07.2023

HACIA UN MODELO LATINOAMERICANO DE ADECUACIÓN PARA LA TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES

Luca Belli, Ana Brian Nougrères, Jonathan Mendoza Iserte,
Pablo A. Palazzi y Nelson Remolina Angarita

FGV DIREITO RIO
CENTRO DE TECNOLOGIA E SOCIEDADE

CETyS
Centro de Estudios en Tecnología y Sociedad

Universidad de SanAndrés

UNITED NATIONS HUMAN RIGHTS SPECIAL PROCEDURES
SPECIAL RAPPORTEURS, INDEPENDENT EXPERTS & WORKING GROUPS

Universidad de los Andes

CPDP LatAm
cpdp.lat

Discussion paper **presentado en la Computers, Privacy and Data Protection Conference Latin America (CPDP LatAm) 2023 para recibimiento de comentarios. La versión consolidada de este trabajo será publicada en "Protección de datos personales: doctrina y jurisprudencia. CETYS, CDYT, 2023, Buenos Aires".**

Hacia un modelo latinoamericano de adecuación para la transferencia internacional de datos personales

Luca Belli[1], Ana Brian Nougrères[2], Jonathan Mendoza Iserte[3], Pablo A. Palazzi[4] y Nelson Remolina Angarita[5]

Los autores dedican este trabajo a la memoria del Prof. Danilo Doneda (1970-2022).

Discussion paper **presentado en la Computers Privacy and Data Protection Conference Latin America (CPDP LatAm) 2023 para recibimiento de comentarios. La versión consolidada de este trabajo será publicada en "Protección de Datos personales: Doctrina y Jurisprudencia. CETYS, CDYT, 2023, Buenos Aires".**

RESUMEN: Este breve estudio presenta el régimen normativo de las transferencias internacionales de datos personales con base en la legislación de varios países latinoamericanos (Argentina, Brasil, Colombia, México y Uruguay), su régimen general y las distintas excepciones consideradas en la regulación existente. Finalmente, luego de explicar las divergencias se proponen distintas alternativas para crear un régimen de adecuación para América Latina.

PALABRAS CLAVE: transferencias internacionales, datos personales, adecuación, cláusulas contractuales modelo, binding corporate rules, códigos corporativos vinculantes, derecho internacional, Argentina, Brasil, Colombia, México, Uruguay, países "adecuados", "Privacy Shield", Schrems I, Schrems II, América Latina, Convenio 108, Red iberoamericana de Protección de datos personales.

---

[1] Professor at Fundação Getulio Vargas (FGV) Law School, Rio de Janeiro, director del Center for Technology and Society (CTS-FGV) and the CyberBRICS project, Director of the Latin-American edition of the Computers Privacy and Data Protection conference (CPDP LatAm).

[2] Doctora en Derecho y Ciencias Sociales por la Facultad de Derecho de la Universidad de la República Oriental del Uruguay, Relatora Especial de las Naciones Unidas en materia de Privacidad por el Consejo de Derechos Humanos de las Naciones Unidas desde el 1 de agosto de 2021.

[3] Secretario de Protección de Datos Personales del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).

[4] Profesor de Derecho Universidad de San Andrés (Argentina), Director del CETyS - Centro de Tecnologia y Sociedad de Universidad de San Andrés, Director del Diplomado Internacional de protección de datos personales de la Universidad de San Andrés.

[5] Profesor de Derecho Universidad de los Andres, Director del GECTI (Univ. de los Andes), ex director de datos personales de la Superintendencia de Comercio de Colombia.

Discussion paper **presentado en la Computers, Privacy and Data Protection Conference Latin America (CPDP LatAm) 2023 para recibimiento de comentarios. La versión consolidada de este trabajo será publicada en "Protección de datos personales: doctrina y jurisprudencia. CETYS, CDYT, 2023, Buenos Aires".**

SUMARIO

1. INTRODUCCIÓN

En el ámbito de la protección de datos personales, un tema que ha sido clave para impulsar el desarrollo y la adopción de normatividad en esta materia son las transferencias internacionales de datos, que son de gran importancia en la actualidad debido a la globalización y a la naturaleza cada vez más interconectada de nuestra sociedad. En un mundo cada vez más digital, las empresas y organizaciones necesitan transferir datos constantemente entre diferentes países y regiones para poder realizar sus actividades y operaciones diarias.

La importancia de las transferencias internacionales de datos radica en varios aspectos uno de ellos es el comercio internacional, ya que permiten a las empresas transferir información sobre productos, servicios, pagos y otros aspectos comerciales a nivel global. Por otro lado, las transferencias internacionales de datos son cruciales para la investigación y el desarrollo en diversos campos, como la ciencia, la tecnología y la medicina, ya que permiten a los investigadores compartir datos e información para avanzar en sus investigaciones.

Las transferencias internacionales de datos también plantean desafíos en términos de privacidad y seguridad de la información. Por ello, se han establecido marcos normativos y acuerdos internacionales para garantizar la protección de datos personales y la privacidad de los individuos en el contexto de las transferencias internacionales de datos.

Uno de los mecanismos más conocidos es el procedimiento de adecuación de terceros países de conformidad a la legislación del país o región de que se trate. Ejemplo de lo anterior, es el proceso de adecuación para terceros países de la Unión Europa, al cual por el lado latinoamericano solo lo han completado Argentina y Uruguay, y en proceso se encuentran Colombia y México.

Este mecanismo no es el único existente, alrededor del mundo se han iniciado debate en torno a la regulación de las transferencias internacionales en los bloques económicos existentes como el compuesto por Brasil, Rusia, India, China y Sudáfrica, mejor conocido como BRICS. De igual manera la discusión ha llegado al más alto nivel y el tema ha sido puesto en las agendas de los países más acaudalados en el G7 integrado por Alemania, Canadá, Estados Unidos de América, Francia, Italia, Japón y Reino Unido.

2. JUSTIFICACIÓN

Los expertos en privacidad y protección de datos personales de los países de la región latinoamericana se han dado cuenta de que la transformación digital es un elemento esencial para el futuro de sus economías y sociedades. En esta perspectiva, la protección de datos se convierte en una prioridad clave para fomentar entornos digitales

prósperos, donde las personas disfrutan de protecciones y las empresas se benefician de la seguridad jurídica.

Dado el notable valor económico y estratégico que han adquirido los datos personales, la regulación de esta "nueva clase de activos" se convierte también en un factor esencial para la afirmación de la soberanía digital. En los últimos cinco años, la necesidad apremiante de regular los datos personales ha estimulado la propuesta, adopción e implementación de marcos de protección de datos cada vez más compatibles.

Por lo anterior, en la región latinoamericana nace la iniciativa de poner en marcha la creación de un modelo latinoamericano de adecuación para garantizar el libre flujo de datos personales entre los países de la región, tomando como punto de partida los procesos de adecuación vigentes en el mundo.

El continente americano, por su ubicación geográfica, se convierte en un punto de encuentro entre los cinco continentes, por lo que establecer un estándar común facilitaría el tratamiento y flujo de datos personales, en un ejercicio que beneficiará a todos los involucrados, desarrolladores, sector privado y el usuario final de los productos y servicios que se ofrecen.

3. ALCANCE DEL TRABAJO

Esta iniciativa está enfocada y dirigida a los países que integran la región latinoamericana. La propuesta servirá de orientación y guía para las autoridades de protección de datos personales de la región y pretende ser un instrumento por el cual se establezca un estándar común para la garantía y salvaguarda de los datos personales en las transferencias transfronterizas de datos personales.

4. METODOLOGÍA DEL TRABAJO

El presente documento tiene como objetivo sentar las bases de un modelo latinoamericano de adecuación, que como otros ejercicios existentes no solo en la región sino a nivel internacional, se rigen por los parámetros necesarios para dar confiabilidad y seguridad al tratamiento de datos personales.

Por lo anterior, los países que sean parte de este modelo deberán integrar los antecedentes normativos que regulan la protección de datos personales en sus respectivas jurisdicciones y enfatizar la regulación emitida en cuanto al tratamiento de datos personales en las transferencias nacionales e internacionales, de ser el caso.

Asimismo, en caso de que la regulación de su país establezca un procedimiento de adecuación para terceros países, deberá señalar el procedimiento implementado o, en su caso, si el país en cuestión ya ha sido aprobado como país adecuado ante un proceso

de adecuación, señalar la experiencia y requisitos que tuvo que cumplir para dicha aprobación.

En cuanto al procedimiento para adoptar un acto de ejecución relativo a la adecuación de la protección de los datos personales, éste iniciará con un análisis exhaustivo del ordenamiento jurídico del tercer país, específicamente de su legislación en la materia.

De manera específica se evalúan, entre otros, los siguientes aspectos:

- El marco jurídico y su ámbito de aplicación material y personal;
- Los compromisos internacionales adquiridos por el tercer país, así como las obligaciones resultantes de su participación en sistemas multilaterales o regionales, en particular en relación con la defensa de los derechos humanos y de la protección de los datos personales, y el cumplimiento de esas obligaciones;
- Los derechos de los titulares acceso, rectificación, cancelación, oposición y portabilidad);
- Los deberes y obligaciones de los responsables y encargados del tratamiento, incluyendo la observancia obligatoria de los principios de protección de datos personales reconocidos a nivel internacional;
- Las limitaciones para realizar transferencias de datos personales ulteriores;
- Las medidas de supervisión del cumplimiento de la norma, incluyendo la existencia de una autoridad de control independiente encargada de supervisar las normas en materia de protección de datos y de hacerlas cumplir. Esta autoridad debe actuar con total independencia e imparcialidad en el desempeño de sus funciones y en el ejercicio de sus competencias.
- La existencia de recursos administrativos y acciones judiciales efectivos, incluida la indemnización por daños y perjuicios, que pueda ejercer el titular cuando se vulnere su derecho o, incluso, por acciones u omisiones por parte de la autoridad de control;
- La existencia de salvaguardas específicas para el tratamiento de datos personales en el contexto de acciones judiciales y penales, de seguridad nacional, entre otros casos particulares.

El presente compendio de información de los países de la región latinoamericana es un primer ejercicio de acercamiento a conocer el estado del arte en cuanto a la regulación vigente en materia de transferencias de datos personales. Una vez completado este primer ejercicio, se determinarán mecanismos adicionales que faciliten la difusión e promoción del modelo en la región.

