TRANSFERENCIAS INTERNACIONALES A PAÍSES CON NIVELES ADECUADOS Y NO ADECUADOS DE PROTECCIÓN. ASPECTOS PRÁCTICOS[1]

INTRODUCCIÓN

Hemos visto cómo la integración económica y social ha implicado notoriamente un aumento de los flujos transfronterizos de datos personales entre los agentes públicos y privados, de la vida económica y social de los países de la Unión Europea. A la par, el intercambio de datos personales entre empresas establecidas en los diversos Estados miembros de la Unión Europea experimenta un gran desarrollo, y los gobiernos nacionales, aplicando el derecho comunitario, han colaborado para otorgar el espacio sin fronteras que constituye el mercado interior en Europa.

En este orden de cosas, la dictación de la Directiva 95/46/CE ha facilitado que haya una legislación armonizada, lo que está permitiendo además que la transmisión o transferencia de datos personales entre los países miembros se realice con una adecuada seguridad, estableciéndose legislaciones equiparadas en cuanto a los niveles de protección de derechos y libertades de las personas. Esto ha demostrado que la protección de los datos personales no puede ser dirigida exclusivamente a nivel nacional.

Establecido como principio, la libre circulación de los datos, y habida consideración de la globalización y estado de avance de las tecnologías, es un hecho innegable que los relativos a las personas circulen de un Estado a otro de manera considerable y frecuente, lo que exige necesariamente una protección a estos datos.

Por ello, cuando estas transferencias internacionales se realizan fuera del Espacio Económico Europeo, las diversas regulaciones internacionales comunitarias han prescrito, en variados términos, que los países afectados por tales transferencias deben ofrecer garantías comparables de protección de la vida privada a sus derechos y libertades fundamentales y que garanticen el ejercicio de sus respectivos derechos o que el tercer país –importador del dato- garantice un nivel adecuado de protección.

TRANSFERENCIAS INTERNACIONALES

Una **Transferencia Internacional de Datos**, constituye un tratamiento que consiste en la transmisión o transporte de datos, fuera de un Estado, realizado por el responsable del tratamiento directamente a una persona natural (física) o jurídica, que los recibirá en un tercer país, para someterlos a un nuevo tratamiento de datos, bien sea por cuenta propia o por cuenta del transmitente de los datos.

Intervienen en este proceso dos agentes: un exportador de los datos y un importador de los mismos. **Exportador** de datos es el responsable del tratamiento que transfiera los datos personales. **Importador** de datos es el responsable del tratamiento que acepta recibir del exportador datos personales para su posterior tratamiento, o el encargado del tratamiento que convenga en recibir del exportador datos personales para su posterior tratamiento en nombre de éste, conforme a las instrucciones que aquél le entrega.

REGULACIÓN.

[1] Ponencia para Seminario Regional de Protección de Datos, Montevideo, Uruguay (1° al 4 de junio de 2010). Elaborado por **Jessica Matus Arenas**, abogada de la Unidad de Normativa y Regulación del Consejo para la Transparencia. Coautora del libro "La Cesión de Datos Personales", Editorial Lexis Nexis, 2006. Cocreadora del sitio Web http://protecciondedatospersonales.cl/

Encontramos diversos instrumentos regulatorios que se refieren a estos flujos internacionales:

1. Directrices de la ONU. Las Directrices para la regulación de los archivos de datos personales informatizados, aprobadas en el año 1990 por las Naciones Unidas, establecen respecto del "flujo transfronterizo de datos" (expresión que utiliza), que: *"9. Cuando la legislación de dos o más países afectados por un flujo transfronterizo de datos* ***ofrezca salvaguardas similares*** *para la protección de la intimidad, la información debe poder circular tan libremente como dentro de cada uno de los territorios afectados. En caso de que* ***no existan salvaguardas recíprocas****, no deberán imponerse limitaciones indebidas a tal circulación, sino solamente en la medida en que lo exija la protección de la intimidad".* En otras palabras, 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 salvaguardas recíprocas se limitarán las transmisiones en la medida que lo exija la protección de la intimidad.

Estas Directrices establecen, dentro de las garantías mínimas que deben prever las legislaciones nacionales, la designación de una "autoridad que, de acuerdo con su sistema jurídico interno, vaya a ser responsable de supervisar la observancia de los principios arriba establecidos. Esta autoridad ofrecerá garantías de imparcialidad, independencia frente a las personas o agencias responsables de procesar y establecer los datos, y competencia técnica. En caso de violación de lo dispuesto en la ley nacional que lleve a la práctica los principios anteriormente mencionados, deben contemplarse condenas penales u otras sanciones, junto con los recursos individuales adecuados"[2], esta es una de las mayores falencias que presenta nuestro país a la hora de pensar en cumplir los estándares internacionales en materia de protección de datos.

2. Convenio 108 del Consejo de Europa. Respecto de los flujos transfronterizos de datos (término empleado), el Capítulo III, en su artículo 12, numeral 2° dispone que "*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*", esta es la regla general; sin embargo, cualquier Parte del Convenio, tiene la facultad de establecer una excepción: "*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****; y 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"*[3].

El Convenio utiliza la expresión "equivalente", tan ambigua como el término utilizado por las Directrices de la ONU "comparable" o "similar", o el de las Directrices de la OCDE y Directiva Europea 46/95/CE "adecuado".

