál sea la interpretación que se dé a esta nueva excepción, podría llegar a convertirse en una amenaza para la protección de datos en Europa.

III. El RLOPD regula los procedimientos tramitados por la AEPD. Aquellos que están relacionados con las transferencias internacionales de datos son: el procedimiento de autorización de transferencias internacionales de datos y el de suspensión temporal de las mismas.

Para que la transferencia internacional de datos pueda considerarse conforme, el RLOPD exige la autorización del Director de la AEPD. Ésta se otorgará en caso de que el exportador aporte las garantías adecuadas. Es decir, cuando el responsable del tratamiento aporte un contrato escrito, celebrado entre el exportador y el importador, en el que consten las necesarias garantías de respeto a la protección de la vida privada de los afectados y a sus derechos y libertades fundamentales y se garantice el ejercicio de sus respectivos derechos. A tal efecto, se considera que establecen las adecuadas garantías los contratos que se celebren de acuerdo con lo previsto en las Decisiones de la Comisión Europea que den cumplimiento a lo establecido en la Directiva 95/46/CE. También podrá otorgarse la autorización para la transferencia internacional de datos en el seno de grupos multinacionales de empresas cuando hubiesen sido adoptados por los mismos normas o reglas internas en que consten las necesarias garantías de respeto a la protección de la vida privada y el derecho fundamental a la protección de datos de los afectados y se garantice asimismo el cumplimiento de los principios y el ejercicio de los derechos reconocidos en la normativa española sobre protección de datos.

En el caso de la solicitud de autorización en base a cláusulas contractuales, el procedimiento tiene fijado un plazo máximo para dictar y notificar resolución de tres meses, a contar desde la fecha de entrada en la AEPD de la solicitud. Si en dicho plazo no se hubiese dictado y notificado resolución expresa, se entenderá autorizada la transferencia internacional de datos.

La autorización podrá ser denegada por el Director de la AEPD en base a alguna de las causas tasadas que vienen recogidas en el RLOPD.

La autorización o denegación de la transferencia internacional de datos deberá notificarse al solicitante de la autorización. Cuando se resuelva autorizar la transferencia, ésta se inscribirá en el Registro General de Protección de Datos. También se dará traslado de la resolución de autorización o denegación de la autorización al Ministerio de Justicia, al efecto de que se proceda a su notificación a la Comisión Europea y a los demás Estados miembros.

A este tipo de procedimiento le pueden quedar los días contados. De acuerdo a la interpretación literal de la propuesta de Reglamento de protección de datos de la UE, una transferencia efectuada en virtud de cláusulas tipo de protección de datos (ya hayan sido adoptadas por la Comisión o bien por una autoridad de control), no requerirá nuevas autorizaciones. Sólo en el caso de cláusulas contractuales entre el responsable o el encargado del tratamiento y el destinatario de los datos, que no se correspondan a los modelos anteriores, deberían ser autorizadas por una autoridad de control.

En el RLOPD se regula la suspensión temporal de la transferencia de datos hacia un importador ubicado en un tercer Estado (ya se haya declarado la existencia de un nivel adecuado de protección, o a Estados que no proporcionen dicho nivel), cuando concurra alguna de las circunstancias que el propio reglamento regula. El acuerdo de suspensión lo podrá adoptar el Director de la AEPD, previa audiencia del exportador. Esta decisión será notificada a la Unión Europea.

El acuerdo de suspensión deberá ser motivado y fundarse en las causas previstas en el propio RLOPD.

En el procedimiento sobre instrucción y resolución de la suspensión temporal, se exige dar traslado del acuerdo al exportador, a fin de que en el plazo de quince días

formule lo que a su derecho convenga. Una vez recibidas las alegaciones o cumplido el plazo señalado, el Director dictará resolución acordando, en su caso, la suspensión temporal de la transferencia.

La suspensión se inscribirá en el Registro General de Protección de Datos, dándose traslado de la resolución al Ministerio de Justicia, al efecto de que se proceda a su notificación a la Comisión Europea y a los demás Estados miembros.

El RLOPD también contempla el levantamiento de la suspensión temporal de transferencias internacionales de datos. La suspensión se levantará tan pronto como cesen las causas que la hubieran justificado, mediante resolución del Director de la AEPD, del que se dará traslado al exportador. Y de la misma forma que antes se había actuado para la suspensión se deberá proceder ante el levantamiento de la suspensión: se dará traslado de la resolución al Registro General de Protección de Datos, a fin de que la misma se haga constar en el Registro.

La notificación de este acuerdo deberá efectuarse tanto al exportador de datos personales como al Ministerio de Justicia, al efecto de que se proceda a su notificación a la Comisión Europea y a los demás Estados miembros.

En el proyecto de Reglamento de protección de datos de la UE se continúa manteniendo la potestad de las autoridades de control para suspender los flujos de datos hacia un destinatario situado en un tercer país o hacia una organización internacional.

En cuanto al procedimiento para la autorización de normas corporativas vinculantes, la normativa española nos ofrece escasa regulación. En el RLOPD se regula que para que proceda la autorización del Director de la AEPD será preciso que las normas o reglas resulten vinculantes para las empresas del Grupo y exigibles conforme

al ordenamiento jurídico español. Esta autorización implicará la exigibilidad de lo previsto en las normas o reglas internas tanto por la Agencia como por los afectados cuyos datos hubieran sido objeto de tratamiento. En este sentido se pretende dejar, en el ámbito de las reglas corporativas vinculantes, sin efecto el contenido del artículo 1089 del Código Civil. En éste se estipula que "las obligaciones nacen de la ley, de los contratos y cuasi contratos, y de los actos y omisiones ilícitos o en que intervenga cualquier género de culpa o negligencia". Por lo tanto, la declaración unilateral de voluntad, por regla general, no es fuente de obligaciones.

El RLOPD no da mayor concreción al procedimiento para la autorización de las reglas corporativas vinculantes ni informa de los detalles que se exigirán por parte de la AEPD. Sus requisitos y contenido lo deberemos extraer de los Documentos elaborados por el Grupo de Trabajo del art. 29.

El procedimiento de autorización de las reglas corporativas vinculantes ha sido muy criticado por la lentitud y complejidad para llegar a acuerdos con todas las autoridades nacionales participantes en dicho proceso. Se han aplicado cambios para mejorar el procedimiento de coordinación de las diferentes autoridades a través del reconocimiento mutuo, pero a fecha de hoy sigue siendo un proceso difícil. Solamente las grandes corporaciones pueden acceder a esta vía.

La propuesta de Reglamento de protección de datos de la UE quiere acabar con las dificultades actuales para la obtención de autorizaciones de reglas corporativas vinculantes mediante un impulso decidido.