En los próximos puntos analizamos uno por uno (por orden alfabético) el sistema de transferencias internacionales en Argentina, Brasil, Colombia, México y Uruguay. Este análisis sirve de base para entender cómo funciona actualmente cada sistema legal de los países mencionados, y a partir de allí buscar elementos comunes que permitan desarrollar un modelo latinoamericano de adecuación.

5. ARGENTINA

5.1. INTRODUCCIÓN AL SISTEMA ARGENTINO

La ley de protección de datos personales n. 25.326 fue aprobada en el año 2000. Su reglamentación mediante decreto 1558 fue aprobada en el año 2001.

Argentina fue declarado país adecuado por la Unión Europea el 30 de junio de 2003[6]. Argentina ha ratificado el Convenio 108 y el Convenio 108 modernizado.

5.2. REGLAS SOBRE TRANSFERENCIA INTERNACIONAL Y EXCEPCIONES

El art. 12.1 de la ley de protección de datos personales prohíbe la transferencia de datos personales de cualquier tipo con países que no proporcionen niveles de protección adecuados.

Según el art. 12.2 de la citada norma, la prohibición no regirá en algunos supuestos que son: a) Colaboración judicial internacional; b) Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del afectado, o una investigación epidemiológica; c) Transferencias bancarias o bursátiles, en lo relativo a las transacciones respectivas y conforme la legislación que les resulte aplicable; d) Cuando la transferencia se hubiera acordado en el marco de tratados internacionales en los cuales Argentina sea parte; e) Cuando la transferencia tenga por objeto la cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo y el narcotráfico.

La ley argentina contempló limitadas excepciones para la importancia del tema. El decreto reglamentario las amplió inspirándose en las previstas en el art. 26 de la entonces vigente Directiva Europea de Protección de Datos del año 1995 lo que implicó una mayor armonización con el régimen europeo.

Por otra parte, razones de lógica llevaban a concluir que Argentina no podía aislarse en un mundo interconectado y por ello resultaba necesario adoptar resguardos tales como las medidas contractuales para permitir continuar con las transferencias existentes entre empresas de un mismo grupo económico o controlante y controladas.

El decreto reglamentario (art. 12, decreto 1558/2001) establece que la prohibición de transferir datos personales hacia países u organismos internacionales o supranacionales que no proporcionen niveles de protección adecuados, no rige cuando el titular de los datos hubiera consentido expresamente la cesión.

[6] Decisión de la Comisión, de 30 de junio de 2003, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo sobre la adecuación de la protección de los datos personales en Argentina, Diario Oficial n° L 168 de 05/07/2003 p. 19, bit.ly/3OUe6mz

El decreto reglamentario de la ley de protección de datos también agrega que "No es necesario el consentimiento en caso de transferencia de datos desde un registro público que esté legalmente constituido para facilitar información al público y que esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo, siempre que se cumplan, en cada caso particular, las condiciones legales y reglamentarias para la consulta" (art. 12 de la ley 1558/2001).

Finalmente, siguiendo la Directiva Europea (art. 26), el art. 12 del decreto reglamentario permite a las partes que transfieren datos en forma internacional a países no adecuados recurrir a contratos o cláusulas que aseguren una protección adecuada. Pese a que el decreto 1558/2001 autorizaba el uso de fórmulas contractuales para transferir datos personales a jurisdicciones con leyes "no adecuadas", hasta el año 2016 la DNPDP nunca aprobó un modelo oficial.

5.3. LA DISP. 60/2016 SOBRE ADECUACIÓN Y CLÁUSULAS CONTRACTUALES MODELO

Mediante la Disp. 60/2016 la agencia de datos personales de Argentina[7] hizo lo siguiente:

- aprobó dos contratos modelo para usar para transferir datos a países no adecuados;
- reglamentó la necesidad de solicitar autorización para usar un modelo diferente al oficial;
- determinó un listado de países "adecuados" al sistema argentino de datos personales;
- dejó abierta la puerta para seguir incluyendo nuevos países en la "lista blanca" de países aprobados.

Como es dable observar la agencia argentina de datos personales en un mismo acto normativo hizo dos cosas importantes: realizó un listado de países adecuados y aprobó modelos de contratos para transferencia internacional de datos personales.

Con anterioridad a la Disp.60/2016, no se requería aprobación previa por la DNPDP. Tampoco existía un modelo de contrato tipo aprobado por la autoridad reguladora argentina, como sí sucedía en Europa con las cláusulas contractuales tipo.

Los responsables y encargados de tratamiento eran libres de realizar los contratos para transferencia internacional sin una guía específica de la DNPDP ni su previa aprobación. Si bien no había aprobación previa, la DNPDP a pedido de parte podía analizar los borradores de contratos y emitir un dictamen sobre la adecuación del mismo si el

[7] PALAZZI, Pablo, Las transferencias internacionales de datos personales en el anteproyecto de ley de protección de datos personales, en Revista Latinoamericana de Protección de Datos Personales, n. 4 (2018).

responsable del tratamiento optaba por presentarlo. Estos dictámenes formaron un cuerpo de jurisprudencia administrativa que permitía interpretar los requisitos para dar base legal a una transferencia internacional de protección de datos personales a una jurisdicción no adecuada.

En la práctica los responsables y encargados de tratamiento usaban un modelo que seguía muy de cerca el aprobado en la Unión Europa, conforme se podía concluir de los dictámenes de la DNPDP que sugerían modificaciones a los contratos presentados o aprobaban el presentado a autorización con breves cambios referidos a la cita de normativa local en vez de la europea.

5.4. DETERMINACIÓN DE PAÍSES ADECUADOS EN LA DISP. 60/2016

La finalidad de la Disp. 60/2016 es "garantizar un nivel adecuado de protección de datos personales en los términos del artículo 12 de la ley 25.326 en aquellas transferencias de datos que tengan por destino países sin legislación adecuada".

Según el art. 1 de la Disp. 60/2016 los modelos deben ser usados "en aquellas transferencias de datos que tengan por destino países sin legislación adecuada". Si el país de destino tiene legislación adecuada, entonces no deben usarse modelos contractuales ni ningún contrato, más allá de que las partes son libres de reglamentar la transferencia con un contrato genérico de procesamiento de datos, de locación de servicios o uno genérico de outsourcing (cumpliendo los requisitos del art. 25 de la ley y del decreto). Esta decisión da sustento a la libertad de las partes de no usar contratos de transferencia cuando ésta tiene lugar hacia países de la Unión Europea (o reconocidos por tal Unión como adecuados), donde la legislación obviamente es adecuada porque la UE es el modelo de la ley argentina.

5.5. ¿CUÁLES SON LOS PAÍSES ADECUADOS PARA LA AUTORIDAD ARGENTINA?

El art. 3 de la Disposición 60/2016 establece que a los fines de la aplicación de la presente disposición se consideran países con legislación adecuada a los siguientes: Estados miembros de la Unión Europea y miembros del Espacio Económico Europeo (EEE), Suiza, Guernsey, Jersey, Isla de Man, Islas Feroe, Canadá (sólo respecto de su sector privado), Andorra, Nueva Zelanda, Uruguay e Israel (sólo respecto de los datos que reciban un tratamiento automatizado).

Con este listado “positivo” de países, Argentina adopta un modelo similar de "lista blanca" sin decirlo, es decir, se suma a autorizar transferencias a países que son adecuados según la UE. Se adopta este sistema, pero sin adherir por escrito y estrictamente a la UE. Las conclusiones similares a las de la UE tienen lógica porque Argentina sigue el modelo europeo de protección de datos personales. Pero también esto implica de alguna forma delegar una función soberana en otro país.

Conforme indican los considerandos de la Disposición 60, en un expediente que tramitó en la DNPDP el Ministerio de Justicia se analizó la legislación de aquellos países calificados como legislación adecuada por parte de la Unión Europea, concluyéndose sobre el nivel equivalente de las normativas de dichos países respecto de la Ley argentina de protección de datos. El expediente que se cita es un estudio que hizo la DNPDP (cuando dependía del Ministerio de Justicia y antes de ser transferida a la órbita de la AAAIP) en el año 2012 y que determinó esa lista. Pero la lista no es cerrada, puesto que la agencia argentina podría de oficio o a pedido de partes interesadas realizar los estudios sobre otros países u organismos internacionales.

Es por eso que la norma aclara que "Esta enumeración será revisada periódicamente por esta Dirección Nacional, publicando la nómina y sus actualizaciones en su sitio oficial en Internet". Esta actualización podría servir para incluir nuevos países adecuados, o para retirar de la lista algunos países que no den garantías adecuadas para mantener la adecuación.

El Reino Unido, después de su salida de la Unión Europea (Brexit) tenía que ser reevaluado como un tercer país para ver si era "adecuado". Pese a no estar en la UE, si mantenía su infraestructura de legislación y agencia independiente de protección de datos, podrá seguir siendo país adecuado a los fines de transferir datos personales. La UE terminó declarando país adecuado al Reino Unido el 28 de junio de 2021. Pero Argentina, ya en el año 2019 modificó la Disp. 60 mediante la Resolución AAIP 34/2019 incluyendo al Reino Unido como país adecuado a pedido del propio Reino Unido[8].

Estados Unidos no está mencionado en la “white list” de la DNPDP porque en la práctica la DNPDP de Argentina siempre consideró que no tiene una ley general de protección de datos como el resto de los países europeos ni una agencia de protección de datos independiente. Tampoco aparecen mencionados países latinoamericanos tales como

[8] Los considerandos de la Resolución AAIP 34/2019 dicen así: “Que se ha recibido una solicitud por parte del DEPARTAMENTO DE SERVICIOS DIGITALES, CULTURA, MEDIOS Y DEPORTE DEL REINO UNIDO DE GRAN BRETAÑA E IRLANDA DEL NORTE, requiriendo a la AGENCIA DE ACCESO A LA INFORMACIÓN PÚBLICA que adopte las medidas necesarias a fin de garantizar que el flujo internacional de datos personales desde la REPÚBLICA ARGENTINA al REINO UNIDO DE GRAN BRETAÑA E IRLANDA DEL NORTE se mantenga de manera ininterrumpida tras la salida del REINO UNIDO DE GRAN BRETAÑA E IRLANDA DEL NORTE de la UNIÓN EUROPEA. Que de acuerdo a lo informado en la solicitud respectiva y de conformidad con la revisión de antecedentes por parte de la AGENCIA DE ACCESO A LA INFORMACIÓN PÚBLICA, los estándares de protección de datos personales proporcionados por el REINO UNIDO DE GRAN BRETAÑA E IRLANDA DEL NORTE se han mantenido e incluso se han reforzado con respecto a la situación normativa del Estado requirente al momento en el que la entonces DIRECCIÓN NACIONAL DE PROTECCIÓN DE DATOS PERSONALES habría decidido incluir a los Estados miembros de la UNIÓN EUROPEA -comprendiendo al REINO UNIDO DE GRAN BRETAÑA E IRLANDA DEL NORTE- en la enumeración de países con legislación adecuada (artículo 3 de la Disposición 60 - E/2016). Que, por los motivos expuestos, la AGENCIA DE ACCESO A LA INFORMACIÓN PÚBLICA considera que el REINO UNIDO DE GRAN BRETAÑA E IRLANDA DEL NORTE continúa proporcionando un nivel de protección adecuado en los términos de la Ley Nº 25.326.”.