Respecto de la existencia de una autoridad de control, el Convenio no se encarga de ello, no obstante, mediante el Protocolo Adicional de Convenio Nº 108 para la Protección de las Personas con respecto al tratamiento automatizado de Datos de Carácter Personal y relativo a Transferencias de Datos, se incorpora.

3. Directrices de la OCDE. Estas Directrices, relativas a la protección de la intimidad y de la circulación transfronteriza de datos personales, reconocen que existe el peligro de que las disparidades en las legislaciones nacionales pudieran obstaculizar la libre circulación transfronteriza de datos personales, y que las restricciones a esta circulación podrían ocasionar graves trastornos

[2] Principio 8. Supervisión y sanciones.
[3] Artículo 12, numeral 3°.

en importantes sectores de la economía, tales como la banca y los seguros. Por este motivo, señala el texto, "los países miembro de la OCDE han considerado necesario elaborar Directrices que ayuden a armonizar la legislación nacional relativa a la intimidad y que, a la vez que defiendan tales derechos, impidan interrupciones en la circulación internacional de datos. Representan un consenso sobre principios básicos que pueden incorporarse a la legislación nacional existente o servir de fundamento para la legislación en aquellos países que todavía no dispongan de ella".[4]

Como principios básicos de aplicación nacional se establecen los de limitación en la recogida de los datos, licitud, calidad de los datos, especificación de la finalidad, limitación de su uso, seguridad, responsabilidad, entre otros. Cabe añadir que estas Directrices deben considerarse como criterios mínimos susceptibles de ser suplementadas con medidas adicionales para la protección de la intimidad y las libertades individuales.

En materia de transferencia internacional de datos, las Directrices recomiendan que los Estados incorporen a su normativa interna principios básicos, entre ellos, la cooperación y coordinación a nivel internacional, *medidas razonables y oportunas para garantizar la circulación transfronteriza, ininterrumpida y segura de los datos personales, incluso el tránsito a través de algún país miembro (*principio de seguridad en el tráfico de los datos); l*a circulación transfronteriza de datos entre dos países miembro no debería restringirse, salvo que* el segundo país aún no haya observado sustancialmente estas Directrices, por ejemplo; entre otras. En definitiva, se intenta nuevamente buscar un equilibrio entre la protección de la intimidad y la libre circulación internacional de la información.

4. Directiva 95/46/CE. En consonancia con la línea de respeto y reconocimiento de los derechos y libertades fundamentales de las personas físicas seguida en los últimos años por la Unión Europea, la norma nace con el objeto de garantizar su protección y, en particular, la del derecho a la intimidad en el tratamiento de sus datos personales, garantizando el principio de la libre circulación de tales datos entre los Estados miembros.

La transferencia de datos personales a países terceros se encuentra contenido en el Capítulo IV de la Directiva, en el que se establecen primeramente los principios y luego las excepciones, en los artículos 25 y 26, respectivamente.

La regla general es que la transferencia fuera del ámbito comunitario sólo puede efectuarse cuando exista un **nivel de protección adecuado** en aquel país. Si bien la Directiva no contribuyó a clarificar los conceptos ambiguos de los textos internacionales ya analizados, el Grupo de Trabajo creado por el artículo 29 de la Directiva –G29-, mediante Documentos de Trabajo que adoptan, ha contribuido a la interpretación de tal expresión, así como también las Decisiones del Consejo de Europa[5].

PAÍSES CON NIVEL ADECUADO Y NO ADECUADO/ ASPECTOS PRÁCTICOS

[4] Busca reconciliar los valores fundamentales en oposición (intimidad y libre circulación de información), como el resto de los instrumentos jurídicos internacionales; la elaboración de normas y prácticas compatibles; que la circulación transfronteriza de datos personales contribuya al desarrollo económico y social; fomentar la libre circulación de información entre los países miembro y evitar la creación de obstáculos injustificados al desarrollo de las relaciones económicas y sociales entre los países miembro. Directrices relativas a la Protección de la Intimidad y de la Circulación Transfronteriza de Datos Personales, de 23 de septiembre de 1980, Organización para la Cooperación y Desarrollo Económico -OCDE-. [en línea] Fuente: <https://www.agpd.es/portalweb/canaldocumentacion/legislacion/organismos_internacionales/ocde/common/pdfs/OCDE-Directrices-sobre-protecci-oo-n-de-privacidad-Trad..pdf> [consulta 14 de octubre de 2008].

[5] A modo ejemplar, **WP 4 (5020/97)** «Primeras orientaciones sobre la transferencia de datos personales a terceros países — Posibles formas de evaluar la adecuación», documento de debate adoptado por el Grupo de trabajo el 26 de junio de 1997; **WP 7 (5057/97)** Documento de trabajo: «Evaluación de la autorregulación industrial: ¿En qué casos realiza una contribución significativa al nivel de protección de datos en un país tercero?», adoptado por el Grupo de trabajo el 14 de enero de 1998; **WP 9 (5005/98)** Documento de trabajo: «Conclusiones preliminares sobre la utilización de disposiciones contractuales en caso de transferencia de datos personales a terceros países», adoptado por el Grupo de trabajo el 22 de abril de 1998; y uno de los más importantes, el Documento **WP 12**: «Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la Unión Europea», adoptado por el Grupo de trabajo el 24 de julio de 1998. [en línea] Fuente: <http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp12es.pdf> [consulta el 30 de octubre de 2008].

El **artículo 25** de la Directiva dispone que el **"carácter adecuado"** del nivel de protección de un país tercero se evalúa "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".