IV. Antes de la entrada en vigor del Tratado de Lisboa, la legislación relativa a la protección de datos en el espacio de libertad, seguridad y justicia estaba repartida entre

el primer pilar (protección de datos con fines privados y comerciales, con la aplicación del método comunitario), el segundo pilar (política exterior y de seguridad común, que estaba regulada en el Título V del TUE) y el tercer pilar (cooperación policial y judicial en materia penal, cubierta por el Título VI del TUE). El proceso decisorio se regía por normas diferentes. Con el Tratado de Lisboa la estructura de pilares ha desaparecido, quedando integrada la cooperación policial y judicial en materia penal dentro del método comunitario.

Por ser anterior al Tratado de Lisboa, en la Directiva 95/46/CE se establece que sus disposiciones no se aplicarán al tratamiento de datos personales efectuado en el ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario. Entre éstas se encontraba la cooperación policial y judicial en materia penal.

El tratamiento de datos por las autoridades policiales y judiciales en materia penal lo regula esencialmente la Decisión Marco 2008/977/JAI del Consejo, que también es anterior al Tratado de Lisboa.

La Decisión Marco 2008/977/JAI ha tenido una desigual aplicación en los países de la UE. Por otra parte su ámbito de aplicación se limita a los datos personales que son o han sido transmitidos o puestos a disposición entre Estados miembros o intercambiados entre Estados miembros e instituciones u organismos de la UE. Ello significa que el tratamiento de datos personales que no haya sido objeto de intercambio queda fuera del ámbito de aplicación de las disposiciones de la UE que regulan ese tratamiento y salvaguardan el derecho fundamental a la protección de datos.

Además, la Decisión Marco no afecta, entre otros, al conjunto completo y coherente de disposiciones de protección de datos que rigen el funcionamiento de Europol, Eurojust, el Sistema de Información de Schengen (SIS) y el Sistema de Información Aduanero (SIA), ni a los que permiten a las autoridades de los Estados miembros acceder directamente a determinados sistemas de datos de otros Estados miembros.

Si nos centramos en el tema de las transferencias internacionales de datos, la Decisión Marco exige entre otras condiciones, para poder efectuarlas, que el Estado miembro del que se hayan obtenido los datos haya dado su consentimiento a la transferencia.

La transferencia de datos sin el consentimiento previsto en el apartado anterior solo podrá permitirse si es esencial para la prevención de una amenaza inmediata y grave a la seguridad pública de un Estado miembro o de un tercer Estado o a intereses esenciales de un Estado miembro, y si el consentimiento previo no puede obtenerse a tiempo. En este caso habrá que informar sin demora a la autoridad encargada de otorgar el consentimiento.

Que el tercer Estado (u organismo internacional de que se trate) garantice un nivel adecuado de protección en el tratamiento de datos previsto no es condición imprescindible para poder efectuar la transferencia internacional.

La Decisión Marco tampoco prevé criterio o mecanismo común alguno para evaluar la adecuación. Esto significa que cada Estado miembro evaluará conforme a su

propia discreción el nivel de adecuación previsto por el tercer país o el organismo internacional.

Por las grandes limitaciones de la Decisión Marco, y fruto de los cambios normativos del Tratado de Lisboa surge la propuesta de Directiva de protección de datos en el marco de la cooperación policial y judicial en materia penal.

Esta Directiva, que sustituiría a la Decisión Marco 2008/977/JAI, fija las normas sobre la protección de los datos personales tratados con fines de prevención, detección, investigación o persecución de delitos y para las actividades judiciales correspondientes.

La propuesta de Directiva aplica los principios generales de la protección de datos a la cooperación policial y judicial en materia penal, siempre en total respeto de la naturaleza específica de cada uno de estos ámbitos. Establece condiciones y criterios mínimos armonizados para toda posible limitación de las reglas generales.

En cuestión de las transferencias internacionales, los Estados miembros deben velar por que una transferencia a un tercer país solo se lleve a cabo si es necesaria para la prevención, investigación, detección y enjuiciamiento de infracciones penales o la ejecución de sanciones penales, y si el responsable del tratamiento en el tercer país u organización internacional es una autoridad competente a tenor de la Directiva. Puede llevarse a cabo una transferencia en los casos en que la Comisión haya decidido que el tercer país o la organización internacional de que se trate garantizan un nivel adecuado de protección, o cuando se hayan ofrecido unas garantías apropiadas.

La Comisión puede determinar que algunos terceros países, un territorio o un sector del tratamiento en un tercer país, o una organización internacional ofrecen un nivel

adecuado de protección de datos, proporcionando así seguridad jurídica y uniformidad en toda la Unión en lo que se refiere a los terceros países u organizaciones internacionales que se considera aportan tal nivel de protección. En estos casos, se pueden realizar transferencias de datos personales a estos países sin tener que obtener ninguna otra autorización.

En los casos en que no existan razones para autorizar una transferencia, deben permitirse excepciones, si fuera necesario, para proteger el interés vital del interesado o de otra persona, o para proteger intereses legítimos del interesado en caso de que la legislación del Estado miembro que transfiere los datos personales así lo disponga, o cuando sea indispensable para prevenir una amenaza inminente y grave para la seguridad pública de un Estado miembro o de un tercer país, o en determinados casos a efectos de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, o en casos específicos para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial.

Si hemos de valorar la norma actual y la que previsiblemente se convertirá en la nueva regulación, podemos afirmar que la entrada en vigor de la Decisión Marco 2008/977/JAI significó un paso adelante en la protección de datos dentro de su campo de acción. Sin embargo se trató de una regulación poco ambiciosa. Podemos criticar su limitado ámbito de aplicación, el amplio margen de maniobra a los Estados miembros para transponer las disposiciones de la Decisión Marco a su Derecho interno, la falta de mecanismos de interpretación común, el instrumento elegido para efectuar dicha regulación (una Decisión Marco), una excepción demasiado amplia al principio de limitación de la finalidad y la ausencia de disposiciones que prevean una diferenciación

de las distintas categorías de datos en función de su grado de exactitud o fiabilidad, y en particular una diferenciación de los datos basados en hechos de los basados en opiniones o valoraciones personales, así como una diferenciación de las distintas categorías de interesados (delincuentes, sospechosos, victimas, testigos, etc.).

Las limitaciones mencionadas, junto con otras a las que no hemos hecho referencia, exigen una revisión a fondo de la normativa actual.

A la hora de elegir el instrumento legal, la Comisión ha propuesto que el nuevo marco en materia de protección de datos conste de:

- Un Reglamento (que sustituye a la Directiva 95/46/CE) en el que se fija el marco jurídico general de protección de datos de la UE.
- Una Directiva (que sustituye a la Decisión Marco 2008/977/JAI), que fija las normas sobre la protección de los datos personales tratados con fines de prevención, detección, investigación o persecución de delitos y para las actividades judiciales correspondientes.