México o Colombia, excepto Uruguay que fue declarado país adecuado por la Comisión Europea[9].

El modelo contractual aprobado por la Disp. 60/2016 debe ser usado por las partes que transfieren datos. Si se apartan del modelo se deberá pedir autorización a la DNPDP. El pedido de autorización debe hacerse hasta 30 días después de la firma del contrato. Pero nada impide que se lo presente antes, e incluso sin haber firmado el contrato.

Ello surge del art. 2 de la Disp. 60/2016 que establece: "...aquellos responsables de tratamiento que efectúen transferencias de datos personales a países que no posean legislación adecuada en los términos del artículo 12 de la Ley 25.326 y su Decreto reglamentario 1558/01, y utilicen contratos que difieran de los modelos aprobados en el artículo anterior o no contengan los principios, garantías y contenidos relativos a la protección de los datos personales previstos en los modelos aprobados, deberán solicitar su aprobación ante esta Dirección Nacional presentándolos, a más tardar, dentro de los TREINTA (30) días corridos de su firma".

Entendemos que este reconocimiento de adecuación realizado por la DNPDP no se extiende automáticamente a organizaciones que usen “binding corporate rules” — BCRs- o que tengan implementadas cláusulas contractuales tipo siguiendo el modelo europeo para cubrir transferencias internacionales. El reconocimiento de adecuación es a las jurisdicciones mencionadas en el art. 3 y a los fines de evitar la necesidad de tener un acuerdo al transferir datos exclusivamente a esas jurisdicciones.

Si una entidad está transfiriendo datos personales en base a un modelo anterior no aprobado u homologado por la DNPDP, o en base a otras vías como los binding corporate rules (BCR) deberá cumplir con la Disp. 60/2016. La BCRs son un conjunto de reglas o cláusulas corporativas vinculantes que tienen por objeto establecer las prácticas que una entidad lleva a cabo en materia de tratamiento de datos de carácter personal con la finalidad de facilitar las transferencias internacionales de datos en el seno de dicha corporación. Las BCRs constituyen un instrumento que los grupos multinacionales pueden hacer valer ante las autoridades de protección de datos, para garantizar la legalidad de las operaciones de transferencia de datos en su organización, independientemente de que el país de destino garantice o no un "adecuado nivel de protección" conforme a la normativa vigente en el país de origen de los datos. Los BCR fueron reconocidos en la Argentina mediante Resolución 159/2018 de la AAIP.

Los más prudente en estos casos sería o bien someter el contrato a usar a autorización, o bien usar el modelo contractual aprobado.

[9] PALAZZI, Pablo, Las transferencias internacionales de datos personales en el anteproyecto de ley de protección de datos personales, en Revista Latinoamericana de Protección de Datos Personales, n. 4 (2018).

En Argentina a partir de la Disposición 60/2016, existe un "modelo oficial" de contrato aprobado por la DNPDP, que sigue los lineamientos de las cláusulas tipo vigentes en Europa al 2018. De hecho, el art. 1 de la Disp. 60/2016 las denomina "cláusulas contractuales tipo" y los considerandos de la Disposición 60 las indican como fuente de la norma. Faltaría que Argentina actualice estas cláusulas modelo a las aprobadas por la UE en 2021.

La Disp. DNPDP 60 aprobó dos modelos, (i) uno para transferencia internacional de datos a otro responsable, caso típico la casa matriz que centraliza datos de las subsidiarias locales; (ii) el otro modelo es para la prestación de servicios, que podrá ser con la casa matriz o con un tercero que provee servicios y que, lógicamente, está fuera de país, sino no habría transferencia internacional.

La lectura de las cláusulas del contrato modelo permite colegir que el contrato tiene ciertos elementos esenciales destinados a brindar un nivel adecuado de protección en la transferencia y que deben estar presentes en los contratos que se usen apartándose del modelo. Estos elementos mínimos son:

- Referencia a la ley 25.326, al definir los conceptos de "datos personales", "datos sensibles", "tratamiento", "responsable" y "titular del dato",
- Identificación de la "autoridad" o "autoridad de control" con la DNPDP.
- Referencia al art. 25 de la ley 25.326 al referenciar al "importador" o "encargado del tratamiento", en el modelo de contrato de transferencia internacional para la prestación de servicios.
- Definir la "legislación de protección de datos" como la ley 25.326 y normativa reglamentaria.
- Detallar la finalidad y la clase de datos personales que se transfieren.
- Establecer ciertas obligaciones mínimas para el importador, esto es quien recibe los datos. Estas obligaciones mínimas incluyen: medidas de seguridad, cumplimiento del principio de finalidad, establecer una persona de contacto dentro de la organización del importador, permitir auditorías o inspecciones por un tercero auditor o incluso por la autoridad de contralor, notificar pedidos de cesión de autoridades extranjeras o accesos no autorizados (16), atender los pedidos de derecho de acceso, destruir los datos terminado el contrato o cumplida la finalidad, llevar un registro de las obligaciones asumidas y, el más importante: tratar los datos personales de conformidad con la ley N° 25.326, de protección de datos personales.
- Solidaridad entre ambas partes: cada una de las partes deberá responder ante los titulares de los datos por los daños que le hubiese provocado como resultado de la afectación de derechos reconocidos en el contrato de transferencia en los términos previstos por la ley 25.326, sus normas reglamentarias y derecho de fondo de Argentina. Esto puede dar lugar a reclamos de responsabilidad civil

extracontractual, administrativa sancionatorio o incluso contractual. Por ejemplo, la cláusula 5 del modelo aprobado por la DNPDP dice que "En aquellos casos en que se alegue incumplimiento por parte del importador de datos, el titular del dato podrá requerir al exportador que emprenda acciones apropiadas a fin de cesar dicho incumplimiento".

- Cláusula sobre terceros beneficiarios: ambos modelos de contrato contienen una cláusula sobre terceros beneficiarios o “third party beneficiary”. Mediante esta cláusula los titulares de los datos, podrán exigir al Importador (con quien no tienen relación directa) en carácter de terceros beneficiarios, el cumplimiento de las disposiciones de la ley 25.326 relacionadas con el tratamiento de sus datos personales
- Ley aplicable y jurisdicción: se establece la ley argentina y la autoridad de contralor; incluso en el caso de terceros beneficiarios, el importador se somete a la jurisdicción argentina, tanto en sede judicial como administrativa (esto es la jurisdicción administrativa de la DNPDP). Esta cláusula se impone en virtud del orden público que tiene la norma (art. 44 ley 25.326).
- Resolución del contrato: en caso que el importador de datos incumpla las obligaciones que le incumben en virtud de las cláusulas modelo de la DNPDP, el exportador de datos deberá suspender temporalmente la transferencia de datos personales al importador hasta que se subsane el incumplimiento. Asimismo, el contrato se tendrá por resuelto, por una suspensión mayor a 30 días, por incumplimiento de la ley, o por decisión de la DNPDP que establezca que el importador o el exportador de datos han incumplido el contrato.
- El modelo de contrato para prestación de servicio contiene una cláusula adicional relativa a subtratamiento de datos y un mayor detalle en las obligaciones que debe asumir una vez finalizada la prestación de los servicios de tratamiento de los datos personales.

En suma, son todos resguardos contractuales que tienden a que la DNPDP pueda tener un control sobre la transferencia del dato personales en caso de analizar el contrato.

5.6. ¿CÓMO SE DETERMINA CUÁNDO UN PAÍS ES ADECUADO?

Hay varios modelos en el derecho comparado. Algunos países listan las jurisdicciones que consideran como adecuadas a los fines de transferir datos personales (régimen conocido como "white list" o lista blanca). Otros pueden optar por listar países que no se consideran adecuados, una suerte de "lista negra". Finalmente, otros países pueden optar por no listar uno u otro país adecuado, sino adherir a las aprobaciones que haga otra jurisdicción.

Además de tener listas blancas o listas negras, es posible "engancharse" al régimen de otro país. Es el caso de Israel y Uruguay. En el caso de Uruguay, su agencia de protección de datos dictó la Res.17/2009 mediante la cual reconoció como países con protección

adecuada a todos aquellos países considerados como tales por la Comisión de la Unión Europea[10]. Israel sigue un modelo similar, su ley de protección de datos reconoce como adecuados aquellos países que la UE reconozca como adecuados.

Con esta tesis, la agencia de protección de datos respectiva se "ahorra" el trabajo de analizar la adecuación de cada país. Por lo tanto, para Uruguay Argentina sería adecuado pues así fue reconocido por la UE y dejaría de serlo si la UE revocara la adecuación de Argentina. Pero también lo fue por un tiempo Estados Unidos en virtud del Acuerdo de Puerto Seguro (Safe Harbor). Esta tesis presenta un problema: cuando el país en el cual se apoya la agencia modifica el status de la adecuación, como ocurrió entre la UE y Estados Unidos luego del caso "Schrems", ese país deja de ser adecuado para el país "enganchado". Eso mismo ocurrió con Israel respecto a transferencias a Estados Unidos luego del caso "Schrems". Uruguay sin embargo no emitió ninguna resolución luego del caso "Schrems", priorizando las relaciones comerciales por sobre las restricciones a los flujos de datos personales.

La ley 25.326 omitió explicar en detalle cómo se determina que un país u organismo internacional es adecuado a los fines del art. 12 de la ley. Pero el decreto reglamentario estableció ciertas pautas que permiten concluir cuándo un país es adecuado.

El decreto reglamentario facultó a la DNPDP a "evaluar, de oficio o a pedido de parte interesada, el nivel de protección proporcionado por las normas de un Estado u organismo internacional".