Lo previsto en este artículo 25 es uno de los aspectos de la Directiva que mayor polémica ha suscitado en terceros países, conforme al cual se prohíbe la exportación de datos personales, y por tanto, se impide la realización de transacciones comerciales a aquellos países que no respeten los criterios de privacidad de la Unión Europea.

No obstante lo evidenciado, es la doctrina y estudiosos de la materia los que realizan los mayores esfuerzos en influir en los gobiernos latinoamericanos para que la protección de datos sea un tema puesto en la cartera de proyectos legislativos.

¿QUÉ DEBE ENTENDERSE POR "PROTECCIÓN ADECUADA"?

En principio, 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.

La expresión "protección adecuada"[6] se refiere, en primer término, a que los terceros países deben garantizar el conjunto de principios básicos de protección de datos contenido en la Directiva Europea, y garantizar dichos principios de una manera efectiva, por ello, como se ha expresado, no basta la sola legislación que plasme estos principios, sino que se establezcan los medios idóneos para ejercitar estos derechos, esto es, que exista un órgano de control responsable de la protección de datos no sólo autónomo sino independiente, con un campo de aplicación amplio, esto es, público y privado, facultades de fiscalización y sancionadoras, un catálogo de infracciones y sanciones que sean disuasivas para los responsables de bancos de datos, acciones administrativas y/o judiciales, medidas de seguridad, la promoción de los derechos de los titulares de datos y de las obligaciones respecto de los bancos de datos, disponer de sistemas de responsabilidad y reparación para los afectados cuando no se de cumplimiento a las normas establecidas.[7]

El Grupo de Trabajo del artículo 29 ha publicado orientaciones sobre la elaboración de las evaluaciones del nivel adecuado de protección de terceros países, así mediante el WP 4, XV

[6] El autor Yves Poullet explica "de acuerdo con el famoso "*Methodology Paper*" (Documento sobre Metodología), adoptado por el Grupo del Artículo 29 en 1998, debe distinguirse el concepto de protección adecuada de otros conceptos como los de "protección equivalente" o "protección suficiente". En efecto, de acuerdo con "*Methodology Paper*", "protección adecuada" no significa "protección equivalente". La equivalencia habría requerido una comparación analítica estricta entre dos documentos de naturaleza similar, es decir, entre la ley extranjera y la de la UE. En otras palabras, el criterio de una protección equivalente habría requerido la adopción por parte del país tercero de una legislación, que podría considerarse una copia de la Directiva. Con el requisito de protección adecuada la cuestión que habría que resolver sería diferente y podría expresarse de la siguiente manera: considerando los riesgos específicos para la privacidad relacionados con un TID y considerando el número y la calidad de los datos transferidos, los tipos de usos que busca la transferencia, las posibles transferencias futuras, etc., podemos considerar si la protección de los datos de los interesados está o no garantizada, de acuerdo con los principales requisitos de la Directiva de la UE". **POULLET, YVES**. 2006. "Flujos de datos transfronterizos y extraterritorialidad: la postura europea". Revista española de Protección de Datos Nº 1, Julio-Diciembre. Madrid, Agencia de Protección de Datos de la Comunidad de Madrid-Civitas.

[7] Justamente a este tipo de deficiencias presentes en la legislación nacional se hace referencia en **GONZÁLEZ HOCH, Francisco**. "Modelos comparados de protección de la Información Digital y la Ley chilena de Datos de Carácter Personal. Cuadernos de Extensión Jurídica Nº 5 Tratamiento de datos personales y protección de la vida privada, Estudios sobre la Ley Nº 19.628, sobre protección de los datos de carácter personal". 2001. Facultad de Derecho de la Universidad de los Andes.

D/5020/97, de 26 de junio de 1997, se publicaron las *Primeras Orientaciones sobre la transferencia de datos personales a terceros países. Posibles formas de evaluar la adecuación.* Pero sin duda, el documento más importante, y considerado en las Decisiones de la Comisión de las Comunidades Europeas es el **WP 12** DG XV D/5025/98, de 24 de julio de 1998, denominado *Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la Unión Europea*[8].

El WP 12 del G29 sienta pautas para analizar transferencias a terceros países, incluyendo un análisis de la autorregulación industrial, la función de disposiciones contractuales, las excepciones al requisito de adecuación y cuestiones de procedimiento. Asimismo, distingue la aplicación del enfoque a los países que han ratificado el Convenio 108, de aquellos que no lo han hecho.

Ya se esbozó que: a) fuera del ámbito comunitario es menos común encontrar medios de procedimiento para asegurar el cumplimiento de las normas de protección de datos; b) que los signatarios del Convenio Nº 108 debían incorporar los principios de la protección de datos en su legislación, pero no se requerían mecanismos complementarios tales como una autoridad de control; c) que las directrices de la OCDE sólo exigen que "se tengan en cuenta" en la legislación nacional y no prevén procedimientos para garantizar que las directrices resulten en una protección efectiva de las personas físicas. Esto es lo que señala también el WP 12 de 1998, agregando que "las últimas directrices de la ONU sí incluyen disposiciones de control y sanciones, lo que refleja una creciente sensibilización a nivel mundial sobre la necesidad de aplicar debidamente las normas de protección de datos".

El Grupo concluye que el análisis de la protección adecuada comprende dos elementos básicos: el contenido de las normas aplicables y los medios para asegurar su aplicación eficaz.

