Transferencias internacionales a países con niveles adecuados y no adecuados de protección. Aspectos prácticos

Federico Carnikian[(*)]

(*) Doctor en Derecho y Ciencias Sociales. Asesor de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC).
Miembro del Grupo de Jurisprudencia del Instituto de Derecho Informático de la Universidad de la República.

1. Introducción

En el marco de la Sociedad de la Información, las ventajas que brindan las Tecnologías de la Información y Comunicación (TIC), permiten un intercambio continuo y automatizado de datos entre distintos Estados, a efectos de la prosecución y ejecución de una gran diversidad de actividades comerciales a nivel internacional, necesarias para el desarrollo de sus cometidos.

Es en este ámbito donde se debe prestar un especial resguardo a los datos personales de los titulares, ante la eventual vulneración de sus derechos, en virtud del constante y muchas veces desproporcionado tránsito de la información que les concierne y afecta.

Atento a la complejidad que reviste la temática en análisis, comenzaremos por abordar las transferencias internacionales de datos personales –en adelante TIDP- dentro del ámbito comunitario europeo para luego detenernos en las transferencias internacionales efectuadas a países que en la actualidad no cuentan con un nivel adecuado de protección, prestando especial énfasis en la situación uruguaya.

A nivel internacional, y más precisamente en el ámbito europeo existe un gran desarrollo normativo y jurisprudencial relativo a las TIDP.

No es posible realizar un estudio de las TIDP, sin nombrar dos instrumentos de gran relevancia e impacto internacional concernientes a la protección de los datos personales.

Al respecto, tenemos el Convenio Nº 108 del Consejo de Europa, de 1 de octubre de 1985, para la protección de las personas con respecto al tratamiento automatizado de los datos personales (en adelante Convenio 108) y la Directiva Nº 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante la Directiva).

Sin perjuicio de ello, y de conformidad con lo dispuesto en la Directiva mencionada, la Comisión Europea elaboró varias Decisiones en lo que respecta a la celebración de cláusulas contractuales tipo a efectos de la realización de TIDP a países que no cuentan con un nivel adecuado de protección.

Destacamos la Decisión Nº 2004/915/CE de 27 de diciembre de 2004 por la cual se modifica la Decisión Nº 2001/497/CE, en lo relativo a la introducción de cláusulas contractuales tipo para la transferencias internacionales de datos personales a terceros países y la Decisión Nº 2002/16/CE de 20 de febrero de 2002 relativa a las cláusulas contractuales tipo a los encargados de tratamiento establecidos en terceros países.

Con fecha 12 de febrero de 2010, se publicó la Decisión Nº 2010/87/CE -que deroga la Nº 2002/16/CE- relativa a las cláusulas contractuales tipo para la transferencia de datos personales relacionadas a la subcontratación de servicios efectuadas por un encargado de tratamiento establecido en un tercer país a otros encargados de tratamientos.

El presente trabajo tiene como intención, proporcionar una visión del régimen general de las TIDP y una primera apreciación y análisis del régimen de éstas desde la perspectiva del ordenamiento jurídico uruguayo.

No obstante lo señalado, y como punto de partida, es necesario precisar qué se entiende por transferencia internacional de datos y cuáles son sus distintas variantes.

2. Concepto

Como punto de partida, es interesante destacar lo que el autor Miguel Ángel Davara Rodríguez[1] expresa al respecto de la dualidad terminológica utilizada tanto el Convenio Nº 108 como la Directiva 95/46/CE, -éstos hablan de flujos y de transferencia de datos indistintamente- *"para nosotros el flujo de datos indica movimiento de datos y la transferencia incluye, además la acción de transferir, puede haber flujo de datos entre dos extremos sin que uno de ellos haya tomado ninguna acción de transferir datos". (…) "exige el concepto de transferencia una acción, característica que no se encuentra en el concepto de flujo…".*

El concepto de TIDP, se encuentra recogido en algunos instrumentos internacionales.

En la Recomendación de 23 de septiembre de 1980 dictada por la Organización para la Cooperación y el Desarrollo Económico (OCDE) se indica: *"por circulación transfronteriza de datos personales se entenderá los movimientos de datos personales a través de fronteras nacionales".*

La Instrucción Nº 1/2000 de 1 de diciembre de 2000, de la Agencia Española de Protección de Datos (AEPD), relativa a las normas por las cuales se rigen los movimientos internacionales de datos de carácter personal, define a las transferencias internacionales *como "toda transmisión de datos de carácter personal fuera del territorio español".*

[1] DAVARA RODRIGUEZ, Miguel Ángel "La Transferencia Internacional de Datos". Revista Española de Protección de Datos Julio – diciembre, 2006. Página. 23.

Se sostiene a nivel doctrinario que una transferencia internacional es en primer lugar una forma de tratamiento, que constituye una cesión o comunicación de datos personales y es promovida por un responsable del tratamiento[2].

De las definiciones expuestas anteriormente y de la normativa señalada supra, es posible identificar –a prima facie- la participación de dos partes. Esto es, el transmitente de la información o exportador de datos y el receptor de dicha información o importador de los datos personales.

Si bien en los instrumentos señalados no se brindan definiciones de exportador e importador de los datos, sí lo hacen las Decisiones aprobadas por las Comisión Europea al respecto de las cláusulas contractuales tipo para la realización de TIDP a países no adecuados.

Haciendo especial énfasis en la situación uruguaya, se procede a citar las definiciones que contempla el Decreto Nº 414/009 de 31 de agosto de 2009 reglamentario de la Ley uruguaya, Nº 18.331 de Protección de Datos Personales y Acción de Habeas Data –en adelante LPDP-.

La normativa señalada define al exportador de datos como: *"la persona física o jurídica pública o privada, situada en territorio uruguayo que realice, conforme a lo dispuesto en el presente reglamento, una transferencia de datos de carácter personal a otro país*" - literal E) del artículo 4 del Decreto Nº 414/009 de 31 de agosto de 2009 -.

Por su parte, el importador de datos es toda: *"persona física o jurídica, pública o privada, receptora de los datos de otro país, en caso de transferencia internacional de éstos, ya sea responsable del tratamiento, encargada del tratamiento o tercero"*-literal F) del artículo precitado-.

Al respecto de la definición de transferencias internacionales, el literal H) del artículo señalado la define como: *"tratamientos de datos que supone una transmisión de éstos fuera del territorio nacional, constituyendo una cesión o comunicación, y teniendo por objeto la realización de un tratamiento por cuenta del responsable de la base de datos o tratamiento establecido en territorio uruguayo".*

Cabe agregar que las TIDP siempre poseen el carácter de internacional y se refieren exclusivamente a las transferencias de datos personales[3].

---

[2] SANCHO VILLA, Diana "Normas Corporativas vinculantes (Binding Corporate Rules): aspectos sustantivos y de cooperación internacional de autoridades. Revista Española de Protección de Datos Enero – junio de 2008. Página 39.

[3] El literal D) del artículo 4 de la Ley Nº 18.331, de 11 de agosto de 2008, de Protección de Datos Personales y Acción de habeas Data (en adelante LPDP) define al dato personal como toda: "información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables".

En síntesis y de un análisis de las Decisiones de las Comunidades Europeas reseñadas y parte de la doctrina internacional, podemos definir a las TIDP como: *"toda transmisión de datos personales fuera de un Estado realizada por el exportador de datos de forma directa a un importador de datos, que los recibe en otro país, tratándolos por cuenta propia -para someterlos a un nuevo tratamiento - o por cuenta ajena y bajo las instrucciones del exportador de datos".*

3. Modalidades de las TIDP

Abordaremos el presente apartado contemplando en primer término, las figuras relacionadas con la realización de TIDP, diferenciando el concepto de cesión o comunicación de datos, de la prestación de servicios por parte de un Encargado de tratamiento, para luego dedicarnos a las variantes que estas transferencias presentan.

Esta diferenciación, nos permite comprender la distinción que las Decisiones de la Comunidad Europea realizan cuando hablan de transferencias de datos, y cuál es el régimen que les aplica en cada caso.

3.1. Figuras relacionadas con las TIDP

Cuando estamos ante una típica cesión o comunicación de datos personales, existen dos partes involucradas, esto es, un emisor y un receptor o destinatario de la información.

Los distintos regímenes relativos a la protección de los datos personales, contienen preceptos dedicados exclusivamente a la protección de los derechos de los titulares de los datos en casos de cesiones o comunicaciones. Incluso podríamos afirmar que estamos en presencia de un derecho de la comunicación de datos.