Si la DNPDP llegara a la conclusión de que un Estado u organismo no protege adecuadamente a los datos personales, la DNPDP debe elevar al PEN un proyecto de decreto para emitir tal declaración. La norma requiere un decreto solo para el caso de una declaración de falta de adecuación, no así para su reconocimiento. Ello da validez a la Disp. 60/2016. En la práctica este "no reconocimiento" expreso nunca ha ocurrido. Es decir, la legislación argentina permite crear un “black list” de países no adecuados pero el país nunca se ejerció esta facultad.

El decreto 1558/2001 también establece que "el carácter adecuado del nivel de protección que ofrece un país u organismo internacional se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos; en particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración de tratamiento o de los tratamientos previstos, el lugar de destino final, las normas de derecho, generales o sectoriales, vigentes en el país de que se trate, así como las normas profesionales, códigos de conducta y las medidas de seguridad en vigor en dichos lugares, o que resulten aplicables a los organismos internacionales o supranacionales".

[10] Consultar el punto respectivo de esta nota donde se analiza el sistema legal de Uruguay.

Finalmente, el decreto reglamentario dispone "Se entiende que un Estado u organismo internacional proporciona un nivel adecuado de protección cuando dicha tutela se deriva directamente del ordenamiento jurídico vigente, o de sistemas de autorregulación, o del amparo que establezcan las cláusulas contractuales que prevean la protección de datos personales".

La Disp. DNPDP 60 fue más directa y en el art. 3 enuncia los países adecuados. No es necesario entonces hacer un análisis del país de destino de la transferencia, a menos que el país no esté mencionado en la lista del art. 3 de la Disp. DNPDP 60/2016. En este caso la DNPDP si deberá hacer el análisis interno para incluirlo en la lista como ocurrió con el Reino Unido luego del Brexit.

5.7. ¿CÓMO SE SABE SI UN PAÍS QUE NO ESTÁ EN LA LISTA ES ADECUADO Y QUÉ MÉTODO DEBE USARSE PARA DETERMINARLO?

Para comenzar, si el país no está listado en el art. 3, ni fue objeto de un reconocimiento expreso por la DNPDP, en principio no es adecuado. Por eso es importante que la DNPDP amplíe su lista a algunos países latinoamericanos que si son adecuados y que desarrolle un método para explicar cómo se llega a ello.

En tal sentido, entendemos que lo más conveniente para Argentina sería adoptar el método ideado por la Unión Europea para analizar la adecuación de países extranjeros a través de varios documentos de trabajo emanados del Working Party del art. 29 (ahora EDPB). En este contexto, el documento de trabajo la Unión Europea concluyó que todo análisis significativo de la protección adecuada debe comprender los dos elementos básicos: (i) el contenido de las normas aplicables y (ii)los medios para asegurar su aplicación eficaz.

Tomando la Directiva 95/46/CE como punto de partida, y teniendo en cuenta las disposiciones de otros textos internacionales sobre la protección de datos, el documento señala que debería ser posible lograr un "núcleo" de principios de "contenido" de protección de datos y de requisitos "de procedimiento y de aplicación", cuyo cumplimiento pudiera considerarse un requisito mínimo para juzgar adecuada la protección. Este documento fue actualizado por el EDPB bajo RGPD.

El documento enuncia los siguientes principios básicos (Principios de contenido): (i) 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; (ii) Principio de proporcionalidad y de calidad de los datos - los datos deben ser exactos y, cuando sea necesario, estar actualizados. Los datos deben ser adecuados, pertinentes y no excesivos con relación al objetivo para el que se transfieren o para el que se tratan posteriormente; (iii) 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; (iv) 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; (v) Derechos de acceso, rectificación y oposición - el interesado debe tener derecho a obtener una copia de todos los datos a él relativos, y derecho a rectificar aquellos datos que resulten ser inexactos. En determinadas situaciones, el interesado también debe poder oponerse al tratamiento de los datos a él relativos; (vi) 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; (vii) Datos sensibles - cuando se trate de categorías de datos "sensibles", deberán establecerse protecciones adicionales, tales como la exigencia de que el interesado otorgue su consentimiento explícito para el tratamiento; (viii) Mercadotecnia directa - en el caso de que el objetivo de la transferencia de datos sea la mercadotecnia directa, el interesado deberá tener en cualquier momento la posibilidad de negarse a que sus datos sean utilizados con dicho propósito y (ix) Decisión individual automatizada - cuando el objetivo de la transferencia sea la adopción de una decisión automatizada en el sentido del artículo 15 de la Directiva, el interesado deberá tener derecho a conocer la lógica aplicada a dicha decisión, y deberán adoptarse otras medidas para proteger el interés legítimo de la persona.

Respecto a los "Mecanismos del procedimiento y de aplicación" el documento del WP29 explica que en Europa existe un amplio 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. Sin embargo, en otras partes del mundo no siempre se encuentran estas características. 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. Los objetivos de un sistema de protección de datos son básicamente tres: (i) Ofrecer un nivel satisfactorio de cumplimiento de las normas. 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 (ii) 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, y (iii) 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.

La Decisión de la Comisión Europea de 30/06/2003 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo sobre la adecuación de la protección de los datos personales en Argentina analizó el sistema legal de protección de datos personales vigente en Argentina en base a las pautas antes citadas y concluyó que el mismo era adecuado al régimen europeo. Pero con algunas salvedades. En efecto, la decisión llamó la atención sobre varios aspectos de la ley argentina, que a nuestro juicio requieren una reforma legislativa futura.

En función de estos parámetros, y luego de un análisis extenso la Comisión de la Unión Europea con la intervención del Working Party ha declarado adecuados a ciertos países. Argentina siguió el mismo criterio al reconocer a los mismos países listados en la Disp. 60/2016.

6. BRASIL

6.1. LAS TRASFERENCIAS INTERNACIONALES DE DATOS EN EL SISTEMA BRASILEÑO: LA LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES (LGPD) Y LA NECESIDAD DE REGULACIÓN DE LA ACTIVIDAD POR LA AUTORIDAD NACIONAL DE PROTECCIÓN DE DATOS (ANPD)

La Ley 13.709/2018, conocida como la Ley General de Protección de Datos Personales (LGPD), establece del tratamiento de datos personales en Brasil, que incluye normas específicas sobre transferencias de datos personales. Entre los principales deberes establecidos por la legislación, destaca la necesidad de cumplir con normas y procedimientos específicos para realizar transferencias internacionales de datos personales.

Los mecanismos de transferencia internacional de datos se han convertido en llaves para el desarrollo de la economía digital y, también, para garantizar la efectividad de los derechos a la protección de datos personales. Estos mecanismos fomentan la interoperabilidad legislativa[11] entre los diferentes sistemas normativos, la sostenibilidad de los flujos de datos, los cuales deben permitirse solo en la medida en que no se perjudiquen los derechos de los usuarios.

En esta perspectiva, es importante destacar que la LGPD consagra un mecanismo de aplicación extraterritorial de protección de datos que se aplica independientemente de la ubicación de la sede de la entidad o de la ubicación de los datos procesados, siempre y cuando que los datos procesados se refieran a personas físicas ubicadas en Brasil o cuando los datos personales procesados fueron recolectados en Brasil.

Los datos recopilados en Brasil son considerados como datos pertenecientes al titular de datos que se encontraba en Brasil en el momento de recopilación. La LGPD también se aplica, independientemente de la ubicación del territorio o entidad, o la ubicación de los datos son procesados, si el objetivo de la actividad de procesamiento de una entidad es ofrecer o fornecer bienes o servicios a personas físicas ubicadas en Brasil.

Para comprender el funcionamiento de la disciplina brasileña de protección de datos es, por lo tanto, necesario proporcionar una breve explicación terminológica preliminar, que será detallada en la siguiente sección.

[11] BELLI, Luca & DONEDA Danilo, Data Protection in the BRICS Countries: Legal Interoperability through Innovative Practices and Convergence. International Data Privacy Law, Volume 13, Issue 1, February 2023, Pages 1–24, https://doi.org/10.1093/idpl/ipac019

6.2. LOS CONCEPTOS DE DATOS PERSONALES, LA TRANSFERENCIA INTERNACIONAL Y LOS AGENTES DE TRATAMIENTO

Cabe destacar que el art. 5, inciso X de la LGPD incluye explícitamente la transferencia como ejemplo de actividad de tratamiento que implica "toda operación realizada con datos personales", mientras que define la "transferencia internacional" en su art. 5, XV, como "la transferencia de datos personales a un país extranjero o a una organización internacional de la cual el país sea miembro".

Es importante entender que el concepto de “transferencia” no está limitado al envío de datos personales de un país a otro: el almacenamiento de datos personales fuera del país y el acceso remoto a datos personales desde el extranjero, también son consideran como una “transferencia internacional” a efectos de la legislación.

Además, es importante recordar que la LGPD tomó notable inspiración en la conceptualización europea de dato personal, definiéndolo en el art. 5, I como "toda información relacionada con una persona natural identificada o identificable". Sin embargo, diferentemente del marco regulatorio europeo, la LGPD no define qué es un dato "identificable", por lo tanto, puede incluir un espectro extremadamente amplio de datos cuya transferencia debe estar sujeta al régimen establecido por la LGPD.

Es importante destacar también que el marco regulatorio brasileño no se aplica a los datos anonimizados, definidos como "datos relacionados con un titular que no pueden ser identificados, considerando el uso de medios técnicos razonables y disponibles en el momento de su tratamiento". No obstante, se aplica igualmente a los datos personales sensibles definidos como "datos personales sobre origen racial o étnico, creencias religiosas, opiniones políticas, afiliación a un sindicato o a una organización de carácter religioso, filosófico o político, datos relacionados con la salud o la vida sexual, datos genéticos o biométricos, cuando estén vinculados a una persona natural[12]”.

Finalmente, la LGPD se aplica a los controladores de datos y a los operadores de datos, que son conocidos conjuntamente como “agentes de tratamiento”, los cuales pueden ser empresas, sectores públicos, instituciones, bien como organizaciones sin fines lucrativos. El art. 5.º, VI da LGPD define al controlador como la “persona natural o jurídica, de derecho público o privado, a quien corresponden las decisiones relativas al tratamiento de datos personales”, es decir, la entidad responsable por definir como los datos personales serán tratados, con cuales finalidades y para quien. El art. 5.º, VII LGPD define el operador como una “persona natural o jurídica, de derecho público o privado, que realiza el tratamiento de datos personales en nombre del controlador”, es decir, la entidad que implementa las decisiones tomadas por el controlador.