La adopción de dos regímenes distintos, uno para asuntos civiles, y otro de asuntos penales y orden público ha sido criticada en amplios sectores que opinan que el procesamiento de datos en el ámbito de la cooperación judicial y policial en asuntos penales requiere al menos tanta protección como la prevista en el Reglamento, en lugar de una protección inferior como la que se ha establecido en la Directiva.

En este punto podemos expresar nuestra visión crítica con respecto a la elección de la Directiva como instrumento normativo. La propia Comisión Europea expresó en multitud de ocasiones su malestar con la transposición de la Directiva 95/46/CE en

buena parte de los Estados miembros. Esa incorrecta transposición llevó a una fragmentación de las legislaciones nacionales imposibilitando el establecimiento de un marco armonizado y coherente en materia de protección de datos. Pero ese mal precedente no ha impedido que se elija de nuevo una Directiva para la regulación del tratamiento de datos personales por las autoridades competentes a efectos de la prevención, investigación, detección y enjuiciamiento de infracciones penales o a la ejecución de sanciones penales, y a la libre circulación de estos datos.

Otro punto que puede causar conflicto se encuentra en la dificultad de distinguir el ámbito de aplicación del nuevo Reglamento (como instrumento general de protección de datos personales) y el de la Directiva. Hay una serie de actividades en las que las autoridades de los diferentes Estados miembros tienen objetivos de ejecución legal o simplemente administrativos (así por ejemplo en materia de aduanas, inmigración o medio ambiente). Ello supondría que la Directiva y el Reglamento pueden aplicarse a la misma institución en Estados distintos, lo que no casa con la pretendida armonización y coherencia.

La Directiva tampoco establece un derecho para oponerse al tratamiento de datos personales. Ello es especialmente importante para el caso de que determinadas personas puedan limitar el tratamiento ulterior de sus datos en el momento en que finalice el proceso legal.

Ya en el campo de las transferencias de datos, el responsable del tratamiento no tiene obligación de informar al interesado para transferir datos personales a terceros países.

También podemos destacar las excepciones para transferir datos personales sin decisión de adecuación ni salvaguardias apropiadas. A menos que el contenido de este artículo se interprete de forma restrictiva, es posible que se convierta en el instrumento habitual a la hora de efectuarse transferencias internacionales. La excepción puede convertirse en la regla habitual.

Pese a todas las limitaciones que encontramos en la propuesta de Directiva, no seríamos justos si no se reconoce el gran paso adelante que su entrada en vigor supondrá para la protección de datos personales. Partiendo de un punto tan bajo como es la Decisión Marco 2008/977/JAI, incluso con grandes carencias, significa un avance importante.

V. En este último punto se quiere incidir de forma muy breve en dos consideraciones fundamentales:

- El avance que se está produciendo en materia de protección de datos en la Unión Europea es imparable.
- El avance sigue siendo insuficiente. A pesar de todos los esfuerzos normativos, la legislación va a remolque de la innovación tecnológica.

Como ya hemos manifestado anteriormente, cuando en 1995 se adoptó la Directiva 95/46/CE se dio un gran paso para defender el derecho fundamental a la protección de datos y garantizar la libre circulación de estos datos entre los Estados miembros.

Otro paso importantísimo se dio cuando la Directiva se complementó años más tarde con la Decisión Marco 2008/977/JAI, destinada a la protección de datos personales en el marco de la cooperación policial y judicial en materia penal.

Las dos normas han sido criticadas por sus limitaciones, pero no hay que olvidar que han sido un punto de partida excepcional. Siguen existiendo divergencias (a veces de gran calado) entre las diferentes normas nacionales, pero nadie puede discutir el gran paso adelante que han representado.

Después de los años transcurridos, la Comisión Europea ha considerado imprescindible proceder a actualizar la normativa actual. Es necesario reforzar los derechos de los ciudadanos, adaptar la normativa vigente a la evolución tecnológica contemplando instrumentos inexistentes en el momento en que se aprobó la Directiva 95/46/CE (redes sociales, *cloud computing*), reforzar el mercado interior, reducir la burocracia innecesaria, facilitar el flujo de información entre los países miembros y terceros países.

La propuesta de Reglamento es evidente que garantizará una aplicación más armónica de la ley, facilitando la libre circulación de los datos. Junto a ello, traerá beneficios a casi todas las partes interesadas: a los particulares, a los responsables del tratamiento, a los encargados del tratamiento y a las autoridades de protección de datos.

En cuanto a la propuesta de Directiva, también supone un avance muy considerable sobre la regulación actual. Esto queda muy claro en el campo que pasa a cubrir: ya no habrá distinciones entre el tratamiento de datos personales en casos nacionales y transfronterizos.

En segundo lugar hacíamos referencia a la insuficiencia del avance normativo. Para ver un ejemplo de la misma podemos centrarnos en las transferencias internacionales de datos. No podemos negar que hay mejoras importantes en la propuesta de Reglamento,

especialmente en la regulación de las reglas corporativas vinculantes. Estas mejoras no sólo se contienen en el texto normativo sino también en su espíritu: se reconoce que la regulación de las transferencias internacionales ha dificultado el funcionamiento de las empresas en sus relaciones con países terceros. Para remediar el problema se simplifican las transferencias de datos fuera de la UE a la vez que se garantiza la protección de los datos personales.

Aun así, la figura de la transferencia internacional de datos tiene verdaderos problemas con las nuevas aplicaciones tecnológicas que aparecen cada vez de forma más acelerada. Prueba de ello lo encontramos en el *cloud computing*, tecnología con un crecimiento exponencial y con un grado de incumplimiento masivo con la actual normativa reguladora de las transferencias internacionales. La Directiva 95/46/CE no presenta respuestas adecuadas en su regulación, pero lo más grave de esta problemática es que la propuesta de Reglamento que todavía no ha entrado en vigor tampoco ofrece soluciones válidas. La Ley va un paso atrás (o más de uno) de las innovaciones tecnológicas.

BIBLIOGRAFÍA

ADSUAR, Y: "Cloud computing vs. protección de datos de carácter personal". Revista Actualidad Jurídica Aranzadi nº 846 de 2012.

ACED FÉLEZ, E: "Transferencias internacionales de datos personales entre Europa y USA". Ponencia del II Congreso Mundial de Derecho Informático de 23 a 27 de septiembre de 2002 en Madrid.

ÁLVAREZ RIGAUDIAS, C: "Las transferencias internacionales de datos personales y el nivel equiparable o adecuado de protección". Revista Actualidad Jurídica Uría Menéndez nº 12 de 2005.

ANCOS FRANCO, H: "La regulación de las transferencias internacionales de datos de carácter personal como barrera al comercio internacional: de la Directiva 95/46 a los acuerdos UE-terceros estados". Revista de Derecho Comunitario Europeo nº 6 de 1999.