La razón de esta especial tutela, radica en que ante una eventual comunicación, y en el caso de no dar cumplimiento de ciertas condiciones legales, dichas cesiones estarán contrariando los principios generales de protección de datos personales.

En este sentido y siguiendo al autor reseñado, siempre que se trate de un tratamiento de información, se estará en presencia de al menos tres etapas o fases del procesamiento de datos[4].

Una primer etapa de recolección de los datos, donde el titular tiene total control de la información; una segunda fase de tratamiento de esa información y su utilización para los fines para los cuales fueron recogidos, donde si bien el control no es absoluto, el tratamiento se encuentra limitado por los principios

[4] DAVARA RODRIGUEZ, Miguel Ángel, "La transferencia internacional de datos". Ob. Cit. Página 24.

reinantes en la materia, en especial los principios de legalidad, finalidad, veracidad de los datos, etc; y una tercera etapa constituida por una eventual comunicación o cesión de los datos.

Es en este último caso donde para dar cumplimiento a la normativa de protección de datos, el emisor de la información deberá: a) obtener el consentimiento del interesado; b) informar al titular la finalidad de la comunicación; c) proporcionar la información relacionada con él o los destinatarios de los datos a efectos de su identificación.

Asimismo, la comunicación de datos sólo será legítima cuando sea efectuada en virtud de un interés legítimo para el cumplimiento de los fines del emisor y receptor de los datos -artículo 17 de la LPDP-.

En este sentido, las previsiones concernientes a proteger a los interesados en este tipo de situaciones son en razón a que el titular es vulnerable de perder de forma casi total el control de su información, trayendo consigo un tratamiento desleal e ilegítimo.

Las mismas fases de tratamiento se dan en supuestos de transferencias internacionales, recolección, tratamiento y posterior transmisión de los datos dentro los parámetros ya señalados.

Por lo tanto, y atento a lo dispuesto en la LPDP cuando estamos en presencia de transferencias internacionales que involucran a dos Responsables del tratamiento, se deberá dar cumplimiento también a los mismos requisitos exigidos para que una cesión de datos sea con arreglo a derecho -principio del previo consentimiento informado del titular de los datos, informar al titular acerca de la finalidad y las consecuencias que tiene transferir esa información, identificación del destinatario, y que las cesiones tengan como objeto el cumplimiento de los fines directamente relacionados con el interés legítimo del emisor y destinatario de los datos-.

En consecuencia, este tipo de TIDP -de Responsable del tratamiento a Responsable- constituyen una cesión o comunicación de datos propiamente dicha.

Además, interesa destacar que la información contenida en una base de datos sometida al tratamiento por parte de un Responsable, es trasmitida a otra base de datos perteneciente a otro Responsable a efectos de su posterior o mejor dicho, nuevo tratamiento de información.

A modo de reflexión decimos que el concepto de transferencia subyace al de comunicación de datos, en virtud de que las transferencias pueden constituir o no una cesión de datos personales.

Por ejemplo, un Responsable del tratamiento trasmite los datos pertenecientes a los empleados de su empresa, a la empresa matriz que centraliza la gestión

de recursos humanos, decidiendo este último sobre su finalidad contenido y uso del tratamiento[5]. En este caso, el receptor de los datos –como Responsable del tratamiento- realiza un posterior o nuevo tratamiento de los datos, decidiendo sobre la utilización y objeto que le dará a éstos.

Asimismo se agrega a lo expuesto, que en estos casos el importador de datos asume el riesgo o les es trasladada la responsabilidad del tratamiento de la información.

Sin embargo, ante la prestación de un servicio al Responsable por parte de un Encargado de tratamiento, la situación se modifica sustancialmente.

En los supuestos donde un Responsable trasmite datos personales a un Encargado de tratamiento, situado en otro Estado con el objeto de que éste preste un servicio, no estamos ante una comunicación de datos propiamente dicha.

A diferencia de las TIDP de Responsable del tratamiento a Responsable -donde existen tres fases del tratamiento-, en este segundo caso por lo general tenemos sólo un tratamiento de la información.

Esto significa que, el Encargado de tratamiento solamente accede a la base de datos perteneciente al Responsable y ejecuta las tareas encomendadas bajo la dirección e instrucciones de éste. Por lo tanto, el Encargado del tratamiento, no tiene potestad alguna para decidir sobre la finalidad, contenido y uso del tratamiento, limitándose a ejecutar los servicios que fueron acordados previamente con el Responsable.

Existen varias normativas, que excluyen expresamente estas situaciones del concepto de comunicación de datos. A vía de ejemplo, tenemos el artículo 14 del Decreto Nº 414/009 de 31 de agosto de 2009.

Tomando como referencia el ejemplo planteado acerca de los datos de recursos humanos, puede suceder que exista un Encargado del tratamiento que trate los datos por cuenta del Responsable, siendo éste el que decide cuándo se pagan los salarios, se fijan las fechas de licencia, entre otros ejemplos.

Otra prestación típica de servicios por parte de un Encargado de tratamiento podría ser el servicio de telemarketing o atención al cliente, donde éste trata la información en virtud de las directivas acordadas con el Responsable.

Aquí podemos decir que la responsabilidad por el riesgo del tratamiento, es mantenida por el Responsable.

[5] Curso Fundación CEDDET “La protección de los datos personales 1ª Edición”, Módulo 3, Página 81.

3.2. Tipos de TIDP recogidas por la normativa de protección de datos personales

Luego del análisis descrito anteriormente, se considera que de acuerdo con las definiciones contenidas en el Decreto reglamentario de la LPDP, estamos en condiciones de afirmar que la normativa uruguaya regula dos modalidades de TIDP:

a) de Responsable del tratamiento a Responsable: atento a que la definición mencionada expresa, que estamos ante un tratamiento que constituye una cesión o comunicación de datos y además que el concepto de importador de datos regulado, es omnicomprensivo abarcando también al Responsable del tratamiento establecido en otro país.

En este tipo de transferencia -como ya lo desarrollamos en el apartado anterior- existe una comunicación de datos propiamente dicha aplicándose los requisitos para las cesiones de datos dispuestos en el artículo 17 de la LPDP.

En efecto, el importador de datos -Responsable receptor de la información- realiza un nuevo tratamiento sobre éstos decidiendo sobre su uso, finalidad y contenido; y

b) de Responsable del tratamiento al Encargado del tratamiento: en virtud de que la normativa uruguaya permite al Responsable del tratamiento contratar los servicios de un Encargado del tratamiento, quien trata la información por cuenta ajena en relación con las directivas e instrucciones que aquél le establece.

La posición sustentada supra, se desprende fundamentalmente de un análisis interpretativo de la normativa vigente en materia de protección de datos personales en Uruguay, así como también de los criterios internacionales de mayor recibo en la materia que le fueron objeto de inspiración.

Siguiendo esta línea de razonamiento, por Dictamen Nº 8/2010 de 19 de marzo de 2010, del Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales estableció: *"Que en virtud de lo establecido por los literales E), F) y H) del artículo 4 del Decreto reglamentario, se considera que las transferencias internacionales reguladas por la normativa nacional vigente de protección de datos personales, son las que constituyen una cesión o comunicación de datos strictu sensu, esto es, de Responsable a Responsable de la base de datos, como las que tengan por objeto la realización de un tratamiento por cuenta del responsable de la base de datos, esto es, de Responsable a Encargado del tratamiento".*

Este mismo criterio es recogido por parte de la doctrina española la que afirma que: "de acuerdo al ordenamiento español, es posible distinguir dos tipos de transferencias internacionales, en función de la calificación del sujeto receptor de los datos: La primer modalidad se encuentra recogida en el art. 11 de la

LOPD[6], según la cual el sujeto transmitente puede provocar una cesión o transmisión de datos a un tercero localizado en el extranjero, operación que supone que el tercero que actúa por cuenta propia decidiendo sobre la finalidad, uso y contenido del tratamiento. La segunda modalidad está relacionada con el art. 12 de la LOPD, ya que en esta el sujeto que comunica los datos, lleva a cabo la transmisión de los mismos, a otro sujeto ubicado en el extranjero para que se realice un determinado tratamiento a su nombre y por su cuenta"[7].
De todas maneras la volatilidad de las situaciones que se pueden presentar en la práctica, produce la necesidad de analizar el caso concreto, superando quizás esta primera apreciación del tema.