Se habla de un "núcleo" de principios de "contenido" de protección de datos y de requisitos "de procedimiento/de aplicación", cuyo cumplimiento pudiera considerarse un requisito mínimo para juzgar adecuada la protección. Dicha lista mínima podría eventualmente ser alterable, reconociendo que en algunos casos será necesario ampliarla, mientras que en otros reducirla.

Estos **PRINCIPIOS DE CONTENIDO**, el WP12 los sistematiza de la siguiente forma:

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[9].

2) **Principio de proporcionalidad y de calidad de los datos.** Los datos deben ser exactos y, cuando sea necesario, estar actualizados. Además, 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[10].

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.

[8] El texto DG XV D/5025/98 WP 12, [en línea] Fuente: <https://www.agpd.es/portalweb/canaldocumentacion/docu_grupo_trabajo/wp29/1998/common/pdfs/wp12_es.pdf> [consulta 15 de octubre de 2008].
[9] Las únicas excepciones a esta norma serían las necesarias en una sociedad democrática por una de las razones expuestas en el artículo 13 de la Directiva.2
[10] Las únicas excepciones permitidas deben corresponder a los artículos 11.23 y 13 de la Directiva.

5) **Derechos de acceso, rectificación y oposición.** El interesado debe tener derecho a obtener una copia de todos los datos relativos a él, 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[11].

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[12].

Junto con estos principios básicos, a título de ejemplo, se indican principios adicionales que deberán aplicarse a tipos específicos de tratamiento. En primer lugar, respecto de los **datos sensibles**, deben adoptarse medidas adicionales como el consentimiento expreso del afectado para su tratamiento. En segundo término, tratándose de datos que se transfieran para efectos de marketing (**mercadotecnia directa**), el titular debe en cualquier momento tener la posibilidad de negarse a que sus datos sean utilizados con este propósito. Un tercer principio adicional se refiere al hecho de que cuando el objeto de la transferencia sea adoptar una decisión automatizada respecto de un individuo, éste debe tener derecho a conocer la lógica aplicada a dicha decisión y adoptarse todas las medidas necesarias para proteger el interés legítimo de la persona.

Respecto de los **MECANISMOS DEL PROCEDIMIENTO/DE APLICACIÓN**, existe consenso en que un sistema de "supervisión externa", en forma de una autoridad independiente, es una característica necesaria de un sistema de cumplimiento de la protección de datos.

Continúa el WP12 que "con el fin de sentar las bases para evaluar el carácter adecuado de la protección ofrecida, 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".

En definitiva, y con objeto de delimitar el concepto de protección adecuada, se señalan cuáles son los objetivos fundamentales que debe perseguir un sistema de protección de datos:

1) Ofrecer un **nivel satisfactorio de cumplimiento** de las normas. Ningún sistema puede garantizar el 100 % de cumplimiento, pero algunos son mejores que otros[13].

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

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

En definitiva, a la hora de evaluar el nivel adecuado de protección ofrecida en países terceros, la Comisión debería tener en cuenta la diferencia de desarrollo jurídico, económico y tecnológico entre los países terceros y los estándares europeos. Así lo expresa PALAZZI, conforme a lo indicado por el Parlamento Europeo al elaborar su informe sobre el Acuerdo Puerto Seguro; una protección adecuada no entraña por sí misma que el tercer país disponga de normas análogas a las de la Unión, sino que, independientemente del tipo de protección legislativa vigente en dicho país, el

[11] Las únicas excepciones a estos derechos deben estar en línea con el artículo 13 de la Directiva.
[12] Las únicas excepciones permitidas deben estar en línea con el artículo 26.1 de la Directiva.
[13] "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". WP12. 7p.

titular de los datos ha de recibir protección efectiva. Se considerará efectiva cuando sea posible medir su eficacia con referencia a datos objetivos[14].

En conclusión, y conforme a lo previsto por el artículo 25 para el nivel de protección adecuada deben evaluarse **todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos**, en particular:

- **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.**

Cabe mencionar que entre los Estados miembros y la Comisión existe una forma de control al establecerse en la Directiva que "se informarán recíprocamente de los casos en que consideren que un tercer país no garantiza un nivel de protección adecuado con arreglo a lo señalado precedentemente".

¿QUIÉN DEBE DECLARAR EL NIVEL "PROTECCIÓN ADECUADA" DE UN PAÍS TERCERO?

La Directiva impone a los Estados miembros una **obligación** de velar por que los datos personales no se transfieran a un tercer país a menos que garantice un nivel de protección adecuado, y establezca que la evaluación de la adecuación se lleva a cabo teniendo en cuenta todas las circunstancias. La Directiva no especifica, sin embargo, si se debe confiar a una autoridad la tarea de evaluar la adecuación de la protección de los datos en terceros países. Por tanto, es posible que la legislación nacional de los Estados miembros confíe esta tarea a las **autoridades nacionales de protección de datos**, cuya autorización puede exigirse para que la transferencia de datos personales a un tercer país pueda llevarse a efecto[15].

En el caso español, a modo ejemplar, se dispone que para que puedan efectuarse transferencias internacionales de datos, se requiere la autorización previa de la autoridad de control existente en dicho país, esto es, la Agencia Española de Protección de Datos; sin embargo, dicha autorización no será necesaria, conforme al artículo 66 del Real Decreto por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (entre otros casos que veremos más adelante) cuando el Estado en el que se encontrase el importador ofrezca un nivel adecuado de protección conforme a lo previsto en el Capítulo II del Título VI de dicho Reglamento, esto es, cuando el Director de la AEPD haya acordado mediante resolución que un determinado país proporciona un nivel adecuado de protección de datos. Asimismo, no se requerirá, según el artículo 68 del mismo cuerpo legal, cuando el nivel adecuado de protección haya sido declarado por la **Comisión Europea**.