- "La progresiva configuración de las transferencias de datos como objeto del tráfico comercial internacional". Revista Información Comercial Española nº 788 de 2000.

APARICIO SALOM, J: *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal*. Aranzadi. Navarra 2009.

ARENAS NAON, P. M: "Los procedimientos administrativos en materia de transferencias internacionales de datos de carácter personal". Revista de Derecho UNED nº 5 de 2009.

ARENAS RAMIRO, M: *El derecho fundamental a la protección de datos personales en Europa*. Tirant lo Blanch y AEPD. Valencia 2006.

- "La protección de datos personales en los países de la Unión Europea". Revista Jurídica de Castilla y León nº 16 de 2008.
- "¿Ficheros públicos o privados?: La Sentencia de la Audiencia Nacional `Fundación Hospital Alcorcón´". Revista digital datospersonales.org, nº 36 de noviembre de 2008.
- "Los cambios previstos en la Directiva 95/46/CE de protección de datos personales". Revista digital datospersonales.org, nº 50 de abril de 2011.

BLAS, F: "Transferencias internacionales de datos, perspectiva española de la necesaria búsqueda de estándares globales". Revista Derecho del Estado nº 23 de 2009.

BRU CUADRADA, E: "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 los Estudios de Derecho y Ciencia Política de la UOC nº 5 de 2007.

CARNIKIAN, F: "Transferencias internacionales a países con niveles adecuados y no adecuados de protección. Aspectos prácticos". Ponencia del Seminario Regional de Protección de Datos de 1-4 de junio de 2010 en Montevideo.

CARRASCOSA GONZÁLEZ, J: "Circulación internacional de datos personales informatizados y la Directiva 95/46/CE". Revista Actualidad Civil nº 2 de 1997.

CERDA SILVA, A: "El *nivel adecuado de protección* para las transferencias internacionales de datos personales desde la Unión Europea". Revista de Derecho de la Pontificia Universidad Católica de Valparaíso (Chile). XXXVI de primer semestre de 2011.

COTINO HUESO, L: *(Coord) Libertades, democracia y gobierno electrónicos*. Comares. Granada 2006.

- "La posible recepción de la protección de datos personales en los estatutos de autonomía". Revista digital datospersonales.org, nº 18 de noviembre de 2005.

DAVARA RODRÍGUEZ, M. **A:** *El abogado y la protección de datos*. Ilustre Colegio de Abogados de Madrid. Madrid 2004.

DE FRUTOS GÓMEZ, J. M: "El régimen de la Unión Europea sobre la protección de datos personales". Presentación para VIII Encuentro Iberoamericano de Protección de Datos de 29 y 30 de septiembre de 2010. Ciudad de México.

DE MIGUEL ASENSIO, P. A: "La protección de datos personales a la luz de la reciente jurisprudencia del TJCE". Revista de la Facultad de Derecho de la Universidad de Granada, 3ª época, nº 7 de 2004.

FENÁNDEZ ALLER, C: "Algunos retos de la protección de datos en la sociedad del conocimiento. Especial detenimiento en la computación en nube (*cloud computing*)". Revista de Derecho Uned, nº 10 de 2012.

GÓMEZ SÁNCHEZ, Y: *Derecho Constitucional Europeo: Derechos y Libertades*. Sanz y Torres. Madrid 2008.

- *Derechos y Libertades*. Sanz y Torres. Madrid 2003.
- "La protección de los datos genéticos: el derecho a la autodeterminación informativa". Revista DS: Derecho y Salud, vol. 16 de 2008.
- "Las bases de datos genéticos para aplicaciones policiales". Cuadernos de la Guardia Civil: Revista de seguridad pública nº 35 de 2007.
- "Los datos genéticos en el Tratado de Prüm". Revista de Derecho Constitucional Europeo nº 7 de 2007.

GUERRERO PICÓ, Mª. C: "El derecho fundamental a la protección de los datos de carácter personal en la Constitución Europea". Revista de Derecho Constitucional Europeo nº 4 de 2005.

LEENES, R: "¿Quién controla la nube?". Revista de los Estudios de Derecho y Ciencia Política de la UOC nº 11 de 2010.

MARTÍNEZ MARTÍNEZ, R: "El derecho fundamental a la protección de datos: perspectivas". Revista de los Estudios de Derecho y Ciencia Política de la UOC nº 5 de 2007.

MARZO PORTERA, A. Mª: "Privacidad y Cloud Computing, hacia dónde camina Europa". Revista de la Facultad de Ciencias Sociales y Jurídicas de Elche. Volumen I, nº 8 de 2012.

MIRALLES LÓPEZ, R: "Cloud computing y protección de datos". Revista de los Estudios de Derecho y Ciencia Política de la UOC nº 11 de 2010.

ORTEGA GIMÉNEZ, A: "Internet, publicación de datos personales y transferencias internacionales de datos: la sentencia del TJCE *Lindqvist*, de 6 de noviembre de

2003 (asunto C-101/01-Bodil Lindqvist)". Revista Actualidad Jurídica Aranzadi nº 790 de 2010.

- "Qué entendemos por transferencia internacional de datos según la última jurisprudencia del Tribunal de Justicia de las Comunidades Europeas". Revista SCRIPT-ed de la Universidad de Edimburgo, volumen 1, nº 3, de 2004.
- "La transferencia internacional de datos en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal y el derecho internacional privado". La Ley: Revista jurídica española de doctrina, jurisprudencia y bibliografía, nº 2 de 2005.

REBOLLO DELGADO, L: *Vida privada y protección de datos en la Unión Europea*. Dykinson. Madrid 2008.

- *El Derecho fundamental a la intimidad*. Dykinson. 2ª Ed. Madrid 2005.
- *Derechos fundamentales y protección de datos*. Dykinson. Madrid 2004.
- "Derechos de la personalidad y datos personales". Revista de Derecho Político de la UNED nº 44 de 1998.
- "Veinticinco años de relación entre la informática y los derechos al honor y a la intimidad personal y familiar". Revista de Derecho Político de la UNED números 58 y 59 de 2003 – 2004.
- "El Secreto de las comunicaciones: problemas actuales". Revista de Derecho Político de la UNED números 48 y 49 de 2000.
- "Constitución y Técnicas de Reproducción Asistida". Boletín de la Facultad de Derecho de la UNED nº 16 de 2000.
- "Criptología y delito cibernético". Informática y Derechos números 27 a 29 de 1998.

REBOLLO DELGADO, L y GÓMEZ SÁNCHEZ, Y: *Biomedicina y protección de datos*. Dykinson. Madrid 2008.

REBOLLO DELGADO, L y SERRANO PÉREZ, Mª. M: *Introducción a la protección de datos*. Dykinson. Madrid 2008.

REMOLINA ANGARITA, N: *Cláusulas contractuales y transferencia internacional de datos personales*, en la obra de VV. AA: *Obligaciones y Contratos en el Derecho Contemporáneo*. Universidad de La Sabana. Bogotá 2010.