Atento a ello se sostiene, que la temática tratada es discutible y podrá ser objeto de un estudio más pormenorizado en el futuro.

4. TIDP dentro del ámbito comunitario de la Unión Europea

El Convenio 108 proporcionó las directivas generales acerca de cuáles son las disposiciones aplicables al flujo transfronterizo de datos, siendo el primer instrumento normativo que recogió la temática que abordamos en el presente trabajo. De todas maneras, esta afirmación no tiene por motivo dar a entender que sus preceptos y principios no continúen siendo aplicables y siendo objeto de consideración.

Por su parte, la Directiva homogenizó la regulación de protección de datos personales y el sistema de las transferencias internacionales, otorgando un marco de referencia dotado de mayor practicidad, dando las pautas y orientaciones generales a los países integrantes de la Comunidad europea.

De un análisis de la Directiva, y a juicio del informante, cuando la transferencia se realiza entre Estados miembros de la Comunidad, o a un Estado integrante del Espacio Económico Europeo -Islandia, Liechtenstein y Noruega- no estamos en presencia de una TIDP.

Lo señalado anteriormente es atento a que cuando la Directiva habla de transferencias internacionales, siempre hace referencia a la transmisión de información de un Estado miembro de la Unión Europea o del Espacio Económico Europeo -en adelante EEE-, hacia un tercer Estado externo siendo éste externo al ámbito europeo[8].

---

[6] Ley Orgánica Española de Protección de Datos de Carácter Personal Nº 15/1999, de 13 de diciembre de 1999 -en adelante LOPD-.
[7] ORNELA NUÑEZ, Lina y MARTINEZ ROJAS, Edgardo. "Transferencias internacionales de datos personales: su protección en el ámbito del comercio internacional y la seguridad nacional". Biblioteca Jurídica del Instituto de Investigaciones Jurídicas de la UNAM, www.juridicas.unam.mx. Página visitada el 19 de mayo de 2010.
[8] Citamos por ejemplo el Considerando Nº 56, 57 y 59 de la Directiva y los artículos 25 y 26 del mismo cuerpo normativo.

En los supuestos mencionados, se trata de una comunicación simple de datos donde deberán cumplirse todos los requisitos establecidos tanto en la Directiva como en cada regulación de protección de datos existente en los distintos países.

Otro argumento que coadyuva con lo señalado, es que estamos ante un sistema comunitario, donde la libre circulación de datos personales es uno de los ejes básicos para el desarrollo del comercio interno entre los distintos Estados integrantes de dicha Comunidad, y este presupuesto no puede estar coartado ni a la solicitud de autorización especial para la transferencia ni sometida a la complejidad del régimen que las afecta.

4.1 Países con nivel Adecuado de Protección

Resulta muy difícil realizar un trabajo de TIDP sin hacer referencia acerca de qué se entiende por nivel adecuado de protección[9].

El artículo 29 de la Directiva creó el Grupo de protección de las personas en lo que respecta al tratamiento de los datos personales, más conocido con el nombre de G29.

El G29 posee carácter consultivo e independiente, y entre sus cometidos se encuentra el relativo al dictado de Dictámenes sobre el nivel adecuado de protección existente dentro de la Comunidad Europea y en terceros países[10].

A los efectos de realizar un correcto estudio, acerca de que se entiende por nivel adecuado de protección, el G29 toma como punto de partida el análisis de dos aspectos fundamentales[11]:

A) Núcleo de principios de contenido

[9] Al respecto es interesante destacar lo expresado por parte de la doctrina española. Adecuado significa un estándar mínimo de protección, en cambio equivalente establece un estándar que se evalúa en función del nivel de protección del Estado transmisor. DAVARA RODRIGUEZ, Miguel Ángel. Ob. Cit. Página 47.
El autor señalado agrega que el carácter de adecuado se refiere al nivel de protección no a la protección como tal. Un nivel de protección adecuado no prejuzga necesariamente la ausencia de protección equivalente. Cabe admitir que el concepto de nivel adecuado es más débil que el de protección equivalente. Ver HEREDERO HIGUERAS, M. "La Directiva Comunitaria de Protección de Datos de Carácter Personal". Aranzandi. Pamplona, 1997. Página 187.

[10] El Artículo 30 de la Directiva establece que: "El Grupo tendrá por cometido: a) estudiar toda cuestión relativa a la aplicación de las disposiciones nacionales tomadas para la aplicación de la presente Directiva con vistas a contribuir a su aplicación homogénea; b) emitir un dictamen destinado a la Comisión sobre el nivel de protección existente dentro de la Comunidad y en los países terceros…".

[11] Ver 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 U.E. Disponible en http://www.edps.europa.eu/EDPSWEB/edps/lang/en/Home/Consultation/OpinionsC.Página visitada el 22 de mayo de 2010.

a) Principio de limitación de objetivos: los datos deben tratarse con un objetivo específico y posteriormente utilizarse o transferirse únicamente en cuanto ello no es incompatible con el objetivo de la transferencia. Las excepciones a este principio las encontramos en la Directiva de la Unión Europea[12].

b) Principio de proporcionalidad y de calidad de los datos: los datos deben ser exactos y cuando sea necesario estar actualizados. Los datos deben ser pertinentes y no excesivos con relación al objetivo para el que se transfieren o para el que se tratan posteriormente.

c) *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 a lo expuesto, las encontramos en el art. 13 y 11.2 de la Directiva.

d) 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, incluido el Encargado del tratamiento, no debe tratar los datos salvo por instrucción del Responsable del tratamiento.

e) *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 inexactos.

f) Restricciones respecto a transferencias sucesivas a otros terceros países: únicamente debe 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 art. 26.1 de la Directiva.

B) Mecanismos de aplicación

Para poder evaluar el carácter adecuado de protección, el G29 afirma que es necesario distinguir los objetivos de un sistema normativo de protección de datos, y sobre esta base juzgar la variedad de diferentes mecanismos de procedimientos judiciales y no judiciales utilizados en terceros países.

Los objetivos de un sistema de protección de datos son básicamente tres:

a) *Ofrecer un nivel satisfactorio de cumplimiento:* que los Responsables conozcan muy bien sus obligaciones y los interesados conozcan muy bien sus

[12] La Directiva 95/46/CE en su art. 13 prevé las limitaciones y excepciones relativas al alcance de las obligaciones y los derechos previstos en ella. Entre estas limitaciones encontramos las relativas a: la seguridad del Estado, la defensa, la seguridad pública, la prevención, investigación, la detección y la represión de infracciones penales, ente otras.

derechos y medios para ejercerlos. La existencia de sanciones efectivas, disuasorias y sistemas de verificación directa por las autoridades.

b) *Ofrecer apoyo y asistencia a los interesados:* el interesado debe tener la posibilidad de hacer valer sus derechos con rapidez, eficacia y sin costes excesivos.

c) Ofrecer vías adecuadas de recurso a quienes resulten perjudicados: esto es, en caso de que no se observen las normas, obtener una resolución arbitral o judicial y en su caso, las indemnizaciones y sanciones correspondientes.

En síntesis, se deben cumplir los preceptos enunciados en el art. 25.2 de la Directiva, es decir, cumplimientos de las obligaciones de los responsables del tratamiento, un cuerpo normativo que contemple principios básicos de protección de datos personales, medios para su eficaz ejercicio, y la existencia de control de las autoridades de protección de datos personales.

Como vemos, a efectos de considerar si un país posee un nivel adecuado de protección se deberán observar criterios generales, esto es transferencias y categorías de transferencias y específicos concernientes al entorno jurídico existente en el Estado donde se encuentra situado el importador de los datos[13].

En base a lo establecido en la Directiva, la apreciación para evaluar la protección que brinda un país se toma en relación con elementos generales en función de las circunstancias, esto es transferencias y categorías de transferencias y elementos específicos entre los que se destacan: naturaleza de los datos, finalidad y duración del tratamiento, países de origen y países de destino final de las TIDP, normas de derechos generales o sectoriales vigentes, normas profesionales y medidas de seguridad.

Por otra parte, la Unidad Reguladora y de Control de Datos Personales (en adelante URCDP) con motivo de pronunciarse acerca de qué países cuentan con un nivel de protección adecuado, dispuso por Resolución Nº 17 de 12 de junio de 2009, seguir los lineamientos establecidos en la Directiva 95/46/CE y las Decisiones de la Comisión Europea resolviendo que: "*se consideran países apropiados para las transferencias internacionales, aquellos que a juicio de la Unidad cuenten con normas de protección de datos adecuadas y medios para asegurar su aplicación eficaz*"[14].