DECLARACIÓN DE ADECUADACIÓN POR PARTE DE LA COMISIÓN EUROPEA.

La Directiva prevé que la Comisión, asistida por el Comité del artículo 31 de la Directiva, pueda adoptar decisiones en las que haga constar que un país tercero ofrece un nivel de protección

[14] **PALAZZI, Pablo A.** 2002. La Transmisión Internacional de Datos Personales y la Protección de la Privacidad. Buenos Aires, Ad-Hoc.130p.
[15] **2093/05/ES WP 114**, Documento de trabajo, relativo a una interpretación común del artículo 26, apartado 1, de la Directiva 95/46/CE , de 24 de octubre de 1995, adoptado el 25 de noviembre de 2005.

adecuado. Esto último, supone que las transferencias de datos personales a partir de cualquier Estado miembro de la Comunidad Europea (o del Espacio Económico Europeo) se haya permitida y no queda sujeta a autorización alguna por parte de las autoridades nacionales de protección de datos del Estado miembro desde el cual la transferencia se lleva a cabo.

Como ya se ha expuesto, los requisitos mínimos tenidos en consideración por la Comisión para evaluar y otorgar tal declaración de adecuación se encuentran consagrados en el Documento de Trabajo WP 12, del G29.

CONSECUENCIAS PRÁCTICAS FRENTE A LA NO ADECUACIÓN: Autorización previa a la transferencia.

- Producto de la consideración de Chile como no adecuado (y asimismo, todos los países de la región, salvo Argentina), frente a transferencias internacionales de datos en que nuestro país es importador de los mismos, conforme al apartado 2 del artículo 26 de la Directiva, pueden **autorizarse** estas transferencias siempre que el responsable del tratamiento ofrezca garantías suficientes respecto de la protección de la vida privada, de los derechos y libertades fundamentales de las personas, incluyendo la eficacia del ejercicio de los respectivos derechos. La norma permite que dichas garantías puedan derivarse, en particular, de cláusulas contractuales apropiadas[16].

- Por su parte, el apartado 4 del artículo 26 de la Directiva otorga la competencia a la Comisión de establecer determinadas **cláusulas contractuales tipo** que ofrecen las garantías suficientes establecidas en el apartado 2, debiendo los Estados miembros adoptar las medidas necesarias para ajustarse a la decisión de la Comisión.

  Las cláusulas contractuales tipo solamente están relacionadas con la protección de datos. El exportador de datos y el importador de datos tienen plena libertad para incluir cualquier otra cláusula sobre cuestiones relacionadas con sus negocios, siempre que no contradiga las cláusulas contractuales tipo. Asimismo, tienen como efecto exigir a los Estados miembros que no se nieguen a reconocer que estas cláusulas proporcionan las garantías adecuadas.
  El contenido de las cláusulas contractuales tipo se encuentra en la Decisión 2001/497/CE, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a un tercer país; en la Decisión 2002/16/CE, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países; en la Decisión 2004/915/CE, por la que se modifica la Decisión 2001/497/CE en lo relativo a la introducción de un conjunto alternativo de cláusulas contractuales tipo para la transferencia de datos personales a terceros países; y en la reciente la Decisión 2010/87/CE[17], relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, que tiene aplicación a partir del 15 de mayo de 2010.
  Este es el mecanismo que actualmente las empresas chilenas han debido adoptar para celebrar contratos con entidades privadas europeas, particularmente españolas, otorgando garantías por parte del "importador" chileno respecto de la responsabilidad, restricciones a

[16] Las autorizaciones que se otorguen por las autoridades de control en cada uno de los Estados miembros deben informarse a la Comisión Europea, así ésta ejercerá un control respecto de aquellas soluciones. Asimismo, la Comisión puede recomendar cláusulas contractuales tipo mediante Decisiones, estando los Estados miembros obligados a adoptar las medidas necesarias para ajustarse a dichas Decisiones. Es decir, en caso de oposición a la autorización, la Comisión puede anular o confirmar la decisión, de acuerdo con el procedimiento establecido en el artículo 31, y además permite que la Comisión, también de acuerdo con el procedimiento establecido en el artículo 31, pueda juzgar si ciertas cláusulas contractuales tipo ofrecen las garantías suficientes, siendo estos juicios vinculantes para los Estados miembros.

[17] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:ES:PDF

transferencias posteriores y medidas de seguridad y control. Conviene reafirmar que no basta que estos contratos se celebren al amparo de lo resuelto por la Comisión, sino que deben ser aprobados o autorizados por las autoridades de control del Estado exportador.

- Pero además, existe la alternativa de someterse a "códigos de conducta", las denominadas "Reglas Corporativas Vinculantes o *Binding Corporate Rules* (BCR´S), que son mecanismos de autorregulación en el seno de grupos multinacionales, por lo que deberá existir una garantía también de cumplimiento. Para el WP 12, de 1998, por código de autorregulación u otro instrumento debe entenderse "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."[18]

  Las características de las BCR es que son **vinculantes** para las empresas del Grupo y exigibles conforme al ordenamiento jurídico español, o de cualquier país miembro de la Unión Europea. La regulación y recomendaciones de las BCR se encuentran en los Documentos de Trabajo del Grupo de Trabajo del Artículo 29, WP 74[19], WP 107[20] y WP 108[21].