- "¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo?". International Law, Revista Colombiana de Derecho Internacional nº 16 de 2010.

RUIZ MIGUEL, C: "El derecho a la protección de los datos personales en la Carta de Derechos Fundamentales de la Unión Europea: análisis crítico". Revista de Derecho Comunitario Europeo. Año 7 nº 14 de 2003.

SANCHO VILLA, D: *Transferencia internacional de datos personales*. Agencia de Protección de Datos. Madrid 2003.

- *Negocios Internacionales de Tratamiento de Datos Personales*. Civitas. Navarra 2010.
- "Tratamiento de datos para la satisfacción del interés legítimo del responsable: a propósito de la Sentencia de 24 noviembre de 2011 del Tribunal de Justicia". Revista datospersonales.org nº54 de 2012.
- "Protección de datos personales y transferencia internacional: cuestiones de ley aplicable". Revista Jurídica de Castilla y León nº 16 de 2008.

SERRANO PÉREZ, Mª. M: *El derecho fundamental a la protección de datos. Derechos español y comparado*. Thomson-Civitas. Madrid 2003.

- "El derecho fundamental a la protección de datos. Su contenido esencial", Nuevas Políticas Públicas. Anuario multidisciplinar para la modernización de las administraciones, (on-line), Instituto Andaluz de Administración Pública, 2005.
- "Una aproximación a la regulación de los datos médicos a la luz de la nueva Ley de Protección de Datos 15/1999, de 13 de diciembre y de la Ley Sanitaria 41/2002, de 14 de noviembre", Noticias de la Unión Europea, núm. 235-236, agosto-septiembre 2004.
- "La protección de datos relativos a la salud en la legislación española y en la normativa comunitaria", Noticias de la Unión Europea, vol. 1, núm. 187/188, agosto-septiembre 2000.

TÉLLEZ AGUILERA, A: *La protección de datos en la Unión Europea. Divergencias normativas y anhelos unificadores*. Edisofer. Madrid 2002.

TRONCOSO REIGADA, A: *La Protección de Datos Personales. En Busca del Equilibrio*. Tirant lo Blanch. Valencia 2010.

- "El derecho al olvido en Internet a la luz de la propuesta de Reglamento General de Protección de Datos Personales". Revista digital datospersonales.org, nº 59 de octubre de 2012.
- "La declaración de los ficheros de datos personales: acerca de un modelo centralizado o descentralizado". Revista digital datospersonales.org, nº 38 de marzo de 2009.
- "La Administración electrónica y la protección de datos personales". Revista Jurídica de Castilla y León nº 16 de 2008.
- "Historia clínica y privacidad". Revista I+S: informática y salud nº 66 de 2007.
- "La protección de datos personales: una reflexión crítica de la jurisprudencia constitucional". Cuadernos de Derecho Público números 19 y 20 de 2003.

VERDAGUER LÓPEZ, J y BERGAS JANÉ, Mª. A: *Todo Protección de Datos 2012*. Wolters Kluwer España. Madrid 2011.

- *1000 Soluciones de Protección de Datos*. Wolters Kluwer España. Vizcaya 2010.

VV. AA: *Comentario al Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (aprobado por RD 1720/2007, de 21 de diciembre).* Aranzadi. Navarra 2008.

VV. AA: *Derecho y Cloud Computing*. Civitas. Navarra 2012.

VV. AA: *Estudio práctico sobre la protección de datos de carácter personal*. Lex Nova. Valladolid 2005.

VV. AA: "Informe sobre el PNR. La utilización de datos personales contenidos en el registro de nombres de pasajeros: ¿fines represivos o preventivos?". Institut de Ciències Polítiques i Socials (adscrito a la Universidad Autónoma de Barcelona), Working Paper 297, Barcelona 2011.

VV. AA: *Memento Experto Protección de Datos*. Francis Lefebvre. Madrid 2012.

VV. AA: *Principios de Derecho de la Unión Europea*. Colex. Madrid 2000.

VV. AA: *Protección de datos. Comentarios al Reglamento*. Lex Nova. Valladolid 2008.

VV. AA: *Protección de datos. Comentarios al Reglamento de Desarrollo de la LOPD*. Tirant lo blanch. Valencia 2009.

VV. AA: *Todo Protección de Datos 2010*. Wolters Kluwer España. Vizcaya 2009.

DOCUMENTACIÓN UTILIZADA

- Documentos adoptados por el Grupo de Trabajo del artículo 29 de la Directiva. Disponibles en la página web http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm

Se ha trabajado con la mayor parte de ellos. Destacaríamos los siguientes:

- Opinion 08/2012 providing further input on the data protection reform discussions - WP 199 (05.10.2012)
- Opinion 07/2012 on the level of protection of personal data in the Principality of Monaco - WP 198 (19.07.2012)
- Opinion 05/2012 on Cloud Computing - WP 196 (01.07.2012)
- Working Document 02/2012 setting up a table with the elements and principles to be found in Processor Binding Corporate Rules - WP 195 (06.06.2012)
- Opinion 01/2012 on the data protection reform proposals - WP 191 (23.03.2012)
- Opinion 15/2011 Consent - WP 187 (13.07.2011)
- Opinion 11/2011 on the level of protection of personal data in New Zealand - WP 182 (04.04.2011)
- Opinion 7/2010 on European Commission's Communication on the global approach to transfers of Passenger Name Record (PNR) data to third countries - WP 178 (12.11.2010)
- Opinion 6/2010 on the level of protection of personal data in the Eastern Republic of Uruguay - WP 177 (12.10.2010)
- FAQs in order to address some issues raised by the entry into force of the EU Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC- WP 176 (12.07.2010)
- Opinion 1/2010 on the concepts of "controller" and "processor"- WP 169 (16.02.2010)
- Opinion 7/2009 on the level of protection of personal data in the Principality of Andorra - WP 166 (01.12.2009)
- Opinion 6/2009 on the level of protection of personal data in Israel - WP 165 (01.12.2009)

- Second opinion 4/2009 on the World Anti-Doping Agency (WADA) International Standard for the Protection of Privacy and Personal Information, on related provisions of the WADA Code and on other privacy issues in the context of the fight against doping in sport by WADA and (national) anti-doping organizations - WP 162 (06.04.2009)
- Opinion 3/2009 on the Draft Commission Decision on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC (data controller to data processor) - WP 161 (05.03.2009)
- Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules - WP 155 rev 04 (24.06.2008)
- Working Document setting up a framework for the structure of Binding Corporate Rules - WP 154 (24.06.2008)
- Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules - WP 153 (24.06.2008)
- Opinion 2/2007 on information to passengers about the transfer of PNR data to US authorities, Adopted on 15 February 2007 and revised and updated on 24 June 2008 - WP 151 (24.06.2008)
- Joint opinion on the proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, presented by the Commission on 6 November 2007 - WP 145 (05.12.2007)
- Opinion 10/2007 on the 8th Directive on Statutory Audits by the Article 29 Working Party - WP 143 (23.11.2007)
- Opinion 9/2007 on the level of protection of personal data in the Faroe Islands - WP 142 (09.10.2007)
- Opinion 8/2007 on the level of protection of personal data in Jersey - WP 141 (09.10.2007)
- Opinion Nº 5/2007 on the follow-up agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security concluded in July 2007 - WP 138 (17.08.2007)