Como conclusión para la URCDP los países que brindan un nivel adecuado de protección son: los que a juicio de ésta cuenten con normas de protección de datos adecuadas y medios para asegurar su aplicación eficaz, los Estados miembros de la UE y aquellos que la Comisión Europea haya declarado su adecuación.

[13] Curso de la fundación CEDDET "La Protección de Datos Personales 1ª Edición" Módulo 5 Unidad 5.1 (Tratamientos Específicos).
[14] Resolución Nº 17/009 de 12 de junio de 2009 disponible en www.datospersonales.gub.uy. Página visitada el día 21 de mayo de 2010.

4.2. TIDP a países que no cuentan con un nivel adecuado de protección

A contrario sensu de lo expresado en el apartado referido al nivel adecuado de protección, los países que no cuentan con dicho nivel son aquellos que se encuentran físicamente fuera del ámbito del EEE y los que no han obtenido una resolución favorable de la Comisión de las Comunidades Europeas al respecto.

La redacción de la parte final del inciso 2 del artículo 23 de la LPDP, tomando como referencia lo preceptuado en la Directiva, permite que la URCDP pueda autorizar una o varias transferencias internacionales, mediante la existencia de cláusulas contractuales apropiadas u otro mecanismo que ofrezca iguales o mayores garantías. Dicha interpretación se desprende del vocablo "podrá" utilizado por la norma descripta[15]. Con respecto a la autorización de la que habla el artículo citado, se aprobó por dictamen Nº 8/2010 un procedimiento de autorización para la realización de TIDP.

A continuación se pasará al análisis de los aspectos fundamentales que posee este procedimiento de autorización y sus excepciones.

4.3. Procedimiento de solicitud de autorización

En muchos casos los terceros países carecen de una protección uniforme en todos los sectores económicos, o su legislación relativa a la protección de datos, se circunscribe solamente al ámbito público o ciertos sectores en particular.

Por lo tanto es necesario idear mecanismos uniformes tratando de abarcar todo el abanico posible de situaciones, sin traer consigo una demora injustificada del trámite en virtud de los intereses que se encuentran en juego.

El Consejo Ejecutivo de la URCDP por Dictamen Nº 8/010 de 19 de marzo de 2010 aprobó el procedimiento de autorización para la realización de transferencias internacionales a países que no cuenten con un nivel adecuado de protección -en virtud de los términos ya señalados-[16].

---

[15] El inciso 2 del art. 23 de la LPDP dispone: "…la Unidad Reguladora y de Control de Datos Personales, podrá autorizar una transferencia o una serie de transferencias de datos personales a un tercer país que no garantice un nivel adecuado de protección, cuando el responsable del tratamiento ofrezca garantías suficientes respecto a 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 derivar de cláusulas contractuales apropiadas".

[16] Por Considerando Nº VI se resolvió: "…el procedimiento de autorización se desarrollará según lo dispuesto por las normas de derecho administrativo vigentes y lo establecido en los artículos 34 y 35 del Decreto reglamentario. A tal efecto, el exportador de datos presentará la solicitud de autorización con la copia del contrato a celebrarse con el importador, acompañado de un formulario conteniendo información general que deberá ser vertida a la URCDP con el objeto de iniciar el trámite".

En esta línea cabe destacar que este procedimiento sólo opera cuando: el exportador de los datos no se encuentra acogido dentro de las excepciones establecidas en el artículo 23 de la LPDP y en las hipótesis donde el país de destino es considerado como un país que no posee un nivel adecuado de protección.

A) Cumplir con el procedimiento previsto para la inscripción de las Bases de Datos que se posean y obtener una resolución favorable de inscripción del Consejo Ejecutivo de la URCDP[17].

B) Realizar la solicitud de autorización de transferencias internacionales de acuerdo con el artículo 35 del Decreto Nº 414/009, la que deberá poseer el siguiente contenido:

a. identificación de la base de datos y su código de inscripción.

b. realización de una descripción de la transferencia, en donde se podrá informar las características generales de esta.

Atento a ello, se confeccionó un formulario destinado al exportador de los datos, para completar información genérica relacionada con las TIDP. A vía de ejemplo, descripción de las finalidad de la TIDP, tipos de datos, destinatarios, operaciones de tratamiento realizadas sobre la información, entre otras.

También, deberá indicar la finalidad que la justifica, adjuntando la documentación acreditante que entendiera correspondiente.

C) Se formará expediente en el cual recaerá informe jurídico analizando los presupuestos de hecho y de derecho. En éste, se controlará la documentación presentada con arreglo a las disposiciones mencionadas ut supra, aconsejándose o no la autorización.

En el caso de presentarse copia del contrato entre el exportador e importador de datos, además de proceder al control de la representación legal acreditada, se hará el análisis de las cláusulas contenidas en este, pudiendo tomarse como referencia las Decisiones de la Comisión de las Comunidades Europeas relativas a la aprobación de un conjunto de Cláusulas Contractuales Tipo para la realización de TIDP a terceros Estados.

D) En el caso de verificarse observaciones se le dará vista al interesado, el que deberá evacuarlas en el plazo de 10 días hábiles.

E) Una vez levantadas las observaciones o en caso de no constatarse la existencia de estas, se elevará al Consejo Ejecutivo de la URCDP el que, atendiendo a las circunstancias del caso y tomando en cuenta los parámetros internacionales enunciados en el numeral anterior y otras consideraciones que

[17] Ver artículos 28 y 29 de la LPDP y artículos 15 y 16 del Decreto Nº 414/009.

estimare pertinentes, resolverá acerca de si autoriza o no la realización de las transferencias planteadas.

En caso de recaer resolución favorable, se inscribirá la autorización de las transferencias solicitadas en el registro que a tal efecto lleva la URCDP-literal D) del art. 15 del Decreto 414/009-.

F) Finalmente, se notificará de la resolución al exportador de datos personales y posteriormente se publicará.

Es dable destacar que si bien no surge obligatoria la presentación de cláusulas contractuales a efectos de obtener la mencionada autorización, parece ser este el mecanismos o la práctica más generalizada en la actualidad, permitiendo en este caso a la URCDP determinar las características esenciales de las transferencias que se procuren realizar.

Por último podemos decir que dentro de la potestad de autorizar una o una serie de transferencias, se encuentra implícita la de denegar o suspender las mismas.

Al respecto, el Dictamen ya reseñado expresa: “que la URCDP podrá denegar una autorización de transferencia internacional de datos personales a un país que no proporcione un nivel adecuado de protección cuando “*el responsable del tratamiento no ofrezca garantías suficientes respecto a la protección de la vida privada, de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los respectivos derechos”,* o si se constatare un incumplimiento de las disposiciones establecidas en la LPDP y su Decreto reglamentario.

Para finalizar es de recibo señalar, que el procedimiento de autorización, deberá tener como meta a lograr un adecuado balance entre los legítimos intereses empresariales, que se puedan ver perjudicados por la demora en la tramitación de la autorización y el resguardo de los derechos de los titulares de los datos personales contenidos en la normativa nacional vigente.

4.4. Excepciones a la solicitud de autorización

Tanto a nivel internacional como nacional la normativa de protección de datos, permite la ejecución de TIDP, a países que no cuentan con un nivel de protección adecuado, siempre y cuando resulten comprendidos dentro de las excepciones establecidas a texto expreso.

Sin la intención de realizar un análisis profundo de todas las excepciones dispuestas por el artículo 23 de la LPDP, se detendrá el análisis en dos de ellas ya que son las más frecuentes: a) el previo consentimiento del titular de los datos para la transferencia prevista y b) las relativas a la ejecución de un contrato entre el interesado y el responsable del tratamiento o la ejecución de un contrato en interés del interesado.

a) Consentimiento del titular de los datos a la transferencia prevista[18]

El carácter de inequívoco dado por la norma significa que no haya lugar a duda que se ha brindado el consentimiento para realizar la transferencia, en caso contrario, ese consentimiento no será válido.

Este carácter del consentimiento mencionado, deberá ser sumado a los caracteres establecidos en el artículo 9 de la LPDP. Estos son: que sea libre (sin ser objeto de coacción alguna), previo (a la transferencia prevista), expreso (específico para esa situación) e informado, esto es que el titular de los datos personales conozca la finalidad para la cual sus datos serán transferidos y el riesgo que involucra dicha situación.