  Es necesario y relevante que el instrumento sea transparente e incluir el contenido básico de los principios esenciales de la protección de datos.

  Cabe precisar que estas normas corporativas vinculantes están sometidas y autorizadas por el Director de la AEPD.

En resumen, se trate de categoría de contratos o de normas corporativas vinculantes, es requisito para la transferencia internacional de datos personales que la Agencia Española de Protección de Datos emita las respectivas autorizaciones[22].

A estos efectos el artículo 33 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, establece que se requiere la autorización previa del Director de la Agencia cuando se pretenda realizar transferencias temporales o 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 ley española.

El artículo 34 continúa "el carácter adecuado del nivel de protección que ofrece el país de destino se evaluará por la Agencia atendiendo a todas las circunstancias que concurran en la transferencia o

[18] Esta definición abarcaría desde códigos de protección de datos voluntarios elaborados por pequeñas asociaciones industriales con pocos miembros, hasta los detallados códigos de ética profesional aplicables a profesiones enteras como los bancos.

[19] Adoptado el 03 de junio de 2003. [en línea] Fuente: <https://www.agpd.es/portalweb/canaldocumentacion/docu_grupo_trabajo/wp29/2003/common/pdfs/wp74_en.pdf> [consulta 01 de octubre de 2008].

[20] Adoptado el 14 de abril de 2005. [en línea] Fuente: <https://www.agpd.es/portalweb/canaldocumentacion/docu_grupo_trabajo/wp29/2005/common/pdfs/wp107_en.pdf> [consulta 01 de octubre de 2008].

[21] Adoptado el 14 de abril de 2005. [en línea] Fuente: <https://www.agpd.es/portalweb/canaldocumentacion/docu_grupo_trabajo/wp29/2005/common/pdfs/wp108_en.pdf> [consulta 01 de octubre de 2008].

[22] En España, conforme además a la Norma Primera de la Instrucción 1/2000, de 1 de diciembre, de la Agencia Española de Protección de Datos, relativa a las normas por las que se rigen los Movimientos Internacionales de Datos se considera transferencia internacional "toda transmisión de los mismos fuera del territorio español. En particular, se consideran como tales las que constituyan una cesión o comunicación de datos y las que tengan por objeto la realización de un tratamiento de datos por cuenta del responsable de fichero". tal Instrucción ha venido a fijar los criterios orientativos seguidos por la Agencia Española de Protección de Datos en la materia, aclarando a los interesados el procedimiento seguido para dar cumplimiento a las previsiones contenidas en la normativa reguladora de la materia.

categoría de transferencia de datos. En particular, se tomará en consideración la naturaleza de los datos de 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."

Ahora bien, el procedimiento se encuentra establecido en el Reglamento de Desarrollo de la Ley Orgánica 15/1999, aprobado mediante Real Decreto 1720/2007, de 21 de diciembre, en los artículos 137 y siguientes:

- **Iniciación del procedimiento**: Comienza con la respectiva solicitud del exportador, y copia del respectivo contrato de prestación de servicios. Se abre un expediente.
- **Instrucción del procedimiento**: En primer lugar, existe un periodo de información pública, se otorga un plazo de 10 días para que se puedan formular alegaciones, contados desde su publicación en el Diario Oficial del Estado. Transcurrido el plazo, si se hubieren formulado alegaciones, se dará traslado al solicitante de la autorización, quien tiene también un plazo de 10 días para alegar lo que estime procedente.
- **Actos posteriores a la resolución.** Una vez adoptada la resolución que autoriza la transferencia internacional, debe darse traslado de ésta al Registro General de Protección de Datos, para proceder a su inscripción, quien lo hace de oficio. No obstante, denegándose o autorizándose la transferencia, la resolución debe enviarse también al Ministerio de Justicia, para que se proceda a notificar a la Comisión Europea y a los demás Estados miembros de la Unión Europea, conforme a lo dispuesto por la Directiva 95/46/CE.

La duración de este procedimiento, por expresa disposición del artículo 140 del Reglamento, es de un plazo máximo de 3 meses para dictar y notificar la resolución, contados desde la entrada de la solicitud a la AEPD. Pero lo más interesante de dicha norma es que se entiende que se autoriza la transferencia internacional de datos en el evento que no se cumpla en el plazo señalado.

Cabe comentar en este punto que el tiempo de demora en el proceso de autorización ha sido uno de los factores que ha influido en la baja de transferencias a países no adecuados.

Cabe precisar que las autoridades de control tienen potestades de inspección presenciales, así, éstas concurren al país en que los datos se han exportado. El objetivo de la inspección, en el caso español, es verificar el efectivo cumplimiento de la Ley Orgánica 15/1999 y su normativa de desarrollo; principalmente observar la concreción de los servicios prestados, estudiar el modo de acceso, analizar la proporcionalidad, las medidas de seguridad y evaluar el entorno tecnológico de la transferencia; asimismo, concurren donde los responsables exportadores ubicados en el país europeo[23].

Finalmente, constituye falta muy grave, de acuerdo con lo dispuesto en el artículo 44.4.e) de la Ley Orgánica 15/1999, la transferencia temporal o definitiva 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 sin autorización del Director de la AEPD.

