LA TRANSFERENCIA INTERNACIONAL DE DATOS DE CARÁCTER PERSONAL

INTERNATIONAL TRANSFER OF PERSONAL DATA

VICENTE GUASCH PORTAS

Profesor de la Escuela Universitaria de Turismo
del Consell Insular de Ibiza
Doctorando del Departamento de Derecho Constitucional de la UNED

Resumen: La normativa de la Unión Europea 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. Para evitarlo se han regulado minuciosamente las transferencias internacionales de datos. En este trabajo se pretende dar luz a algunos de los aspectos menos conocidos de los movimientos internacionales de datos personales. Analizamos un documento fundamental del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE: el WP 12. Revisamos la competencia de la AEPD en cuanto a la evaluación de los Estados que proporcionan un nivel adecuado de protección. Examinamos la necesidad de cumplir con las disposiciones legales en el caso de transferencia internacional. Por último reflexionamos sobre los cambios previstos en la propuesta de Reglamento comunitario de protección de datos.

Abstract: The European Union legislation in the field of data protection is the most demanding in the world. But there are countries with lax regulation, or no regulation of any kind. These differences may lead to the protection achieved within the Union lost in

the moment that the data may be located in countries with a lower level of protection or completely invalid. To avoid this we have carefully regulated international data transfers. This paper aims to shed light on some of the lesser known aspects of international flows of personal data. We analyzed a fundamental document of the Working Group of Article 29 of Directive 95/46/EC: the WP 12. We review the jurisdiction of the AEPD regarding the evaluation of states that provide an adequate level of protection. We examined the need to comply with the laws in the case of international transfer. Finally we reflect on the changes envisaged in the proposed EU regulation on data protection.

Palabras clave: Transferencia internacional, protección adecuada, protección de datos, nivel adecuado.

Keywords: International transfer, adequate protection, data protection, appropriate level.

Recepción original: 01/10/2012
Aceptación original: 04/10/2012

I. INTRODUCCIÓN

El artículo 5.1.s) 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, 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».

Según esta definición 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.

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. Sin embargo es necesaria la regulación de las transferencias internacionales para garantizar la debida protección de datos.

El gran avance de la tecnología[1], junto con el fenómeno de la globalización, ha llevado a un aumento muy importante de los flujos transfronterizos de datos.

[1] 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

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[2]. Las empresas multinacionales necesitan que la información pueda fluir entre sus diferentes sedes[3]. 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 de datos. Para poder contratar estos servicios, es necesario que los datos sean accesibles a los prestadores de los mismos.

En segundo lugar encontramos 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).

Son pioneras en el ámbito del Derecho las Líneas Directrices de la OCDE sobre protección de la intimidad y los flujos transfronterizos de datos personales de 23 de septiembre de 1980[4]. Ante la llegada

datos para adaptarlas a los cambios que la globalización y las nuevas tecnologías han traído consigo.

[2] 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**

[3] 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**

[4] Véanse las «Lignes directrices régissant la protection de la vie privée et les flux

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 cuando:

1) los Estados receptores «no observen» el contenido de las Directrices;

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

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*[5]. 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.

En la conferencia ministerial de la OCDE «Un mundo sin fronteras: determinación del potencial del comercio electrónico», celebrada en 1998 en 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

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.

[5] 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*.

redes globales y evitar restricciones innecesarias en los flujos transfronterizos de datos personales.

Conviene también la referencia de 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[6], 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 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[7].

En tercer lugar, y sin seguir un orden cronológico, podemos citar el Convenio 108 del Consejo de Europa, para la protección de las

[6] 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.

[7] 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.

personas con respecto al tratamiento automatizado de datos de carácter personal, de 28 de enero de 1981[8].

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.

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[9].

A través de Protocolo Adicional al Convenio 108 (suscrito el 8 de noviembre de 2001)[10], 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».

[8] 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/**

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

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

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.

En cuarto lugar podemos centrarnos en 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 miembros dispondrán que la transferencia a un país tercero[11] 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[12], 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 comunitario. 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,

[11] El documento denominado *FREQUENTLY ASKED QUESTIONS RELATING TO TRANSFERS OF PERSONAL DATA FROM THE EU/EEA TO THIRD COUNTRIES*, elaborado por la Comisión Europea, establece 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**

[12] 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 en la mayor parte de los casos han tenido que ser sustancialmente adaptadas»[13].

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[14].

En quinto y último lugar, analizamos la regulación de nuestro país en relación a la transferencia internacional de datos. Aunque en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante 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 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 (en adelante 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.

En el artículo 33.1 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal se establece que: «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 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

---

[13] 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, 3.ª época, núm. 7, 2004, pág. 397-417.