- Recommendation 1/2007 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data - WP 133 (10.01.2007)
- Opinion 2/2007 on information to passengers about transfer of PNR data to US authorities - WP 132 (15.02.2007)
- Working Document on the processing of personal data relating to health in electronic health records (EHR) - WP 131 (15.02.2007)
- Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT) - WP 128 (22.11.2006)
- Opinion 1/2006 on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime - WP 117 (01.02.2006)
- Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995 - WP 114 (25.11.2005)
- Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules - WP 108 (14.04.2005)
- Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From "Binding Corporate Rules" - WP 107 (14.04.2005)
- Opinion 1/2005 on the level of protection ensured in Canada for the transmission of Passenger Name Record and Advance Passenger Information from airlines - WP 103 (19.01.2005)
- Model Checklist, Application for approval of Binding Corporate Rules - WP 102 (25.11.2004)
- Opinion 8/2004 on the information for passengers concerning the transfer of PNR data on flights between the European Union and the United States of America - WP 97 (30.09.2004)
- Opinion 5/2004 on unsolicited communications for marketing purposes under Article 13 of Directive 2002/58/EC - WP 90 (27.02.2004)

- Opinion 3/2004 on the level of protection ensured in Canada for the transmission of Passenger Name Records and Advanced Passenger Information from airlines - WP 88 (11.02.2004)
- Opinion 1/2004 on the level of protection ensured in Australia for the transmission of Passenger Name Record data from airlines - WP 85 (16.01.2004)
- Opinion 8/2003 on the draft standard contractual clauses submitted by a group of business associations - WP 84 (17.12.2003)
- Opinion 6/2003 on the level of protection of personal data in the Isle of Man - WP 82 (21.11.2003)
- Opinion 5/2003 on the level of protection of personal data in Guernsey - WP 79 (13.06.2003)
- Working Document on Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers - WP 74 (03.06.2003)
- Opinion 6/2002 on transmission of Passenger Manifest Information and other data from Airlines to the United States - WP 66 (24.10.2002)
- Opinion 4/2002 on adequate level of protection of personal data in Argentina - WP 63 (3.10.2002)
- Opinion 8/2001 on the processing of personal data in the employment context - WP 48
- Opinion 7/2001 on the Draft Commission Decision (version 31 August 2001) on Standard Contractual Clauses for the transfer of Personal Data to data processors established in third countries under Article 26(4) of Directive 95/46 - WP 47 (13.09.2001)
- Opinion 2/2001 on the adequacy of the Canadian Personal Information and Electronic Documents Act - WP 39 (26.01.2001)
- Opinion 1/2001 on the Draft Commission Decision on Standard Contractual Clauses for the transfer of Personal Data to third countries under Article 26(4) of Directive 95/46 - WP 38 (26.01.2001)
- Working document "Privacy on the Internet" - An integrated EU Approach to On-line Data Protection - WP 37 (21.11.2000)

- Opinion 4/2000 on the level of protection provided by the "Safe Harbor Principles" - WP 32 (16.05.2000)
- Opinion 3/2000 on the EU/US dialogue concerning the "Safe harbor" arrangement - WP 31 (16.03.2000)
- Opinion 7/99 on the Level of Data Protection provided by the "Safe Harbor" Principles as published together with the Frequently Asked Questions (FAQs) and other related documents on 15 and 16 November 1999 by the US Department of Commerce - WP 27 (December 1999)
- Opinion 6/99 concerning the level of personal data protection in Hungary - WP 24 (7.09.1999)
- Opinion 5/99 on the level of protection of personal data in Switzerland - WP 22 (07.09.1999)
- Opinion 4/99 on the Frequently Asked Questions to be issued by the US Department of Commerce in relation to the proposed "Safe Harbor Principles" on the Adequacy of the "International Safe Harbor Principles" - WP 21 (7.09.1999)
- Opinion 2/99 on the Adequacy of the "International Safe Harbor Principles" issued by the US Department of Commerce on 19th April 1999 - WP 19 (3.051999)
- Opinion 1/99 concerning the level of data protection in the United States and the ongoing discussions between the European Commission and the United States Government - WP 15 (26.01.1999)
- Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive - WP 12 (July 1998)
- Working Document: Preliminary views on the use of contractual provisions in the context of transfers of personal data to third countries - WP 9 (22.04.1998)
- Working Document: Judging industry self regulation: when does it make a meaningful contribution to the level of data protection in a third country? - WP 7 (14.01.1998)

- Discussion Document: First Orientations on Transfers of Personal Data to Third Countries - Possible Ways Forward in Assessing Adequacy - WP 4 (26.06.1997)

- Documentos de la Agencia Española de Protección de Datos (descargables desde su página electrónica www.agpd.es):

- Memorias anuales de la AEPD (2002-2011).
- Informe jurídico sobre las Transferencias Internacionales de datos para la realización de un tratamiento por cuenta del responsable del fichero – Año 2001.
- Informe jurídico sobre la vigencia de la Orden del Ministerio de Justicia e Interior de 2 de febrero de 1995 – Año 2002.
- Informe jurídico 101/2003. Cumplimiento de la LOPD como requisito previo a la transferencia.
- Informe Jurídico 582/2004. Subcontratación de un encargado del tratamiento en tercer país que no ofrece nivel adecuado de protección. Necesidad de intervención del responsable.
- Informe jurídico 493/2005. Transferencia Internacional a consecuencia de un cambio societario.
- Informe jurídico 518/2006. Transferencia de encargado a encargado.
- Informe Jurídico 128/2007. Creación de sistemas de denuncias internas en las empresas (mecanismos de *whistleblowing*).
- Informe jurídico 190/2007. Prestación de servicios de consulta telefónica.
- Informe jurídico 391/2007. Cribado de correo electrónico.
- Informe jurídico 538/2007. Subcontratación de servicio telefónico de llamadas.
- Informe jurídico 108/2008. Transferencia Internacional de encargado a subencargado.
- Informe sobre transferencias internacionales de datos. Inspección sectorial de oficio España-Colombia en centros de atención al cliente. Julio 2007.
- Problemática actual de las transferencias internacionales de datos. Jornada sobre transferencias internacionales de Datos. Madrid, 18 de julio de 2007.