[23] Un Informe sobre transferencias internacionales de datos de la AEPD, da cuenta de la inspección sectorial de oficio realizada en España-Colombia en Centros de Atención al Cliente. [en línea] Fuente: <https://www.agpd.es/portalweb/jornadas/transferencias_internacionales_datos/common/pdfs/INFORME_TIs.pdf> [consulta 15 de octubre de 2008].

ALGUNAS ESTADÍSTICAS DE TRANSFERENCIAS A LATINOAMÉRICA

Respecto de las autorizaciones se debe dimensionar la importancia que éstas tienen para la economía de nuestro país, puesto que muchas veces las empresas europeas optan por contratar, en Latinoamérica, con compañías argentinas. Atendido el hecho de ser un país adecuado conforme a la Comisión Europea, las transferencias internacionales de datos personales no requieren de dicha autorización –cuya tramitación no es menor-, sino simplemente de la notificación de la transferencia a fin de proceder a su inscripción en el Registro General de Protección de Datos:

País importador de los datos	Autorizaciones 2008[24]	Autorizaciones 2009[25]	Autorizaciones 2010 (mayo)[26]	Total últimos 3 años
Chile	1	7	4	12
Perú	4	16	5	25
Colombia	4	12	5	21
Uruguay	4	1	5	10
Paraguay	4	3	2	9
México	3	8	2	13
Ecuador	-	-	1	1
Brasil	3	-	-	3
Costa Rica	1	-	-	1
Nicaragua	-	-	-	-
Panamá	2	-	-	2
El Salvador	-	-	-	-

Estas estadísticas permitirán, en definitiva, observar el panorama general: en los últimos tres años (hasta el mes de mayo de 2010) Chile sólo ha obtenido autorización en 12 oportunidades, y Perú lidera el cuadro con 25 autorizaciones de transferencias internacionales.

Sin embargo, puede observarse que respecto de Argentina, Declaración de Adecuación mediante en 2003, ha alcanzado desde esa fecha hasta el año 2009, 214 ficheros inscritos con destino a este país. La citada Declaración significa que a Argentina no se le aplican las restricciones para la transferencia de datos personales, permitiendo el libre flujo de los datos personales desde la Unión Europea.

Este reconocimiento, sin embargo, se encuentra sujeto a un control permanente que puede ser reevaluada en cualquier momento de conformidad con la experiencia de su funcionamiento o los cambios de la legislación argentina, su aplicación o su interpretación.

[24] Memoria de la AEPD 2008, p.77 [en línea] Fuente: <https://www.agpd.es/portalwebAGPD/canaldocumentacion/memorias/memoria_2008/common/memoria_new_2008.pdf > [consulta 20 mayo de 2010].
[25] [en línea] Fuente: <https://www.agpd.es/portalwebAGPD/resoluciones/autorizacion_transf/auto_transf_2009/index-ides-idphp.php> [consulta 20 mayo de 2010].
[26] [en línea] Fuente: <https://www.agpd.es/portalwebAGPD/resoluciones/autorizacion_transf/auto_transf_2010/index-ides-idphp.php> [consulta 20 mayo de 2010].

GUÍA PARA LA ADECUACIÓN

Durante el VI Encuentro Iberoamericano de Protección de Datos, realizado en el mes de mayo de 2008, la Comisión Europea, con el objeto de preparar las reuniones con los países de la Red Iberoamericana de Protección de Datos Personales, elaboró un cuestionario que contiene preguntas relativas a los aspectos a considerar acerca de la adecuación. De dicho cuestionario contiene las siguientes interrogantes**:**

¿Se considera la protección de datos personales como un derecho fundamental en su país?

I. ¿Existe en su país una normativa sobre protección de datos personales?

1. Ámbito material (entidades sometidas a la ley, entidades privadas, entidades públicas y gubernamentales, actividades sometidas a la ley comerciales, actividades de tratamiento de datos personales por autoridades policiales; entidades y actividades excluidas).
2. Ámbito territorial (nacional o federal, coexistencia con normas regionales o provinciales)
3. Ámbito personal (personas físicas y/o jurídicas)
4. Contenido y explicación del régimen previsto: principios que deben ser respetados por los responsables del tratamiento en las operaciones de tratamiento de datos personales.
5. ¿Existen normas particulares acerca del tratamiento de datos personales sensibles? (datos de salud o relativos a las convicciones políticas o religiosas, etc.)
6. ¿Existen normas especiales acerca de la utilización de datos personales para actividades de mercadotecnia directa?
7. ¿Existen limitaciones o excepciones a los principios de la ley en algunos supuestos de tratamientos de datos personales con miras a salvaguardar un interés público substancial? Cuáles.
8. Derechos de los interesados (acceso, información, rectificación, bloqueo y cancelación).
9. Medios y vías para garantizar la tutela de los derechos de los interesados y exigir el cumplimiento de la ley.
10. ¿Se prevé en la legislación nacional una obligación de notificación de las operaciones de tratamiento de datos personales a la autoridad encargada de la supervisión?
11. ¿Se trata de una obligación general o limitada a determinadas actividades? Indicar cuáles.
12. ¿Existe un registro público llevado por la autoridad de supervisión de las operaciones notificadas?, si no, ¿qué medio de información a los ciudadanos se ha previsto?
13. ¿Contiene la legislación nacional disposiciones relativas a las transferencias de datos personales a los países terceros?