En este sentido, cabe destacar que las empresas interesadas en la ejecución de TIDP a países que no cuentan con un nivel adecuado de protección suelen optar por este mecanismo a efectos de no realizar el trámite de solicitud de autorización.

Al respecto, el consentimiento deberá recabarse y documentarse de acuerdo con lo establecido en el artículo 9 de la LPDP y el artículo 6 del Decreto reglamentario ya mencionado.

Siguiendo la línea sostenida por el G29 decimos que en los casos de transferencias relativas a operaciones de crédito y, siguiendo la tendencia internacional al respecto, podría recabarse el consentimiento previamente a la realización de estas sin necesidad de solicitar autorización en cada oportunidad que se pretendan transferir los datos con destino internacional. Lo mencionado no obsta que en el caso de tratarse de una TIDP de Responsable del tratamiento a Responsable se cumpla con los preceptos en materia de comunicación o cesión de datos[19].

b) excepciones relativas a la ejecución de un contrato[20]

Siguiendo los criterios dictaminados por el G29 se debe tener presente que estas excepciones poseen un carácter amplio, por lo que no sólo deberán ser

[18] El numeral A) del art. 23 de la LPDP establece: “que el interesado haya dado su consentimiento inequívocamente a la transferencia prevista.

[19] El Dictamen aprobado por el Consejo Ejecutivo de la URCDP ya mencionado refiriéndose a un caso en particular y siguiendo para ello los criterios contenidos en el informe del G29, estableció que: “en virtud de la calidad de los datos tratados por AA, se podrá recabar previamente el consentimiento de los titulares de los datos personales, consentimiento que deberá ser guardado con arreglo a lo dispuesto en el art. 6 del Decreto reglamentario. En caso de operaciones de crédito, que se caracterizan por ser de tipo repetitivas y similares, siempre y cuando no se cambie la finalidad del tratamiento, recoger de forma previa el consentimiento aparece como una alternativa viable a efectos de no requerir la autorización correspondiente.

[20] El numeral B) y C) del art. 23 de la LPDP disponen: “que la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales tomadas a petición del interesado; y que la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar en interés del interesado, entre el responsable del tratamiento y un tercero…”

de aplicación estricta sino que se deberá tomar en consideración los siguientes criterios.

Todos los datos transferidos deben ser solamente los necesarios para la ejecución del contrato, en aplicación de los principios sustanciales en materia de protección de datos –en especial, el principio de finalidad y veracidad de los datos.

La excepción solo operará en los casos que la iniciativa contractual a efectos provenga del interesado, a petición del interesado como así lo establece la Ley. A vía de ejemplo, la solicitud que un titular inicia con el motivo de reservar un billete de avión[21].

Asimismo y a título personal se considera, que en estos casos el interesado no posee solo un interés simple-numeral C) del artículo 23 de la LPDP-, sino que se interpreta que la norma se atiene al concepto de tercero beneficiario manejado por la doctrina internacional y recogido en las Decisiones que establecen las cláusulas contractuales tipo. Esto significa que el interesado o titular de los datos sea parte beneficiaria de ese contrato evitando que el mero interés simple transforme en operativa la excepción.

5. Cláusulas Contractuales Tipo

El artículo 26.2 de la Directiva dispone: *"(...) los Estados miembros podrán autorizar una transferencia o una serie de transferencias de datos personales a un tercer país que no garantice un nivel de protección adecuado con arreglo al apartado del art. 25, cuando el responsable del tratamiento ofrezca garantías suficientes respecto de la protección de la vida privada, de los derechos y libertades fundamentales de las personas, así como respecto de los respectivos derechos; dichas garantías podrán derivarse, en particular, de cláusulas contractuales apropiadas.*

Se considera que las cláusulas contractuales tipo (en adelante CCT), son mecanismos contractuales destinados a ofrecer las garantías adecuadas para la protección de la vida privada, los derechos fundamentales y el respeto en el ejercicio de los derechos de los titulares. Es decir que la inclusión de estas cláusulas en un contrato entre el exportador e importador de los datos, están solamente relacionadas con la protección de los datos y ellos tienen la autonomía suficiente para redactar e incluir otras a su arbitrio[22].

[21] El Dictamen del G29 se refiere a este aspecto como la "prueba de necesidad".
[22] Sin embargo, en los casos que se aparten de las cláusulas aprobadas por la Comisión Europea la Autoridad de control tendrá plena libertad para determinar si éstas son suficientes.

Por mandato del apartado 4 del artículo 26 de la Directiva, la Comisión tiene competencia para aprobar ciertos conjuntos de CCT que ofrezcan garantías suficientes[23].
Asimismo, las CCT son uno de los posibles mecanismos a adoptar para ofrecer las garantías necesarias de protección.

La LPDP uruguaya permite la adopción por parte del exportador e importador de datos, una serie de CCT que tengan como finalidad obtener la autorización de la URCDP sometiéndolas a su consideración[24].

Las Decisiones ya mencionadas contienen distintos cuerpos de cláusulas contractuales destinadas a las transferencias de Responsable del tratamiento a Responsable (Decisión 2004/915/CE) y aquellas relativas a las transferencias de Responsable a Encargado de tratamiento (Decisión 2010/87/CE que deroga la Decisión 2002/16/CE).

Al respecto, encontramos un estudio acerca de un modelo tipo de contrato para garantizar un nivel equivalente de protección. Dicho documento, se elaboró ante el consejo de Europa, la Cámara de Comercio Internacional y la Comisión Europea[25].

En palabras del propio G29, en el contexto de las transferencias internacionales a terceros países, el contrato es un medio que permite al responsable del tratamiento ofrecer garantías adecuadas al trasmitir datos fuera de la Comunidad Europea, a un país donde el nivel de protección no sea suficiente.

Para que una cláusula contractual pueda cumplir esta función, debe compensar de manera satisfactoria la ausencia de una protección adecuada mediante la inclusión de los elementos esenciales de la misma, que no existen en una situación determinada.

Las consideraciones a las que se refiere el grupo señalado, son en base a los mismos criterios posibles para determinar el nivel adecuado de protección ya mencionados en el presente trabajo, por lo que a continuación nos

[23] El apartado 4 del artículo 26 de la Directiva dispone: "cuando la comisión decida, según el procedimiento establecido en el apartado 2 del artículo 31, que determinadas cláusulas contractuales tipo ofrecen garantías suficientes establecidas en el apartado 2, los Estados miembros adoptarán las medidas necesarias para ajustarse a la decisión de la Comisión.
[24] El inciso 2 del artículo 23 de la LPDP establece que: " sin perjuicio de lo dispuesto en el primer inciso de este artículo, la Unidad Reguladora y de Control de Datos Personales podrá autorizar una transferencia o una serie de transferencias a un país que no garantice un nivel adecuado de protección, cuando el responsable del tratamiento ofrezca garantías suficientes respecto a 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 de cláusulas contractuales apropiadas", subrayado nuestro.
[25] "Model Contract to ensure equivalent data protection in the context of transborder data flows, with explanatory memorandum". Estrasburgo, 2 de noviembre de 1992.

detendremos en señalar cuáles son las principales cláusulas que contienen las Decisiones de la Comisión Europea al respecto.

Es interesante destacar que es posible que las partes diseñen a su arbitrio las cláusulas contractuales y la sometan a autorización de la autoridad de control de que se trate.

Ahora bien y siempre estando dentro del ámbito europeo, si las partes someten sus cláusulas con arreglo a lo establecido en las Decisiones reseñadas, garantizan la concesión de autorización así como también el ahorro de costes y tiempo. También existe la posibilidad que las partes opten por los modelos contractuales aprobados por la autoridad nacional de protección[26].

5.1. Decisión 2004/915/CE de 27 de diciembre de 2004

Con respecto a las TIDP realizadas de Responsable del tratamiento a Responsable cabe destacar, que la presente Decisión 2004/915/CE de 27 de diciembre de 2004 vino a modificar la Decisión 2001/497/CE de 15 de junio de 2001, introduciendo un conjunto alternativo de cláusulas contractuales tipo para la TIDP a terceros países.

Esta Decisión tiene como característica fundamental la de incluir un nuevo anexo de cláusulas contractuales, donde las partes pueden optar por uno u otro conjunto –u optar por otro fundamento jurídico- sin la posibilidad de combinarlos, ya que es considerado como un todo jurídico.