[12] Ver LGPD art. 5.º, II e 5.º, III.

6.3. LAS CONDICIONES DE LA TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES

La LGPD permite la transferencia internacional de datos personales a países u organizaciones internacionales que ofrezcan un nivel adecuado de protección de datos personales, o cuando el controlador garantice el cumplimiento del régimen de protección de datos establecido en el capítulo V de la LGPD.

El capítulo V de la LGPD, que se denomina específicamente "Transferencia Internacional de Datos", establece en su art. 33, las situaciones legales que autorizan la transferencia internacional de datos personales, y detalla los pilares de la evaluación de adecuación en su art. 34. A su vez, el art. 35 de la LGPD establece que la Autoridad Nacional de Protección de Datos (ANPD) definirá el contenido de las cláusulas contractuales modelo, así como la verificación de cláusulas contractuales específicas para una determinada transferencia, normas corporativas globales o sellos, certificaciones y códigos de conducta, descritos en el inciso II del art. 33. Además, el §1º del art. 35 establece que, para la verificación prevista en el art. 35, se deben considerar los requisitos, condiciones y garantías mínimas para el cumplimiento de los derechos, garantías y principios de la LGPD al transferir datos personales a otra jurisdicción.

Particularmente, el art. 33 es una norma de mayor relevancia en lo que respecta a las condiciones que deben cumplirse para regular la transferencia internacional de datos, estableciendo que dicha actividad está permitida en los siguientes casos:

> *I - para países u organismos internacionales que proporcionen un nivel adecuado de protección de datos personales según lo previsto en esta Ley;*
> *II - cuando el controlador ofrezca y demuestre garantías de cumplimiento de los principios, derechos del titular y régimen de protección de datos previstos en esta Ley, en forma de:*
> *a) cláusulas contractuales específicas para una transferencia determinada;*
> *b) cláusulas contractuales modelo;*
> *c) normas corporativas globales;*
> *d) sellos, certificados y códigos de conducta emitidos regularmente;*
> *III - cuando la transferencia sea necesaria para la cooperación jurídica internacional entre organismos públicos de inteligencia, investigación y persecución, de acuerdo con los instrumentos de derecho internacional;*
> *IV - cuando la transferencia sea necesaria para proteger la vida o la integridad física del titular o de un tercero;*
> *V - cuando la autoridad nacional autorice la transferencia;*

> *VI - cuando la transferencia resulte de un compromiso asumido en un acuerdo de cooperación internacional;*
> *VII - cuando la transferencia sea necesaria para la ejecución de una política pública o una atribución legal del servicio público, siempre que se dé publicidad según lo dispuesto en el inciso I del caput del artículo 23 de esta Ley;*
> *VIII - cuando el titular haya otorgado su consentimiento específico y destacado para la transferencia, con información previa sobre el carácter internacional de la operación, distinguiéndola claramente de otros propósitos; [...]*

Las opciones establecidas en el art. 33 serán exploradas brevemente en las próximas secciones, enfatizando los principales avanzos y los principales límites de cada una de las condiciones previstas en la LGPD.

6.4. EVALUACIÓN DE ADECUACIÓN

La evaluación de adecuación del nivel de protección de datos personales de los países terceros será realizada por la ANPD que desempeña un papel central en el ámbito de la LGPD, siendo el "órgano de la administración pública indirecta responsable por cuidar, implementar y fiscalizar el cumplimento de esta ley". Los criterios que la ANPD debe seguir para llevar a cabo dicha evaluación son definidos por el art. 34 de la LGPD, según el cual la Autoridad tomará en cuenta:

> *I - las normas generales y sectoriales de la legislación vigente en el país de destino o en la organización internacional;*
> *II - la naturaleza de los datos;*
> *III - el cumplimiento de los principios generales de protección de datos personales y derechos de los titulares establecidos en esta Ley;*
> *IV - la adopción de medidas de seguridad previstas en el reglamento;*
> *V - la existencia de garantías judiciales e institucionales para el respeto de los derechos de protección de datos personales; y*
> *VI - otras circunstancias específicas relacionadas con la transferencia.*

La Autoridad aún no ha adoptado una regulación sobre la transferencia internacional de datos personales, aclarando el mecanismo de evaluación del nivel de protección de datos de países extranjeros u organismos internacionales, así como la definición del contenido de cláusulas estándar en contratos, que también le corresponde. Sin embargo, entre el 18 de mayo y el 30 de junio de 2022, llevó a cabo una Consulta Pública sobre Transferencia Internacional de Datos[13].

[13] Ver Consulta de la ANPD em: https://bit.ly/3D3z5MK

6.5. LA CONVOCATORIA PARA COMENTARIOS SOBRE TRANSFERENCIA INTERNACIONAL DE DATOS

El ítem 9 de la agenda reguladora bianual 2021-2022 de la ANPD, aprobada por la Ordenanza Nº 11 del 27 de enero de 2021, se refiere a la regulación de la transferencia internacional de datos personales, incluyendo la evaluación del nivel de protección de datos de países extranjeros u organismos internacionales y la definición del contenido de cláusulas estándar en contratos, que serán analizadas en la próxima sección.

De acuerdo con lo establecido en el artículo 14 de la Ordenanza ANPD Nº 16 de 2021, que aprueba el proceso de regulación en el ámbito de la Autoridad, la consulta ciudadana conocido como "tomada de subsídios" en portugués, así como la recopilación de datos e información que el equipo de la ANPD considere relevantes, se consideran como mecanismos de participación esenciales para el Análisis de Impacto Regulatorio (AIR).

La consulta ciudadana, sin embargo, no debe confundirse solamente como una simples consulta pública orientada al debate de una propuesta de regulación. Por el contrario, debe considerarse ya como una fase preliminar cuya función es prodrómica a la elaboración de una propuesta de regulación para su posterior debate. Por lo tanto, al llevarse a cabo durante el proceso de elaboración de la propuesta normativa, la consulta ciudadana es un instrumento adicional de democracia participativa que permite identificar y mejorar los aspectos significativos relacionados con el tema en cuestión, delimitando los problemas a abordar y las posibles alternativas regulatorias.

Sim embargo, a pesar de ter sido realizada entre mayo y junio de 2022, hasta el día de la redacción de este documento, los resultados de la toma de subsidios no fueron publicados. Dicho atraso parece peculiar, considerando que la regulación de transferencia internacional de datos personales fue explícitamente incluida en la Agenda Regulatoria de los años 2021 y 2022 de la ANPD, aprobada por la supra mencionada Ordenanza nº 16 de 2021.

6.6. CLÁUSULAS CONTRACTUALES ESPECÍFICAS Y CLÁUSULAS CONTRACTUALES MODELO

Como se destaca en el art. 33, el controlador puede realizar la transferencia internacional de datos personales mediante las cláusulas contractuales específicas, siempre que estas cláusulas sean debidamente verificadas y aprobadas por la Autoridad. La LGPD no define el proceso de evaluación de las cláusulas contractuales específicas de la ANPD, su limitación está definida en el art. 35 que dice que " en el análisis de cláusulas contractuales, de documentos o de normas corporativas globales sometidos a la aprobación de la autoridad nacional, se podrán solicitar información adicional o realizar diligencias de verificación sobre las operaciones de tratamiento cuando sea necesario" y para llevar a cabo la verificación de las cláusulas contractuales "deberán considerarse

los requisitos, las condiciones y las garantías mínimas para la transferencia que cumplan con los derechos, las garantías y los principios de esta Ley".

Además de las cláusulas específicas, el art. 33 de la LGPD permite el uso de cláusulas contractuales modelo (CCM) formuladas por la ANPD. Dicha herramienta definirá, por medio de cláusulas modelo, las responsabilidades de las partes involucradas en la transferencia y los derechos de los titulares de los datos que serán transferidos. De esta manera, la adopción de cláusulas contractuales modelos elaboradas por la ANPD, una vez que sean aprobadas, se convertirán en una herramienta valioso de cumplimiento normativo, demostrando la integración de los requisitos y de las responsabilidades establecidas en los contractos que regulan la transferencia de datos personales, sin que la ANPD efectué ulteriores actividades de evaluación.

Desafortunadamente, la LGPD no define el contenido de las cláusulas estándar contractuales, siendo, por lo tanto, necesaria la actividad regulatoria de la ANDP, que se inició con la consulta ciudadana supra mencionada, cuyos resultados todavía no fueron divulgados.

Como destaca la ANPD, las cláusulas contractuales modelo han sido el mecanismo de transferencia internacional de datos más utilizado mundialmente, funcionando inclusive como herramienta de convergencia entre diferentes sistemas. Esto se debe a que este mecanismo permite compatibilizar, a través de contractos, las normas de protección de datos de diferentes jurisdicciones, especialmente las del país que exporta los datos personales[14].

Por lo tanto, es importante destacar que, aunque la actividad regulatoria de la ANPD en relación con las CCM aún se encuentra en una etapa embrionaria, este instrumento es considerado particularmente prometedor por la Autoridad. En este contexto, la reciente adopción de una Guía de Implementación de Cláusulas Contractuales Modelo para la Transferencia Internacional de Datos Personales por parte de la Red Iberoamericana de Protección de Datos, de la cual la ANPD es miembro, podría influir considerablemente en el pensamiento del regulador brasileño[15].

6.7. NORMAS CORPORATIVAS MODELO

Las normas corporativas globales (NCGs) se introdujeron en la LGPD a partir de las Binding Corporate Rules (BCRs) típicas del sistema europeo, y permiten la transferencia internacional de datos personales entre empresas del mismo grupo económico y, por lo

[14] Ver Nota Técnica nº 20/2022/CGN/ANPD Asunto: Proposta de realização de Tomada de Subsídios para regulamentação de transferência internacional de dados pessoais, nos termos dos art. 33 e 35 da LGPD da Lei nº 13.709, de 14 de agosto de 2018.

[15] RIPD (Red Iberoamericana de Protección de Datos). Guía de Implementación de Cláusulas Contractuales Modelo para la Transferencia Internacional de Datos Personales. (2022), https://bit.ly/3pDeH1P

tanto, sujetas a la misma política interna de protección de datos personales. Destacase que, normalmente, las NCGs de un determinado grupo económico no se limitan a la definición de las condiciones de las transferencias internacionales. Son el documento que establece los procedimientos, las políticas y las medidas organizativas y técnicas adoptadas por todo el grupo para garantizar la protección de datos personales.