- Planes sectoriales de oficio sobre las transferencias internacionales. Actuaciones de la inspección de datos. Madrid, 18 de julio de 2007.
- El Procedimiento de Autorización de Transferencias. Jornada sobre transferencias internacionales de datos. Madrid, 18 de julio de 2007.
- Transferencias internacionales de datos para la prestación de servicios. V Encuentro Iberoamericano de Protección de Datos. Lisboa, 8-9 de noviembre de 2007.
- Resolución de autorización de transferencias internacionales de datos. En relación con el expediente TI/000040/2009, relativo a la solicitud de autorización de transferencias internacionales de datos en el seno del grupo multinacional General Electric.
- Cloud Computing y protección de datos personales. Seminario SOCINFO: compartición de recursos y Cloud Computing. Madrid, 11 de enero de 2011.
- Protección de los datos personales en Cloud Computing. Congreso DINTEL CLOUD COMPUTING. Digitalización en la Red. Madrid, 8 de febrero de 2011.
- El impacto de las transferencias internacionales de datos en América Latina. Las políticas preventivas y la autorregulación en la implantación de la normativa de protección de datos. Seminario regional de protección de datos. Cartagena de Indias, 14-16 de junio de 2011.
- Decisiones de Adecuación de la Comisión Europea. Seminario regional de protección de datos. Cartagena de Indias, 14-16 de junio de 2011.
- El régimen de transferencias internacionales de datos a encargados de tratamiento. Cuarta Sesión Abierta de la AEPD. Madrid, 27 de enero de 2012.
- Informe "Utilización del *Cloud Computing* por los despachos de abogados y el derecho a la protección de datos de carácter personal". Informe presentado por la AEPD y el Consejo General de la Abogacía Española el 18 de junio de 2012.
- Resolución de autorización de transferencias internacionales de datos a Perú. En relación con el expediente TI/00126/2012, relativo a la solicitud de autorización de transferencias internacionales de datos de la entidad GLOBAL SALES SOLUTIONS LINE S.L. (encargado de tratamiento).
- Cláusulas contractuales "encargados a subencargados del tratamiento" elaboradas por la AEPD.

- Notificaciones Telemáticas a la AEPD. Preguntas más frecuentes. Revisión de 18 de diciembre de 2012.

- Documentos de los organismos de la Unión Europea:

- Clauses contractuelles types pour le transfert des données à caractère personnel vers des pays tiers – questions fréquemment posées (FAQ). Bruxelles, le 18 juin 2001. MEMO/01/228.
  Disponible en: http://europa.eu/rapid/press-release_MEMO-01-228_fr.htm
- Primer informe sobre la aplicación de la Directiva sobre protección de datos (95/46/CE). Bruselas, 15.5.2003. COM(2003) 265 final.
  Disponible en:
  http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2003:0265:FIN:ES:PDF
- Notificaciones nacionales con arreglo al apartado 3 del artículo 26 de la Directiva e intercambio de mejores prácticas. Director General. Servicios, propiedad intelectual e industrial, medios de comunicación y protección de datos. DG Mercado Interior. Comisión Europea. Bruselas, 21 de agosto de 2003. MARKT/E4/LCN/ck D(2003) 270.
  Disponible en:
  http://ec.europa.eu/justice/policies/privacy/docs/lawreport/notification-art-26_es.pdf
- Communication de la Commision au Conseil et au Parlement. Transfert des données des dossiers passagers (Passenger Name Record – PNR): Une démarche globale de l'Union européenne. Bruxelles, le 16.12.2003. COM(2003) 826 final.
  Disponible en:
  http://eur-lex.europa.eu/LexUriServ/site/en/com/2003/com2003_0826en01.pdf
- Comunicado de prensa: La Comisión obtiene garantías para proteger los datos personales de los pasajeros de vuelos transatlánticos. Bruselas, 17 de mayo de 2004. IP/04/650.
  Disponible en: http://europa.eu/rapid/press-release_IP-04-650_es.htm
- Standart contractual clauses for the transfer of personal data to third countries – Frequently asked questions. Brussels, 7 January 2005. MEMO/05/3.

Disponible en: http://europa.eu/rapid/press-release_MEMO-05-3_en.htm

- Commission staff working paper on the joint review of the implementation by the U.S. Bureau of Customs and Border Protection of the Undertakings set out in Commission Decision 2004/535/EC of 14 May 2004. Washington, 20-21 September 2005. Brussels, 12.12.2005. COM (2005) final.
  Disponible en:
  http://ec.europa.eu/justice/policies/privacy/docs/adequacy/pnr/review_2005.pdf
- Comunicación del Consejo (2006/C 259/01): Nota del Departamento de Seguridad del Territorio Nacional (DHS) de los Estados Unidos de América a la Presidencia del Consejo y a la Comisión relativa a la interpretación de determinadas disposiciones de los compromisos publicados el 11 de mayo de 2004 por el DHS en relación con la transferencia de datos del Registro de Nombres de los Pasajeros (PNR) por las compañías aéreas. Y la correspondiente respuesta de la Presidencia del Consejo y de la Comisión a la nota del Departamento de Seguridad del Territorio Nacional de los Estados Unidos de América. (Ambos documentos se encuentran en el DOUE C 259 de 27 de octubre de 2006).
- Dictamen (tercero) del Supervisor Europeo de Protección de Datos, de 27 de abril de 2007, sobre la propuesta de Decisión Marco del Consejo relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal. (2007/C 139/01). (DOUE C 139 de 23 de junio de 2007).
- Propuesta de Decisión Marco del Consejo sobre utilización de datos del registro de nombres de los pasajeros (Passenger Name Record – PNR) con fines represivos (presentada por la Comisión). Bruselas, 6.11.2007. COM(2007) 654 final. 2007/0237 (CNS).
  Disponible en:
  http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0654:FIN:ES:PDF
- Frequently asked questions relating to transfers of personal data from the EU/EEA to third countries. Data Protection Unit of the Directorate-General for

Justice, Freedom and Security at the European Commission. Marzo de 2009. Disponible en:
http://ec.europa.eu/justice_home/fsj/privacy/docs/international_transfers_faq/international_transfers_faq.pdf