En este sentido y dentro de las modificaciones efectuadas interesa en primer lugar la referida al régimen de responsabilidad [27]

a) Responsabilidad: esta Decisión adopta como alternativa al sistema de responsabilidad solidaria –acogida por la Decisión 2001/497/CE-, un régimen de responsabilidad basado en la obligación de diligencia debida, en virtud de la cual el exportador y el importador de datos responderían ante los interesados por el incumplimiento de sus obligaciones contractuales respectivas.

[26] SANCHO VILLA, Diana. “Protección de Datos Personales y Transferencia Internacional: cuestiones de ley aplicable. Revista Jurídica de Castilla y León Nº 16. Septiembre de 2006. Página 433 y 434.

[27] En la decisión 2001/497/CE en su considerando 18 se dispone: “con objeto de reducir las dificultades prácticas que pudieran experimentar los interesados al intentar exigir el respeto de sus derechos a tenor de estas cláusulas contractuales tipo, el exportador de datos y el importador de datos se considerarán responsables solidarios de los daños y perjuicios resultantes de un incumplimiento de las estipulaciones sujetas a la cláusula de tercer beneficiario”.https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/union_europea/decisiones/common/pdfs/l_18120010704es00190031.pdf. página visitada el 21 de mayo de 2010.

El exportador es así mismo responsable, sino realiza esfuerzos razonables para determinar si el importador es capaz de cumplir las obligaciones jurídicas que le incumben, en virtud de las cláusulas pactadas (culpa in eligendo).

b) Suspensión de transferencias: otra de las cuestiones a destacar, es que la nueva Decisión otorga mayor flexibilidad a las autoridades de protección de datos para la suspensión de transferencias internacionales cuando "el exportador de datos rehúse tomar medidas apropiadas contra el importador de datos para hacerle cumplir las obligaciones contractuales o este último se niegue a cooperar de buena fe con las autoridades de control competentes en materia de protección de datos".

c) Obligaciones del exportador:

- realizar esfuerzos razonables para determinar si el importador de datos es capaz de cumplir las obligaciones jurídicas que le incumben, en virtud de las presentes cláusulas;

- responderá en un tiempo razonable, a las consultas de los interesados y de la autoridad, relativas al tratamiento de datos personales por parte del importador de datos;

- "pondrá a disposición de los interesados, que son terceros beneficiarios a tenor de la cláusula III, y a petición de éstos, una copia de las cláusulas…"

d) Obligaciones del importador:

- poner en práctica las medidas técnicas y organizativas que resulten necesarias para proteger los datos personales contra su destrucción accidental o ilícita, su pérdida o alteración accidental o su divulgación o acceso no autorizados.

- tratará los datos personales para los fines objeto de la transferencia y tiene autoridad legal para ofrecer garantías y cumplir los compromisos previstos en las cláusulas.

- no tiene motivos para creer, en el momento de suscribir las presentes cláusulas, en la existencia de ninguna disposición legal de ámbito local que pueda tener un efecto negativo importante sobre las garantías estipuladas en las cláusulas e informará al exportador de datos -el cual, cuando así se le pida, transmitirá dicha notificación a la autoridad- si tuviera conocimiento de la existencia de alguna disposición de esta índole.

e) Resolución de conflictos: en caso de conflicto o de reclamación interpuesta contra una o ambas partes por un interesado o por la autoridad de control, la una informará a la otra sobre esta circunstancia y ambas cooperarán con el objeto de alcanzar una solución amistosa lo antes posible.

Las partes acuerdan así mismo, estudiar la posibilidad de participar en cualquier otro mecanismo de arbitraje, mediación u otra índole y acatar cualquier decisión de los tribunales competentes o de la autoridad del país de establecimiento del exportador de datos, cuyas decisiones sean finales y contra las que no pueda entablarse recurso alguno.

En síntesis, decimos que las CCT en general contienen –además de las ya enunciadas- otros grupos de cláusulas que se señalan a continuación:
- aquellas relativas a brindar definiciones contenidas en la Directiva;

- las relativas a los terceros beneficiarios[28];

- las que establecen mecanismos de mediación y arbitraje en casos de conflictos entre las partes y el interesado[29];

- las que se corresponden con la cooperación entre las autoridades de control[30];

- las que establezcan que la resolución del contrato por cualquier circunstancia no eximirá a las partes del cumplimiento de las obligaciones y condiciones estipuladas en lo que respecta al tratamiento de los datos transferidos;

- las relacionadas con las medidas de seguridad técnicas y organizativas a adoptar;

- las que definen los detalles de las transferencias –actividades de las partes, finalidad de las TIDP, categorías de los datos, destinatarios de la información, operaciones de tratamiento, etc.

-y aquellas que establecen obligaciones una vez finalizada la relación contractual, como por ejemplo la devolución al Responsable o destrucción de la información objeto de tratamiento.

5.3. Decisión 2010/87/CE de 5 de febrero de 2010[31].

Con fecha 12 de febrero de 2010 se ha publicado la presente decisión relativa a las CCT para la transferencia de datos personales a los encargados de tratamiento establecidos en terceros países, introduciendo la posibilidad de

[28] Son aquellas por las que las cláusulas son también exigibles por el interesado, en particular cuando estos sufran un daño. Curso CEDDET. Ob. Cit. Módulo 3. Página 88.
[29] Estos mecanismos operan si los conflictos no son resueltos de forma amistosa siempre y cuando el interesado invoque la cláusula de tercero beneficiario las partes deberán ofrecer al interesado la elección entre mediación, arbitraje o procedimiento judicial. Ob. Cit. Curso CEDDET. Módulo 3. página 88
[30] Interesa señalar que el Principio de Cooperación Internacional acogido internacionalmente es un pilar fundamental a efectos de que las autoridades de control desempeñen un papel clave en el mecanismo contractual.
[31] http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:ES:PDF. Página visitada el 21 de mayo de 2010.

realizar un subtratamiento de los datos por parte de encargados del tratamiento establecidos también en terceros países[32].
La presente tiene aplicación a partir del 15 de mayo de 2010 derogando la Decisión 2002/16/CE de 20 de febrero de 2002.

Su motivación radicó en la acumulación de experiencia en la aplicación de la Decisión derogada, en virtud del crecimiento considerable de TIDP a países que no cuentan con un nivel adecuado de protección, y la actualización de la Decisión 2002/16/CE donde el fenómeno del subtratamiento no había sido contemplado.

En virtud de la reciente aprobación del instrumento descrito se dedicará especial atención, al ámbito subjetivo de aplicación, al concepto de subtratamiento y subencargado de tratamiento y algunas cláusulas que revisten particular interés.

a) Ámbito subjetivo de aplicación:

La presente Decisión se aplica sólo en los casos donde un encargado de tratamiento -importador- situado en un tercer país, contrata la prestación de un servicio de subtratamiento de la información a un subencargado del tratamiento situado en otro tercer país, en virtud de una TIDP realizada por el importador de los datos -encargado de tratamiento- al subencargado del tratamiento.

En otras palabras, se aplicará a la subcontratación realizada por un Encargado de tratamiento establecido en un tercer país de sus servicios de tratamiento a un subencargado establecido en otro tercer país.

No se aplicará a los casos donde la TIDP sea de Responsable del tratamiento a Responsable[33] -aplicándose la Decisión 2004/915/CE- y tampoco se aplicará en los casos que un encargado de tratamiento establecido en la UE y que realice el tratamiento de datos en nombre del Responsable de tratamiento situado en la UE, subcontrate sus operaciones de tratamiento a un subencargado del tratamiento establecido en un tercer país[34].

---

[32] Al respecto la Decisión 2010/87/CE en su apartado 18 establece: “La presente Decisión debe contener cláusulas contractuales tipo específicas sobre el subtratamiento por un encargado del tratamiento de datos establecido en un tercer país (el importador de datos) de sus servicios de tratamiento a otros encargados (subencargados del tratamiento de datos) establecidos en terceros países. Además, la presente Decisión debe establecer las condiciones que ha de cumplir el subtratamiento para garantizar que los datos personales que se están transfiriendo sigan protegidos con independencia de la sucesiva transferencia a un subencargado del tratamiento.

[33] Es dable destacar que la Decisión 2002/16/CE -derogada por la 2010/87/CE- se aplicaba a las TIDP de Responsable del tratamiento a Encargado. Por lo que la actual Decisión si bien la deroga no modifica su estructura básica de aplicación.

[34] Apartado 23 de la Decisión 2010/87/CE.