El art. 33 de la LGPD no proporciona elementos para comprender cómo se evaluará la conformidad de las NCGs. Sim embargo, el art. 35 establece la necesidad de verificación del contenido de las normas por parte de la Autoridad, especificando que en el "análisis de las cláusulas contractuales, de documentos o de normas corporativas globales presentadas para la aprobación de la autoridad nacional, podrán solicitarse información adicional o llevarse a cabo diligencias de verificación en relación con las operaciones de tratamiento, cuando sea necesario".

Por último, el art. 36 de la LGPD añade que "los cambios en las garantías presentadas como suficientes para cumplir con los principios generales de protección y con los derechos del titular mencionados en el inciso II del art. 33 de esta Ley, deben ser comunicados a la autoridad nacional".

6.8. SELLOS, CERTIFICADOS Y CÓDIGOS DE CONDUCTA

Las partes involucradas en la transferencia internacional de datos personales pueden también utilizar sellos, certificados o códigos de conducta reconocidos por la ANPD para realizar la transferencia de forma compatible con la LGPD. El art. 35 § 1.º, establece que, para la ANPD reconozca, sellos, certificados y códigos de conducta, deberán cumplir los requisitos, las condiciones y las garantías mínimas para el cumplimiento de derechos, garantías y principios de la LGPD.

Además, el art. 35 § 3.º agrega que la "autoridad nacional podrá designar organismos de certificación para el cumplimento de lo determinado en el caput de este artigo, que permanecerán abajo su fiscalización en los termos definidos en reglamento". Sim embargo, destacamos que dichos elementos aún no han sido definidos por la ANPD.

6.9. COOPERACIÓN JURÍDICA INTERNACIONAL

El art. 33 también permite la transferencia internacional de datos cuando sea "necesario para la cooperación jurídica internacional entre órganos públicos de inteligencia, de investigación y de persecución, de acuerdo con los instrumentos del derecho internacional". En relación con esta hipótesis, es importante destacar que se incluyen explícitamente las actividades de inteligencia, investigación y persecución como circunstancias en las cuales la protección del interés público justifica la transferencia de datos, a pesar de la falta de una normativa en materia de protección de datos en el ámbito de dichas actividades en Brasil.

Así como el Reglamento General de Protección de Datos de la Unión Europea, la LGPD elimina a su aplicación para casos de tratamiento de informaciones para la seguranza pública y persecución penal. Sim embargo, diferentemente del sistema europeo, en que hay una legislación específica, la Directiva 2016/680, que reguló la protección de datos personales en el ámbito de las actividades de inteligencia, investigación y persecución, en Brasil, la llamada “Ley General de Protección de Datos Penal” nunca superó la fase de proyecto de ley, no habiendo sido adoptada hasta la fecha y dejando así un importante vacío normativo.

6.10. PROTECCIÓN DE LA VIDA Y DE LA INCOLUMIDAD FÍSICA

La LGPD considera la protección de la vida o incolumidad física del individuo- sea de el mismo o de terceros- como una base legal para el tratamiento de datos. Por lo tanto, parece coherente que el art. 35 § 4.º considere “la protección de la vida o de la incolumidad física” como una justificativa válida para la transferencia internacional de datos personales.

6.11. AUTORIZACIÓN DE LA ANPD

El inciso V del art. 33 establece que la transferencia internacional de datos personales puede realizarse “cuando la autoridad nacional autorice la transferencia”. Esta norma puede convertirse en una verdadera carta sorpresa para la ANPD, que tiene una notable direccionalidad- y potencial licencia de creatividad- para reglamentar las transferencias internacionales de datos en la total ausencia de procedimientos y criterios de evaluación establecidos por la LGPD.

6.12. ACUERDOS DE COOPERACIÓN INTERNACIONAL

El inciso VI del artículo 33 establece que la transferencia internacional de datos personales solo está permitida "cuando la transferencia resulte de un compromiso asumido en un acuerdo de cooperación internacional". Se debe reconocer que la redacción de esta disposición crea una notable confusión, ya que, si se interpreta literalmente, parece considerar la transferencia como generadora del compromiso internacional.

Por lo tanto, cabe destacar que esta norma debe ser considerada como víctima de un error de redacción del legislador, que en lugar de escribir "resultar en", debería haber escrito "resultar de", siendo la transferencia el resultado del compromiso internacional.

7. COLOMBIA

7.1. DEL NIVEL ADECUADO DE PROTECCIÓN

La exportación y la importación de información personal no pueden convertirse en un escenario reductor del nivel de protección que se le confiere al titular del dato en el país desde donde se exportan datos personales. Para la Corte Constitucional de la República de Colombia existen principios que, a pesar de no encontrarse numerados en el artículo 4º de la Ley Estatutaria 1581 de 2012 se entienden incorporados en dicha norma[16]. Uno de ellos es el siguiente "principio de exigencia de estándares de protección equivalentes para la transferencia internacional de datos"

La Corte Constitucional reitera una preocupación internacional de los Estados cuando los datos de sus ciudadanos circulan a través de sus fronteras. Por eso, acude al criterio europeo en la materia, en el sentido de que no se deben enviar datos a países que no garanticen un nivel adecuado de protección. Para dicha entidad, "tal y como se deduce del artículos 26 del proyecto de ley estatutaria, existe una prohibición de transferencia internacional a cualquier tipo de países que no proporcionen niveles adecuados de protección de datos"[17].

Establecer el nivel adecuado no es solo cuestión formal de comparar los textos de las normas locales con las del país a donde se exportarán los datos, sino también de evaluar los mecanismos de protección real (administrativos, judiciales) con que cuenta el titular para que protejan adecuadamente sus datos en otro Estado, así como de verificar la existencia de autoridades de protección de datos independientes, técnicas y eficientes. En otras palabras, se debería establecer el nivel de protección real que ofrece en la práctica un país. En el caso de las autoridades de protección, por ejemplo, se debería considerar el número de quejas ciudadanas recibidas, así como las actuaciones iniciadas para dar respuesta a dichas quejas junto con las órdenes o sanciones emitidas para proteger los derechos y sancionar a los infractores de la regulación sobre tratamiento de datos.

Como es sabido, las regulaciones sobre transferencia internacional de datos o "flujo transfronterizo de datos" procuran garantizar que el nivel de protección de los datos personales de los ciudadanos de un país no disminuya o desaparezca cuando estos deben ser exportados o transferidos a otro u otros países. Por eso, en el caso de la regulación colombiana, por ejemplo, se prohíbe "*la transferencia de datos personales*

16 Cfr. Corte Constitucional, Sentencia C-748 de 2011, numeral 2.6.6.2.

17 Cfr. Corte Constitucional, Sentencia C-748 de 2011, numeral 2.6.6.2.

de cualquier tipo a países que no proporcionen niveles adecuados de protección de datos"[18].

No es absoluta la prohibición de transferir datos a terceros países que carezcan de niveles adecuados de protección. En ciertos casos excepcionales, ello es factible siempre y cuando se cumplan las condiciones que exige la Ley 1581, la jurisprudencia de la Constitucional (C-748/2011) y la eventual reglamentación sobre transferencias internacionales. En situaciones no previstas como excepciones en la citada ley, la SIC debe emitir una declaración de conformidad respecto de dicha transferencia[19].

7.2. DEL RECONOCIMIENTO A COLOMBIA COMO UN PAÍS CON NIVEL ADECUADO DE PROTECCIÓN

La Superintendencia de Industria y Comercio (SIC) de la República de Colombia, como autoridad de protección de datos personales, ha iniciado varios procesos para obtener nivel adecuado de protección de datos. Por ahora, ha sido reconocido por el Centro Financiero Internacional de Dubái como un país que ofrece un nivel adecuado de protección de datos personales[20].

Esta fue la conclusión del 6 de octubre de 2022 del DIFC[21] Office of the Commissioner of Data Protection: "It is for these reasons that the DIFC Office of the Commissioner of Data Protection ("the Commissioner") should grant adequacy recognition to Colombia. The current risk assessment regarding Colombia's laws and regulations, as well as the cultural and environmental approach to privacy and redress, align with the DIFC DP Law 2020 such that transfers to Colombia will receive the same or substantially equivalent protection when exported thereto"[22].

Adicionalmente, desde 2019 inició conversaciones o presentó solicitudes a otras organizaciones o países con el citado propósito. En todos los casos, se suministró, en esencia, la misma información considerada por el DIFC de Dubai.

---

[18] Cfr. República de Colombia. Ley 1581 de 2012, artículo 26

[19] *En los casos no contemplados como excepción en el presente artículo, corresponderá a la Superintendencia de Industria y Comercio, proferir la declaración de conformidad relativa a la transferencia internacional de datos personales. Para el efecto, el Superintendente queda facultado para requerir información y adelantar las diligencias tendientes a establecer el cumplimiento de los presupuestos que requiere la viabilidad de la operación* (par. 1º, art. 26, Ley 1581 de 2012).

[20] Cfr. Superintendencia de Industria y Comercio (SIC). Colombia es reconocida por su nivel adecuado de protección de datos por el Centro Financiero de Dubái. 18 de octubre de 2022, online en https://bit.ly/colombiareconoceadubai

[21] Dubai International Financial Centre Authority

[22] Cfr. Dubai International Financial Centre Authority ("DIFC" or "DIFCA") Commissioner of Data Protection

(2022) Assessment of Colombia's Data Protection Regime as Substantially Equivalent. El texto oficial puede consultarse en: https://bit.ly/aereconoceimientocolombia

Organización o país al que Colombia ha solicitado nivel adecuado	Fecha inicio trámite	Decisión
Comisión Europea	15 de octubre de 2019 iniciaron conversaciones preliminares (Oficio 19-236409 del Superintendente Delegado para la protección de Datos de la SIC)	Pendiente
Reino Unido de Gran Bretaña e Irlanda del Norte	Abril de 2021	Pendiente
Argentina	31 de agosto de 2021 (Oficio 21-348053 del Superintendente Delegado para la protección de Datos de la SIC)	Pendiente
Uruguay	31 de agosto de 2021 (Oficio 21-348062 del Superintendente Delegado para la protección de Datos de la SIC)	Pendiente

Tabla 1 - Listado de solicitudes realizadas por Colombia para obtener nivel adecuado de protección de datos personales

7.3. DE LOS RECONOCIMIENTOS DE NIVEL ADECUADO DE PROTECCIÓN DE DATOS OTORGADOS POR COLOMBIA A OTROS PAÍSES

Para efectos de la circulación transfronteriza de datos, la Superintendencia de Industria y Comercio (SIC) desde el mes de agosto de 2017 ha establecido que los siguientes países tienen nivel adecuado de protección de datos[23]: Alemania; Australia, Austria; Bélgica; Bulgaria; Chipre; Costa Rica; Croacia; Dinamarca; Eslovaquia; Eslovenia; Estonia; España; Estados Unidos de América; Finlandia; Francia; Grecia; Hungría; Irlanda; Islandia; Italia; Japón; Letonia; Lituania; Luxemburgo; Malta; México; Noruega; Países Bajos; Perú; Polonia; Portugal; Reino Unido; República Checa; República de Corea; Rumania; Serbia; Suecia; y los países que han sido declarados con el nivel adecuado de protección por la Comisión Europea (Suiza; Canadá; Argentina, Guernsey, Isla de Man, Jersey, Islas Feroe, Andorra, Israel, Uruguay, Nueva Zelanda y Japón).