[14] 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.

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.

II. UN DOCUMENTO DE TRABAJO FUNDAMENTAL: 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 (en adelante G-29). 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».

II.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 Jessica 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[15].

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 lo dispuesto en el Convenio 108 del Consejo de Europa, que a la vez es concordante con lo incluido en las directrices de la OCDE de 1980 o en las directrices de la ONU. Por todo ello, el G-29 entiende 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 comunitarios. 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[16]. Habrá que considerar entonces no solo el contenido de

[15] Obra citada, pág. 4.

[16] 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

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 G-29 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 G-29, la compilación de una lista básica de condiciones mínimas es un punto de partida útil para cualquier análisis.

---

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**

Los principios de contenido sugeridos por el G-29 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[17].

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, 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

[17] *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.

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.** 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[18], el 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.

[18] *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.

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.

En cuanto a los mecanismos del procedimiento/de aplicación, el G-29 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 G-29 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 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. Este 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.

II.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 WP 12, se contempla la aplicación del enfoque que hemos estado analizando, a los

países que han ratificado el Convenio 108 del Consejo de Europa[19]. Como bien indica el Documento, el Convenio 108 es un 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 G-29 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/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 comunitario 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 su incumplimiento. Con ello se cubrirían 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.

[19] En la página web del Consejo de Europa, a fecha 13 de noviembre de 2012, 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 lo han ratificado, Rusia y Turquía.

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 G-29 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 G-29 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 dirijan de nuevo a la UE o a otro destino que ofrezca una protección adecuada.

Posteriormente 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)[20], en el que se han tenido en cuenta los dos puntos débiles mencionados anteriormente.

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.

[20] En la página web del Consejo de Europa, a fecha 13 de noviembre de 2012, 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.

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 importadores aseguran 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 de intereses legítimos, especialmente los de carácter público.

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.

II.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 G-29 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.

II.4. La función de las disposiciones contractuales

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 Comunidad (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.

II.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 Comunidad 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 comunitario, 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 G-29 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 G-29 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 embarazosa 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[21]. La Comisión 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.

III. LA EVALUACIÓN DE LOS ESTADOS QUE PROPORCIONAN UN NIVEL ADECUADO DE PROTECCIÓN POR PARTE DE LA AEPD

La Comisión Europea está habilitada por la Directiva 95/46/CE para evaluar si un país garantiza un nivel adecuado de protección

[21] 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.

de los datos personales transferidos desde la Unión Europea. Pero existe una segunda vía para efectuar dicho análisis: 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. Nos centraremos en esta segunda vía, bastante menos conocida que la primera.

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 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 RLOPD 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[22] 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[23] 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[24], por la que se aprueba la primera relación de países con protección de datos de carácter personal equiparable a la española, a 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.

[22] 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).

[23] 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.

[24] BOE del 10 de febrero de 1995.

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[25]. 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

[25] BOE del 21 de agosto de 1998.

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 era 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 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»[26]. 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 Ley Orgánica 15/1999, 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 Ley Orgánica, 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, «esta materia, en buena lógica-

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

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»[27]. 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.

IV. 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[28].

Como indican Barceló y Pérez[29], «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 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), etcétera».

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).

---

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

[28] 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/**

[29] 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.

IV.1. 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 Ley Orgánica 15/1999, 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[30] deberá haber informado a los afectados de quiénes serán destinatarios de los datos, así como de la 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 Ley Orgánica 15/1999.

IV.2. 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

[30] 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).

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.

IV.3. 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.

IV.4. 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 está prevista de antemano, 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.

IV.5. 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 de las Comunidades Europeas:

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 de las Comunidades Europeas.

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»[31].

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[32] Hungría[33] y principios de puerto seguro en Estados Unidos[34]), 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 procedimiento a seguir para

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

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

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

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

ordenar la suspensión temporal: la suspensión se acordará previa la tramitación del procedimiento establecido en la sección segunda del capítulo V del título IX del RLOPD.

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.

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

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 Inter-

net. 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[35].

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. En este ámbito, 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, pro-

[35] 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.

porcionando 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 en ninguna parte el concepto de transferencia de datos. En el Dictamen del Comité Económico y Social Europeo sobre la Propuesta de Reglamento[36] 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 G-29 en su Documento WP 191[37] 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):

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

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

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

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 G-29 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[38] 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 G-29 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 pro-

[38] 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

tección de datos también tienen la posibilidad de efectuar dichas evaluaciones. En este sentido se expresa el artículo 67 del RLOPD, si bien como hemos señalado anteriormente, en la práctica no se ha tomado ninguna determinación de adecuación por parte de la AEPD.

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.

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.