Por lo que desde el punto de vista de los sujetos involucrados, el esquema es el siguiente:

- un exportador de los datos situado en la UE, que realiza una transferencia internacional a un Encargado de tratamiento –importador- situado en un tercer país que no cuente con un nivel adecuado de protección.

- un importador de los datos que subcontrata los servicios de otro encargado de tratamiento, o subencargado, situado en un tercer país

- un subencargado de tratamiento que presta servicios acordados entre el Responsable del tratamiento y el Encargado.

B) Definiciones

a) Subencargado de tratamiento: cualquier encargado del tratamiento contratado por el importador de datos o por cualquier otro subencargado de este que convenga en recibir del importador de datos, o de cualquier otro subencargado de este, datos personales exclusivamente para las posteriores actividades de tratamiento que se hayan de llevar a cabo en nombre del exportador de datos, de conformidad con sus instrucciones, las cláusulas contractuales tipo establecidas en el anexo y los términos del contrato que se haya concluido por escrito para el subtratamiento- literal e) del artículo 4 de la Decisión 2010/87/CE-.

b) el subtratamiento consistirá exclusivamente en las operaciones acordadas en el contrato entre el exportador de datos y el importador de datos y no se referirá a operaciones de tratamiento o finalidades diferentes. En el caso que el subencargado de tratamiento no cumpla con sus obligaciones, el importador de datos seguirá siendo responsable frente al exportador de datos.

C) Otras cláusulas que revisten interés

A continuación se destacan algunas cláusulas referidas exclusivamente al subtratamiento de los datos, ya que las restantes son a prima facie similares a las reguladas por las Decisiones ya enunciadas.

a) Obligaciones del exportador de datos:

-como principal novedad se encuentra la dispuesta en el literal i) del Decisión, que establece que este garantizará que el subencargado proporcionará por lo menos el mismo nivel de protección de los datos personales y los derechos de los interesados que el importador de datos en virtud de las presentes cláusulas.

-el exportador de datos conservará la lista de los acuerdos de subtratamiento celebrados con arreglo a las cláusulas y notificados por el importador de datos de conformidad con la letra j) de la cláusula 5, lista que se actualizará al menos

una vez al año. La lista estará a disposición de la autoridad de control de protección de datos del exportador de datos.

b) Obligaciones del importador:

- el importador de datos no subcontratará ninguna de sus operaciones de procesamiento llevadas a cabo en nombre del exportador de datos con arreglo a las cláusulas sin previo consentimiento por escrito del exportador de datos;
- enviará sin demora al exportador de datos una copia de cualquier acuerdo con el subencargado del tratamiento que concluya con arreglo a las cláusulas;

- si el importador de datos subcontrata sus obligaciones con arreglo a las cláusulas, con el consentimiento del exportador de datos, lo hará exclusivamente mediante un acuerdo escrito con el subencargado del tratamiento de datos, en el que se le impongan a este las mismas obligaciones impuestas al importador de datos con arreglo a las cláusulas.

Es relevante destacar que por informe jurídico de la Agencia Española de Protección de Datos -AEPD- se sostiene la posibilidad de la subcontratación de servicios en supuestos de TIDP, basados en el artículo 21 de la LOPD[35].

En este sentido el mecanismo encontrado para permitir que se transfieran datos a un subencargado de tratamiento y a sucesivos sub - subencargados de tratamiento, fue la de poner al Responsable del tratamiento como parte de la relación jurídica, no alcanzando para ello su mera referencia en el contrato.

Es decir, que para ello deberán existir dos contratos, uno celebrado entre el Responsable y le Encargado de tratamiento y otro contrato celebrado entre el Encargado –actuando en nombre del Responsable- con el subencargado de tratamiento –contratos basados en la Decisión 2010/87/CE-.

Asimismo, el subencargado deberá adherirse a las cláusulas concertadas entre el Responsable y el Encargado de tratamiento mediante un instrumento específico firmado por las tres partes, comprometiéndose específicamente el cumplimiento de las cláusulas contenidas en la Decisión estudiada[36].

A modo de cierre del presente apartado, resulta interesante destacar lo resuelto por la URCDP al respecto.

Por Dictamen Nº 8/010 se estableció: “Que con motivo de realizar transferencias a Estados u Organismos que no cuentan con un nivel adecuado de protección, las cláusulas contractuales tipo, (art. 23 infine de la LPDP), aparecen como la práctica más generalizada en pro de alcanzar la debida autorización.”.

[35]Informe Jurídico Nº 0108/2008 de la AEPD. Disponible en https://www.agpd.es/portalwebAGPD/noticias-inicio/Informes_Destacados_16_03_2010_1-ides-idrss.xml
[36] Curso CEDDET. Ob. Cit. Página 97.

6. Reglas Corporativas Vinculantes

Si bien su denominación natural es “Binding Corporate Rules”, su traducción literal corresponde tal lo expresado en el título del presente apartado, por lo que en adelante nos referimos a estas como BCR.

Las BCR surgen en virtud de las propias características funcionales de un grupo de empresas multinacionales, con el objeto de contar con reglas uniformes que regulen la TIDP a distintos países, y con la finalidad de que no tengan que recurrir a mecanismos contractuales *inter partes* entre todos los integrantes del grupo.

Las CCT son uno de los mecanismos existentes que otorgan garantías suficientes para la protección de la vida privada, por lo tanto las BCR aparecen como otras de las alternativas posibles en pro de la salvaguarda de los derechos de los titulares de los datos, en especial los riesgos que la libre circulación de éstos les ocasione[37].

6.1. Concepto

Si bien la normativa de protección de datos relevada no contiene una definición de las BCR, el G29 ha venido trabajando al respecto, dictando varios documentos de trabajo[38].

El G29 los define como: “un cuerpo de reglas o normas vinculantes adoptadas en el seno de un grupo de empresas que operan a nivel internacional, para regir las transferencias de datos que se producen desde las sedes del grupo establecidas en el EEE hacia otras sedes del grupo establecidas en terceros Estados”.

En opinión de la doctrina internacional, las BCR cumplen una función facilitadota del tráfico privado de datos, basada en la autonomía y especialmente adaptada a las estructuras corporativas internacionales[39].

Las estructuras empresariales pueden tener muchas alternativas, teniendo al efecto las clásicas estructuras verticales u horizontales, y aquellas estructuras que atienen a un criterio organizacional de la empresa, tales como la estructura funcional, matricial, proyectizada, entre otras.

---

[37] Ver el apartado 2 del artículo 26 de la Directiva, artículo 33 de la Ley Orgánica Española -LOPD- y el inciso segundo del artículo 23 de la LPDP.

[38] WP 108 de 14 de abril de 2005; WP 107 de 14 de abril de 2005; WP 74 de 3 de junio de 2003; WP 102 de 25 de noviembre de 2004; WP 107 de 14 de abril de 2005; ; WP 108 de 14 de abril de 2005; WP 133 de 10 de enero de 2007. Disponibles en www.europa.eu.int/comm/privacy. Página visitada el 20 de mayo de 2010.

[39] SANCHO VILLA, Diana. “Reglas corporativas vinculantes (Binding Corporate Rules)…”. Ob. Cit. Página 44.

De una primera apreciación de la temática abordada a título personal se expresa, que las BCR son Códigos de Conducta que contienen un conjunto de reglas adaptadas específicamente para facilitar la realización de TIDP dentro de un grupo de empresas multinacionales, de acuerdo con su fisonomía y estructura.[40].

6.2. Ámbito de aplicación

Desde una visión europea el ámbito de aplicación de las BCR es el siguiente.

Recordemos que las BCR son uno de los mecanismos que existen en la actualidad para poder efectuar TIDP a países que no cuentan con un nivel adecuado de protección.

- Partes de los empresarios del grupo establecidos en el EEE exportan los datos a otros empresarios que se encuentran establecidos en terceros países que no cuentan con un nivel adecuado de protección.

- Las BCR solo se aplican dentro del grupo a los datos personales recabados dentro del EEE.

- El responsable de los datos viene dado por sus operaciones sobre los datos y no por su forma jurídica –filial, sucursal, etc.-.

Por lo tanto las BCR no se aplican cuando: todos las empresas se encuentran dentro del EEE, cuando estas operan como importadores de datos y tampoco cuando las empresas situadas en los Estados miembros transfieran datos a empresas situadas en países que han obtenido una declaración de nivel adecuado.