Al mismo tiempo, la SIC, mediante la Circular Externa 5 del 10 de agosto del 2017, ordenó lo siguiente en el parágrafo primero del numeral 3.2:

Sin perjuicio de que las transferencias de datos personales se realicen a países que tienen un nivel adecuado de protección, **los responsables del tratamiento, en virtud del principio de responsabilidad demostrada, debe ser capaces de demostrar que han**

[23] Cfr. SIC Circulares externas 5 y 8 de 2017 y 2 de 2018.

implementado medidas apropiadas y efectivas para garantizar el adecuado tratamiento de los datos personales que transfieren a otro país y para otorgar seguridad a los registros al momento de efectuar dicha transferencia[24].

Como se observa, para transferir datos a otros países no es suficiente que el país de destino esté catalogado por la SIC como un país con nivel adecuado de protección, sino que además es necesario que el responsable del tratamiento pueda demostrar que ha tomado medidas adecuadas, útiles y prácticas para logra estos dos objetivos:

1. Garantizar el adecuado tratamiento de los datos personales que transfieren a otro país.
2. Conferir la seguridad de "los registros al momento de efectuar dicha transferencia".

7.4. ¿QUÉ EXIGE LA AUTORIDAD COLOMBIANA DE PROTECCIÓN DE DATOS PARA ESTABLECER SI UN PAÍS TIENE NIVEL ADECUADO DE PROTECCIÓN DE DATOS?

La regulación colombiana es enfática en señalar con absoluta claridad que los estándares fijados para establecer si un país tiene dicho nivel "*en ningún caso podrán ser inferiores*" [25] a los que la ley 1581 de 2012. Como se observa, para el caso colombiano no se puede enviar datos a un país que tenga un grado de protección inferior al previsto en la precitada norma[26]. Para establecer que otro país cumple con el nivel adecuado, se

[24] Cfr. el numeral 3.2 de la Circular 5 del 2017 de la SIC.

[25] Cfr. República de Colombia. Ley 1581 de 2012, artículo 26

[26] Esto dice el artículo 26 de la Ley Estatutaria 1581 de 2012: ART. 26.—**Prohibición**. Se prohíbe la transferencia de datos personales de cualquier tipo a países que no proporcionen niveles adecuados de protección de datos. Se entiende que un país ofrece un nivel adecuado de protección de datos cuando cumpla con los estándares fijados por la Superintendencia de Industria y Comercio sobre la materia, los cuales en ningún caso podrán ser inferiores a los que la presente ley exige a sus destinatarios.

Esta prohibición no regirá cuando se trate de:

a) Información respecto de la cual el titular haya otorgado su autorización expresa e inequívoca para la transferencia;

b) Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del titular por razones de salud o higiene pública;

c) Transferencias bancarias o bursátiles, conforme a la legislación que les resulte aplicable;

d) Transferencias acordadas en el marco de tratados internacionales en los cuales la República de Colombia sea parte, con fundamento en el principio de reciprocidad;

e) Transferencias necesarias para la ejecución de un contrato entre el titular y el responsable del tratamiento, o para la ejecución de medidas precontractuales siempre y cuando se cuente con la autorización del titular;

deben tener en cuenta los estándares que establezca la SIC para ese propósito, los cuales, dice la parte final del primer párrafo del artículo 26 de la Ley 1581 de 2012, "en ningún caso podrán ser inferiores a los que la presente ley exige a sus destinatarios".

La autoridad colombiana de protección de datos, mediante la Circular 5 del 10 de agosto de 2017 de la SIC estableció lo siguiente que se incorporó en el numeral 3.1. del Capítulo V (Protección de Datos) de la Circular Única de dicha entidad:

"El análisis para establecer sí un país ofrece un nivel adecuado de protección de datos personales, a efectos de realizar una transferencia internacional de datos, estará orientado a determinar si dicho país garantiza la protección de los mismos, con base en los siguientes estándares:

a. Existencia de normas aplicables al tratamiento de datos personales
b. Consagración normativa de principios aplicables al Tratamiento de datos, entre otros: legalidad, finalidad, libertad, veracidad o calidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad.
c. Consagración normativa de derechos de los Titulares.
d. Consagración normativa de deberes de los Responsables y Encargados.
e. Existencia de medios y vías judiciales y administrativas para garantizar la tutela efectiva de los derechos de los Titulares y exigir el cumplimiento de la ley.
f. Existencia de autoridad (es) pública (s) encargada (s) de la supervisión del Tratamiento de datos personales, del cumplimiento de la legislación aplicable y de la protección de los derechos de los titulares, que ejerza (n) de manera efectiva sus funciones."[27]

7.5. DE LA FLEXIBILIDAD PARA EXPORTAR DATOS DESDE COLOMBIA A OTROS PAÍSES

Si bien la Ley Estatutaria es estricta en las reglas de trasferencias internacionales, dichas pautas fueron modificadas por una norma de inferior jerarquía como la citada Circular

f) Transferencias legalmente exigidas para la salvaguardia del interés público, o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

PAR. 1º—En los casos no contemplados como excepción en el presente artículo, corresponderá a la Superintendencia de Industria y Comercio, proferir la declaración de conformidad relativa a la transferencia internacional de datos personales. Para el efecto, el superintendente queda facultado para requerir información y adelantar las diligencias tendientes a establecer el cumplimiento de los presupuestos que requiere la viabilidad de la operación.

PAR. 2º—Las disposiciones contenidas en el presente artículo serán aplicables para todos los datos personales, incluyendo aquellos contemplados en la Ley 1266 de 2008.

[27] Cfr. Numeral 3.1. del Capítulo V (Protección de Datos) de la Circular Única de la SIC. El texto oficial y completo puede consultarse en: https://bit.ly/44vCX4T

5 del 10 de agosto de 2017 de la SIC. Dicha circular aún sigue vigente y no ha sido declarada nula, razón por la cual tiene plena aplicabilidad.

En esa circular se crearon otros caminos no previstos en la Ley 1581 de 2012 para exportar datos desde Colombia a otros países. Señala la mismo lo siguiente que se incorporó en el numeral 3.2. del Capítulo V (Protección de Datos) de la Circular Única de la SIC:

Cuando la Transferencia de datos personales se vaya a realizar a un país que no se encuentre dentro los países considerados con nivel adecuado por la SIC, el Responsable del tratamiento deberá:

a. Verificar sí transferencia está comprendida dentro de una de las causales de excepción establecidas en el artículo 26 de la Ley 1581 de 2012, o,
b. *"Sí ese país cumple con los estándares fijados por la SIC, "casos en los cuales podrá realizar la transferencia".* (Destacamos). Como se observa, la SIC faculta a los exportadores de datos para que ellos (no la SIC) puedan establecer que determinado país cumple con los estándares fijados por dicha entidad. Esto último no lo establece la Ley 1518 de 2012 y es una clara extralimitación de poderes reglamentarios de dicha entidad porque mediante esa circular amplia el contenido y alcance de una Ley Estatutaria, estableciendo una nueva regla que no creó el legislador
c. De no cumplirse ninguna de las anteriores hipótesis, "solicitar la respectiva declaración de conformidad ante esta Superintendencia".

Adicionalmente, y respecto de la declaración de conformidad, la SIC se creó la siguiente regla no establecida en la Ley Estatutaria 1581 de 2012:

> *"Parágrafo: Cuando los Responsables del Tratamiento, que a efectos de cumplir con el principio de responsabilidad demostrada, suscriban un contrato con el Responsable del Tratamiento destinatario de los datos o implementen otro instrumento jurídico mediante el cual señalen las condiciones que regirán la transferencia internacional de datos personales y mediante las cuales garantizarán el cumplimiento de los principios que rigen el tratamiento, así como de las obligaciones que tienen a cargo, se presumirá que la operación es viable y que cuenta con Declaración de Conformidad.*
> *En consecuencia, los Responsables del Tratamiento podrán realizar dicha transferencia, previa comunicación remitida a la Delegatura para la Protección de Datos Personales de la Superintendencia de Industria y Comercio, mediante la cual informen sobre la operación a realizar y declaren que han suscrito el contrato de transferencia u otro instrumento jurídico que garantice la protección de los datos personales objeto de transferencia, lo cual podrá ser verificado en*

> *cualquier momento por esta Superintendencia y, en caso de que se evidencie un incumplimiento, podrá adelantar la respectiva investigación e imponer las sanciones que correspondan y ordenar las medidas a que haya lugar."*[28]

Al margen de su utilidad, la suscripción de un contrato de transferencia o instrumento jurídico no está previsto en la Ley 1581 de 2012 como un reemplazo de la declaración de conformidad.

[28] Cfr. Numeral 3.3. del Capítulo V (Protección de Datos) de la Circular Única de la SIC. El texto oficial y completo puede consultarse en: https://www.sic.gov.co/sites/default/files/normatividad/092022/T%C3%ADtulo%20V%20Versi%C3%B3n%2029-09-2022.pdf

8. MÉXICO

8.1. INTRODUCCIÓN: LAS TRANSFERENCIAS INTERNACIONALES DE DATOS EN EL SISTEMA LEGAL MEXICANO DE PROTECCIÓN DE DATOS PERSONALES

Los datos personales son definidos como cualquier información concerniente a una persona física identificada o identificable, entendida como aquélla cuya identidad puede ser determinada de forma directa o indirecta mediante cualquier información.

La protección de nuestros datos personales es uno de los elementos que integran el concepto de privacidad. Al respecto, algunos autores consideran necesario distinguir entre los términos "privacidad" e "intimidad", toda vez que estiman que la visión norteamericana contempla la privacidad como el derecho a estar aislado y no estar sujeto a la publicidad o escrutinio[29].