- Comunicado de prensa: La Comisaria sostiene que la privacidad de los europeos será un gran desafío en la próxima década. Bruselas, 28 de enero de 2010. IP/10/63.
  Disponible en: http://europa.eu/rapid/press-release_IP-10-63_es.htm
- Comunicado de prensa: Des normes plus strictes pour les transferts de données à caractère personnel de citoyens européens vers des sous-traitants établis dans des pays tiers. Bruxelles, le 5 février 2010. IP/10/130.
  Disponible en: http://europa.eu/rapid/press-release_IP-10-130_fr.htm
- Comunicación de la Comisión sobre el enfoque global de las transferencias de datos de los registros de nombres de los pasajeros (PNR) a los terceros países. Bruselas, 21.9.2010. COM(2010) 492 final.
  Disponible en:
  http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0492:FIN:Es:PDF
- Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Un enfoque global de la protección de los datos personales en la Unión Europea. Bruselas, 4.11.2010. COM(2010) 609 final.
  Disponible en:
  http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_es.pdf
- Comunicado de prensa: La Comisión Europea presenta su estrategia para el refuerzo de las normas de protección de datos de la UE. Bruselas, 4 de noviembre de 2010. IP/10/1462.
  Disponible en: http://europa.eu/rapid/press-release_IP-10-1462_es.htm
- Propuesta de Decisión del Consejo relativa a la celebración del Acuerdo entre la Unión Europea y Australia sobre el tratamiento y transferencia de datos del registro de nombres de los pasajeros (PNR) por los transportistas aéreos al

Servicio de Aduanas y de Protección de las Fronteras de Australia. Bruselas, 19.5.2011. COM(2011) 281 final. 2011/0126 (NLE).
Disponible en:
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0281:FIN:ES:PDF

- Dictamen del Supervisor Europeo de Protección de Datos sobre la propuesta de Decisión del Consejo relativa a la celebración del Acuerdo entre Unión Europea y Australia sobre el tratamiento y transferencia de datos del registro de nombres de pasajeros (PNR) por los transportistas aéreos al Servicio de Aduanas y de Protección de las Fronteras de Australia. Bruselas, 15 de julio de 2011. (2011/C 322/01). (DOUE C 322 de 5 de noviembre de 2011).
- Dictamen del Supervisor Europeo de Protección de Datos sobre la propuesta de Decisión del Consejo relativa a la celebración del Acuerdo entre los Estados Unidos de América y la Unión Europea sobre la utilización y la transferencia de los registros de nombres de los pasajeros al Departamento de Seguridad del Territorio Nacional de los Estados Unidos. Bruselas, 9 de diciembre de 2011. (2012/C 35/03). (DOUE C 35 de 9 de febrero de 2012).
- Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: La protección de la privacidad en un mundo interconectado. Un marco europeo de protección de datos para el siglo XXI. Bruselas, 25.1.2012. COM(2012) 9 final.
  Disponible en:
  http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0009:FIN:ES:PDF
- 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. Bruselas, 25.1.2012. COM(2012) 10 final. 2012/0010 (COD).
  Disponible en:

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:ES:PDF

- Propuesta de 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 (Reglamento general de protección de datos). Bruselas, 25.1.2012. COM(2012) 11 final. 2012/0011 (COD).
  Disponible en:
  http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:ES:PDF
- 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.
  Disponible en:
  http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0012:FIN:ES:PDF
- 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 a la 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.
  Disponible en:
  http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_73_es.pdf

- Dictamen del Supervisor Europeo de Protección de Datos, de 7 de marzo de 2012, sobre el paquete legislativo de reforma de la protección de datos. (2012/C 192/05). (DOUE C 192 de 30 de junio de 2012).
- Dictamen del Comité Económico y Social Europeo, de 23 de mayo de 2012, sobre la «Propuesta de 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 (Reglamento general de protección de datos)». (2012/C 229/17). (DOUE C 229 de 31 de julio de 2012).
- Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Liberar el potencial de la computación en nube en Europa. Bruselas, 27.9.2012. COM(2012) 529 final.

  Disponible en:

  http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:ES:PDF
- Dictamen del Supervisor Europeo de Protección de Datos, de 16 de noviembre de 2012, en cuanto a la Comunicación de la Comisión sobre "Liberar el potencial de la computación en nube en Europa".

  Disponible en:

  http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf
- Dictamen del Comité de las Regiones – Paquete sobre la protección de datos. (2012/C 391/13). (DOUE C 391 de 18 de diciembre de 2012).
- Comunicado de prensa: La UE aprueba las normas sobre protección de datos de Nueva Zelanda, que ayudarán a impulsar el comercio. Bruselas, 19 de diciembre de 2012. IP/12/1403.

  Disponible en: http://europa.eu/rapid/press-release_IP-12-1403_es.htm

- Otros documentos:

- Sentencia del Tribunal Constitucional (Sala Primera) 254/1993, de 20 de julio de 1993, en relación al efecto directo, o en su caso interpretativo, del Convenio nº 108 del Consejo de Europa. Publicada en el BOE de 18 de agosto de 1993.
- Lignes directrices de l'OCDE sur la protection de la vie privée et les flux transfrontières de données de caractère personnel. Service des Publications de l'OCDE. Paris 2001.
- Sentencia de la Audiencia Nacional (Sala de lo Contencioso-Administrativo, Sección Primera) de 15 de marzo de 2002, en relación con la Instrucción número 1/2000, de 1 de diciembre. Sentencia del Tribunal Supremo (Sala de lo Contencioso) de 25 de Septiembre de 2006 (desestimando el recurso de casación interpuesto).
- Estudio sobre Protección de Datos a nivel internacional. Instituto Federal de Acceso a la Información y Protección de Datos (Mexico). Noviembre 2004. Disponible en http://www.ifai.org.mx/
- Documento "Guidance on the use of cloud computing". Information Commissioner's Office (ICO). Octubre 2012. Disponible en http://www.ico.gov.uk
- Documento "Transferts de données à caractère personnel vers des pays non membres de l'Union européenne". Comisión Nacional de Informática y Libertades (CNIL) de Francia. Disponible en http://www.cnil.fr/
- Documento "Les clauses contractuelles types de la Commission Europeenne". Comisión Nacional de Informática y Libertades (CNIL) de Francia. Disponible en http://www.cnil.fr/
- Documento "Le safe harbor". Comisión Nacional de Informática y Libertades (CNIL) de Francia. Disponible en http://www.cnil.fr/
- Documento "Les exceptions". Comisión Nacional de Informática y Libertades (CNIL) de Francia. Disponible en http://www.cnil.fr/
- Documento "Les BCR – Binding Corporate Rules ou Regles Internes d'Enterprise". Comisión Nacional de Informática y Libertades (CNIL) de Francia. Disponible en: http://www.cnil.fr/

- Transferencias internacionales a países con niveles adecuados y no adecuados de protección. Aspectos prácticos. Ponencia de Jessica Matus Arenas para el Seminario Regional de Protección de Datos, Montevideo, Uruguay (1 a 4 de junio de 2010). Disponible en http://www.consejotransparencia.cl/
- Cloud Computing. La tercera ola de las Tecnologías de la Información. Fundación de la Innovación Bankinter. 2010. Disponible en: http://www.fundacionbankinter.org/es/publications
- Guía para empresas: seguridad y privacidad del *cloud computing*. Observatorio de la Seguridad de la Información. Instituto Nacional de Tecnologías de la Comunicación. Octubre de 2011. Disponible en http://www.inteco.es/