En el primer y segundo caso no estamos ante una TIDP propiamente dicha –desde la perspectiva europea- y en el restante no es necesario el sometimiento de este tipo de mecanismos -CCT o BCR- en virtud de que la transferencia no necesita ser sometida a ninguna autorización de las autoridades europeas de protección de datos personales.

Por otra parte, cabe destacar que, hasta la aprobación del WP 133 el G29 se ha basado para sus consideraciones, en aquellas estructuras empresarias de corte vertical o jerárquico.

6.3. Cuestiones generales del procedimiento de autorización

El G29 ha ideado un procedimiento de autorización de las BCR de cooperación y comunicación de oficio entre las autoridades de protección de datos[41].

[40] Ver SANCHO VILLA, Diana. “Reglas Corporativas vinculantes (Binding Corporate Rules)…” Ob. Cit. Página 45. Ver Curso CEDDET. Ob. Cit. Página 101.
[41] Recomendación 1/2007 de 10 de enero de 2007. WP 133.

Este procedimiento es de corte voluntario, de cooperación, coordinado por una autoridad líder y teniendo como fundamento evitar que las empresas soliciten la autorización de las BCR ante las autoridades que se consideren más flexible.

El G29 también propone la adopción de reglas de procedimiento que permitan a las compañías, seguir un único proceso de legitimación ante la autoridad de protección de datos de un Estado miembro, que gestionará el otorgamiento de autorizaciones con las distintas autoridades de los Estados miembros donde el grupo opera.

Un aspecto relevante a destacar, es que las BCR deben ser vinculantes legalmente dentro y fuera del grupo.

Desde el punto de vista de la obligatoriedad interna, las reglas que se adoptan con respecto a las TIDP deberán ser cumplidas por todas las partes integrantes del grupo.

Es recomendable que los empleados que realicen tratamiento de datos personales reciban capacitación al respecto. Asimismo, este tipo de reglas a cumplir pueden estar recogidas en otros Códigos de Conducta perteneciente al grupo de empresas que coadyuven al fortalecimiento del cumplimiento de la normativa de protección de datos personales. A vía de ejemplo, aquellos que contengan normas relativas a las medidas de seguridad para la protección de datos, deber de confidencialidad, etc.

Ateniéndose a la obligatoriedad externa, se sostiene a nivel doctrinario que la carga de la prueba, será del miembro del grupo a quien se imputa la comisión de un tratamiento ilícito, el que deberá probar que no es responsable del mismo.

Asimismo, se sostiene que los interesados -al igual que en las CCT- deben ostentar la calidad de terceros beneficiarios para lo cual las oficinas centrales del grupo o la sociedad europea responsable en materia de protección de datos, deberán asumir las posibles responsabilidades del grupo derivadas de tratamientos ilícitos de los datos. Al respecto, se debería informar al interesado cuál es la oficina donde debe ejercer sus derechos o realizar alguna denuncia en el tratamiento de sus datos.

Parte de la doctrina sostiene que el interesado tiene la opción de presentar una reclamación ante: el miembro del grupo de origen de la transferencia, la sede de dirección del grupo o ante el delegado en el EEE, cuando aquella sede está en un tercer Estado. Esto vendría a ser una cláusula de elección del foro a favor del tercero beneficiario[42].

[42] SANCHO VILLA, Diana. “Reglas corporativas vinculantes (Binding Corporate Rules)…”. Ob. Cit. Página 57.

Al igual que en las CCT, las BCR deberá especificar, la naturaleza de los datos, la finalidad de las transferencias, sometimiento a los principios de protección de datos[43].

En síntesis, y de una primera visión de las BCR, el sistema analizado aparece quizás dotado de una mayor complejidad que el sistema de las CCT, siendo en las dos, el rol de las autoridades de control fundamental para su ejecución[44].
Pero sin embargo para lograr un sistema integrado para la aprobación de las BCR, se debe respetar estrictamente el principio de cooperación internacional, en virtud de las diferencias estructurales, de procedimiento y hasta de interpretación que las autoridades de control poseen.

Asimismo, nunca se debe perder de vista que en la mayoría de los casos es el interesado el principal y primer afectado por el tratamiento ilícito de la información que le concierne, por lo que al igual que concluimos al hablar de las CCT, el procedimiento que se lleve a cabo debe contemplar los intereses en juego y si es necesario ser objeto de revisión continua que contemple los nuevos desafíos que el mundo globalizado nos presenta.

7. Conclusiones

Como apartado final del presente trabajo, se brindarán algunas apreciaciones y reflexiones personales de la temática objeto de estudio.

Para comenzar, se adhiere a la tesis que considera a las transferencias internacionales como de naturaleza compleja y transversal.

Es así que las TIDP, no solo guardan relación con numerosos aspectos recogidos en otros cuerpos normativos, sino también su naturaleza transversal se refleja en la propia normativa de protección de datos, rozando prácticamente todos sus aspectos.

Como hiciéramos referencia al comenzar este trabajo, la Sociedad de la Información a la que asistimos, conlleva la utilización y transmisión de grandes cantidades de información de forma masiva y automatizada. Las nuevas formas de relacionamiento social y comercial que trajo consigo Internet, plantean desafíos continuos al derecho que hacen que el trabajo conjunto de las

[43] Curso CEDDET. Ob. Cit. Página 99 y 100.

[44] En cuanto a la situación uruguaya corresponde señalar el ya citado Dictamen 8/010 por el cual la URCDP estableció que:"…en los casos en que se trate de transferencias internacionales de datos en el ámbito de empresas multinacionales (art. 35 inc. 2 Decreto reglamentario), los códigos de conducta a inscribirse, además de cumplir con los requisitos de forma exigidos, deberán ofrecer *"...garantías suficientes respecto a la protección de la vida privada, de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los respectivos derechos".* Es decir, que se exigirán los mismos requisitos establecidos para realizar las transferencias internacionales de datos".

autoridades de control de protección de datos, se vuelva cada vez más un hito fundamental en este ámbito.

Es en este marco donde la normativa relacionada con la protección de los datos, debe tener un papel protagónico y como meta a lograr la salvaguarda de los derechos de los titulares que se ven perjudicados por el intercambio automatizado de su información personal, sin perder de vista la importancia de otros derechos que pueden estar en juego.

Asimismo, la necesidad del cumplimiento del principio de cooperación internacional -recogido por numerosos instrumentos normativos internacionales-, radica en que el régimen jurídico de las TIDP implica la participación de varios países que poseen regulaciones y concepciones distintas en relación con la protección de datos personales.

Si bien la normativa uruguaya de protección de datos personales vigente tomó como inspiración los parámetros internacionales de mayor recibo en la materia, no es posible, atento a la complejidad del régimen jurídico de las TIDP, realizar una pura extrapolación de la normativa comunitaria a nuestro sistema normativo.

En este sentido, Uruguay se encuentra inserto en el camino hacia la adecuación de sus normas y aparato jurídico, a los estándares internacionales en la materia. Para lograr dicho objetivo, no sólo alcanza con sancionar normativa relacionada a la protección de datos personales, sino que el sistema jurídico se acompase paulatinamente con los derechos que emergen de la naturaleza de dichas normas.

No obstante ello, se considera que la LPDP cuenta con un rico marco normativo que contempla numerosos principios de contenido y mecanismos de aplicación recomendados por los expertos en la materia.

Continuando con esta línea de razonamiento, la Unidad Reguladora y de Control de Datos Personales ha venido trabajando fundamentalmente en la difusión, capacitación, concientización y asesoramiento a los titulares acerca de los derechos relativos a la protección de los datos personales, teniendo oportunidad de pronunciarse acerca de que países se consideran que proporcionan un nivel adecuado de protección y dictaminando al respecto del régimen jurídico de las TIDP en la LPDP y su Decreto reglamentario Nº 414/009[45].

En este sentido las potestades conferidas por la LPDP al Órgano de Control, son similares a las concedidas a las autoridades de control de otros países, las cuales -entre otras- apuntan al cumplimiento de las tareas expuestas

[45] Ver Resolución Nº 17/009 de 12 de junio de 2009 y Dictamen Nº 8/010 de 19 de marzo de 2010. Disponibles en http://www.datospersonales.gub.uy/sitio/documentos-resoluciones.aspx. Página visitada el 22 de mayo de 2010.

precedentemente, teniendo como objetivo principal la tutela de un derecho humando reconocido por la normativa vigente en nuestro país.

Montevideo, 23 de mayo de 2010.