II. Autoridad de supervisión.

14. ¿Existe una autoridad pública o autoridades encargadas de la supervisión del tratamiento de los datos personales y del cumplimiento de la legislación aplicable?
15. ¿Se trata de una autoridad independiente? A este respecto es importante tomar en consideración el procedimiento de nombramiento de la autoridad: a) si es designada por un plazo determinado y no puede ser removido; b) si existe una prohibición de recibir instrucciones por parte de otro organismo o autoridad; c) incompatibilidad para ejercer otra actividad o cargo a fin de evitar conflicto de intereses; d) si las decisiones tomadas por la autoridad pueden ser anuladas por un órgano político, o los recursos materiales y personales de que dispone para llevar a cabo sus funciones.

16. Poderes de la autoridad de protección de datos: a) poderes de investigación (derecho de acceder a los datos que sean objeto de un tratamiento y el de recabar toda la información necesaria para el cumplimiento de su función de control); b) poderes efectivos de intervención (ordenar el bloqueo, la supresión o la destrucción de datos, o incluso prohibir provisional o definitivamente un tratamiento, dirigir una advertencia o amonestación al responsable del tratamiento, imponer sanciones o someter la cuestión a los parlamentos u otras instituciones políticas nacionales); c) posibilidad de interponer recursos contra las resoluciones de la autoridad de supervisión; d) capacidad procesal en caso de infracciones nacionales, o de poner dichas infracciones en conocimiento de la autoridad judicial; e) competencia para recibir y atender reclamaciones efectuadas por los interesados con relación al tratamiento de sus datos personales.

III. Instrumentos internacionales.

17. ¿Aplica su país las Directrices de la OCDE, de 23 de septiembre de 1980?
18. ¿Aplica su país las Orientaciones de las Naciones Unidas, de 14 de diciembre de 1990 relativas a los ficheros de datos personales automatizados?
19. ¿Aplica su país el Pacto Internacional de Derechos Civiles y Políticos, de 16 de diciembre de 1966?

Conforme al contenido de este cuestionario, las respuestas que pudieran resultar son esclarecedoras, el camino de la adecuación en Chile será largo, bajo el supuesto obvio de una reforma a la legislación nacional actual[27].

SITUACIÓN EN CHILE Y LA NECESARIA MODIFICACIÓN A LA NORMATIVA INTERNA.

Como se señalara previamente, al ser considerado Chile un país con un nivel no adecuado de protección en materia de datos personales, ha sido sometido al mecanismo de las cláusulas tipo en los respectivos contratos que suscribe con empresas españolas, con el fin de alcanzar las autorizaciones que correspondan por la Agencia Española de Protección de Datos cuando se pretenden transferencias internacionales de los mismos. Es este el obligado camino que nuestro país deberá seguir mientras no se estatuya una legislación que permita a Chile solicitar a la Comisión Europea la declaración de adecuación de la protección.

Con fecha 01 de octubre de 2008 ingresó al Congreso el Mensaje de S.E. la Presidenta de la República, Nº 687-356, que contiene el proyecto de ley que introduce modificaciones a la Ley N° 19.628 –de Protección de la Vida Privada- y Ley N° 20.285 –de Acceso a la Información Pública-.

Dicho proyecto incluye las modificaciones necesarias para dar cumplimiento al estándar internacional europeo.

Respecto al órgano de control de protección de datos, en el proyecto:

a) Se establece el objeto de velar por el adecuado cumplimiento de la Ley Nº 19.628, por parte de organismos públicos y personas naturales, o jurídicas de carácter privado, junto con establecer un sistema único nacional de Registro de los bancos de datos personales.

[27] Con fecha 01 de octubre de 2008 se ingresó a la Cámara de Diputados el Proyecto de Ley que modifica la Ley Nº 19.628, de Protección de la Vida Privada y la Ley Nº 20.285, de Acceso a la Información de la Administración del Estado. Boletín Nº 6120-07, actualmente en primer trámite constitucional.

b) El Consejo para la Transparencia (órgano o institucionalidad creada para el Acceso a la Información Pública) pasa a denominarse “Consejo para la Transparencia y Protección de Datos Personales”.

c) El ámbito de aplicación de las facultades del Consejo, en cuanto a la protección de datos, sería respecto de organismos públicos y privados.

d) Dentro de las funciones del Consejo, se incorpora un nuevo artículo 33 bis, que establece las atribuciones y funciones relativas a la protección de datos personales. Resultan particularmente importantes las funciones de fiscalización, la dictación de instrucciones de carácter general, el conocimiento de las reclamaciones, la aplicación de las sanciones (multas), el proporcionar información a los titulares de datos, y la entrega de una cuenta anual.

Además, se dispone un régimen de infracciones y sanciones en la modificación de la Ley Nº 19.628. Las sanciones impuestas a organismos públicos, en caso de infracción a la ley, serán la suspensión en el cargo, por un lapso de cinco a quince días, y/o con multa de 20 a 50% de su remuneración; las impuestas a entidades privadas serían multas disuasivas.

Por otro lado, se aclaran conceptos claves como “fuente accesible al público” y “encargado del tratamiento” de los datos, en armonía con el estándar europeo en la materia.

Se vigoriza el “deber de información” al titular del dato por parte de los entes que los recaban.

Respecto del flujo transfronterizo de datos, se dispone un nuevo artículo 5 bis de la Ley Nº 19.628, que regula los movimientos internacionales de datos. En este caso, la autorización previa para este flujo transfronterizo de datos personales deberá otorgarla el Consejo, facultad que también se incorpora en el proyecto.