Ahora bien, el orden jurídico nacional en materia de protección de datos personales en México está estructurado bajo una clasificación que atiende a la naturaleza pública o privada de quienes llevan a cabo el tratamiento de datos personales, es decir, de los responsables.

El derecho humano a la protección de datos personales se encuentra inscrito en el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos ("CPEUM") reconociendo que todas las personas tienen derecho a la protección de sus datos personales, al acceso, rectificación y cancelación, así como a manifestar su oposición, en los términos establecidos por Ley.

Lo anterior, de conformidad con el artículo 1 de la Constitución que reconoce que todas las personas gozarán de los derechos humanos previstos en ésta y en los tratados internacionales de los que el Estado Mexicano sea parte y establece la aplicación del principio pro persona para la interpretación de las normas relativas a los derechos humanos.

[29] Cienfuegos Salgado, David. "El derecho a la intimidad y los actos procesales de imposible reparación. La tesis 1a/J17/2003, sobre admisión y desahogo de la prueba pericial en genética", Revista Lex, México, número 101, 2003, p. 47 y 203.

8.2. ANTECEDENTES NORMATIVOS EN MÉXICO

A partir de la reforma constitucional publicada en el Diario Oficial de la Federación el 1 de junio de 2009[30], se adicionó un párrafo al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos en el cual se dispuso que toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley.

Con base en lo anterior, el 5 de julio de 2010, se publicó en el Diario Oficial de la Federación la Ley Federal de Protección de Datos Personales en Posesión de los Particulares[31], la cual tiene por objeto la protección de los datos personales en posesión de las personas físicas o morales de carácter privado (particulares), a efecto de regular su tratamiento legítimo, controlado e informado, con la finalidad de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas.

Dicha normatividad, tiene como excepciones a las sociedades de información crediticia en los supuestos de la legislación que las regula, así como aquellas personas que realizan la obtención y almacenamiento de datos personales, cuando sea para uso exclusivamente personal, y sin fines de divulgación o utilización comercial.

Por otra parte, resulta necesario hacer referencia al Decreto de reforma constitucional en materia de transparencia, publicado en el Diario Oficial de la Federación el 7 de febrero de 2014[32], por virtud del cual se estableció que la Federación contaría con un organismo autónomo, especializado, imparcial, colegiado, con personalidad jurídica y patrimonio propio, responsable de garantizar el cumplimiento del derecho de acceso a la información pública y a la protección de datos personales en posesión de los sujetos obligados en los términos que establecidos en la ley; creando al actual Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

Asimismo, en la misma reforma constitucional se adicionaron las fracciones XXIX-S y XXIX-T al artículo 73 de la Constitución Política de los Estados Unidos Mexicanos, para

---

[30] DECRETO por el que se adiciona un segundo párrafo, recorriéndose los subsecuentes en su orden, al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, disponible en http://www.diputados.gob.mx/LeyesBiblio/ref/dof/CPEUM_ref_187_01jun09.pdf, consultada el 15 de julio de 2020.

[31] DECRETO por el que se expide la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y se reforman los artículos 3, fracciones II y VII, y 33, así como la denominación del Capítulo II, del Título Segundo, de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, disponible en http://dof.gob.mx/nota_detalle.php?codigo=5150631&fecha=05/07/2010, consultada el 15 de julio de 2020

[32] DECRETO por el que se reforman y adicionan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de transparencia, disponible en http://www.diputados.gob.mx/LeyesBiblio/ref/dof/CPEUM_ref_215_07feb14.pdf, consultada el 15 de julio de 2020.

conferir atribuciones al Congreso de la Unión para expedir las leyes generales reglamentarias que desarrollen los principios y bases en materia de transparencia gubernamental, acceso a la información y protección de datos personales en posesión de las autoridades, entidades, órganos y organismos gubernamentales de todos los niveles de gobierno.

Finalmente, el 26 de enero de 2017 se publicó en el Diario Oficial de la Federación, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados[33], misma que tiene por objeto establecer las bases, principios y procedimientos para garantizar el derecho de las personas a la protección de sus datos personales, en posesión de sujetos obligados, entendiendo por éstos a cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, en los ámbitos federal, estatal y municipal.

8.3. INSTRUMENTOS INTERNACIONALES RELEVANTES DE LOS QUE MÉXICO FORMA PARTE

La Declaración Universal de los Derechos Humanos en su artículo 12 plantea que "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques".

La Declaración Americana de los Derechos y Deberes del Hombre en el artículo 5 titulado "Derecho a la protección a la honra, la reputación personal y la vida privada y familiar" señala que "Toda persona tiene derecho a la protección de la Ley contra los ataques abusivos a su honra, a su reputación y a su vida privada y familiar.

El Pacto Internacional de Derechos Civiles y Políticos en el artículo 17 establece que nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación. De igual forma, se establece que toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

La Convención Americana de Derechos Humanos en el artículo 11 sobre "Protección de la Honra y de la Dignidad" establece tres puntos "Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad", "Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su

[33] DECRETO por el que se expide la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, disponible en http://dof.gob.mx/nota_detalle.php?codigo=5469949&fecha=26/01/2017, consultada el 15 de julio de 2020.

correspondencia, ni de ataques ilegales a su honra o reputación" y "Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques".

En el artículo 16 de la Convención sobre los Derechos del Niño se establece que los niños, niñas y adolescentes tienen el derecho a que se respete su privacidad, y es responsabilidad del Estado proteger este derecho y ese sentido se establece:

1. Ningún niño será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y a su reputación.
2. El niño tiene derecho a la protección de la ley contra esas injerencias o ataques.

Así mismo, en la Convención Internacional sobre la Protección de los Derechos de todos los Trabajadores Migratorios y de sus Familias en específico en el artículo 14 de esta Convención se establece que "Ningún trabajador migratorio o familiar suyo será sometido a injerencias arbitrarias o ilegales en su vida privada, familia, hogar, correspondencia u otras comunicaciones ni a ataques ilegales contra su honor y buen nombre. Todos los trabajadores migratorios tendrán derecho a la protección de la ley contra tales injerencias o ataques". Igualmente se acepta el derecho de los empleados mencionados y sus seres queridos a recibir protección legal en el territorio en el que se encuentren.

La Convención sobre los Derechos de las Personas con Discapacidad incluye el artículo 22, llamado "Respeto de la privacidad", el cual reconoce el derecho de las personas con discapacidad a la privacidad de su hogar, correspondencia, honra y reputación. En específico, el segundo párrafo establece que los Estados deben proteger la privacidad de la información personal y relacionada con la salud y la rehabilitación de las personas con discapacidad en igualdad de condiciones que las demás.

El Convenio 108 fue el primer instrumento jurídicamente vinculante a nivel internacional que se adoptó en cuanto a la protección de datos se refiere. Según el primer artículo de este convenio, su objetivo es garantizar, dentro del territorio de cada parte, el respeto de los derechos y libertades fundamentales de toda persona física, independientemente de su nacionalidad o lugar de residencia. Esto se refiere específicamente al derecho a la privacidad en relación con el tratamiento automatizado de los datos personales de dicha persona ("protección de datos").

El 28 de septiembre de 2018 se dio a conocer en el Diario Oficial de la Federación el decreto Promulgatorio del Convenio para la Protección de las Personas en cuanto al Tratamiento Automatizado de Datos de Carácter Personal, que fue adoptado en Estrasburgo, Francia, el 28 de enero de 1981.

A partir de lo expuesto en los tratados internacionales y documentos mencionados, se puede inferir que:

- México ha firmado diversos acuerdos internacionales que reconocen la importancia de los derechos a la privacidad y la vida privada. Entre estos instrumentos se encuentran la Declaración Universal de los Derechos Humanos, la Declaración Americana de los Derechos y Deberes del Hombre, el Pacto Internacional de Derechos Civiles y Políticos, la Convención Americana de Derechos Humanos, la Convención sobre los Derechos del Niño, la Convención Internacional sobre la Protección de los Derechos de todos los Trabajadores Migratorios y de sus Familias, la Convención sobre los Derechos de las Personas con Discapacidad y el Convenio 108.
- Uno de los acuerdos internacionales en materia de derechos humanos que México ha suscrito y que es especialmente relevante es el Convenio 108, que fue aprobado por la Cámara de Senadores el 26 de abril de 2018 y cuyo decreto fue publicado en el DOF el 12 de junio del mismo año. El Ejecutivo Federal firmó el instrumento de adhesión a este convenio el 19 de junio de 2018 y lo depositó ante el Secretario General del Consejo de Europa el 28 de junio de 2019. La adhesión a este convenio es importante tanto para el Estado mexicano en términos políticos y económicos como para las personas, ya que este instrumento regula un derecho humano fundamental.
- Los acuerdos jurídicos mencionados demuestran que el Estado Mexicano está comprometido con la protección efectiva de los derechos a la privacidad, la vida privada y la protección de datos personales. Es importante destacar que la RIPD, presidida por el INAI en ese momento, elaboró los EPDP, que son disposiciones modernas que establecen principios y derechos para la protección de datos personales. Estos principios pueden ser adoptados y desarrollados por los Estados Iberoamericanos en sus propias legislaciones nacionales, con el objetivo de garantizar un tratamiento adecuado de los datos personales.

8.4. TRANSFERENCIAS NACIONALES E INTERNACIONALES DE DATOS DE CARÁCTER PERSONAL

Las transferencias internacionales de datos son de gran importancia en la actualidad debido a la globalización y a la naturaleza cada vez más interconectada de nuestra sociedad. En un mundo cada vez más digital, las empresas y organizaciones alrededor del mundo necesitan transferir datos constantemente entre diferentes países y regiones para poder realizar sus actividades y operaciones diarias.

Los modelos de protección para las transferencias de datos personales pueden ser muy dispares, dependiendo de la región en las que se realicen. En México, la Ley adopta un modelo propio, pero el articulado de la misma y su Reglamento también pueden ser analizados a la luz de dos de los principales enfoques en materia de privacidad en el mundo: el europeo y el estadounidense, sin olvidar que es esencial que se garanticen

los derechos personales, pero también que no se obstruya el desarrollo comercial y global.

En el marco normativo mexicano las transferencias nacionales e internacionales de datos de carácter personal se encuentran regulados tanto en la Ley Federal de Protección de Datos Personales en Posesión de Particulares, como en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Para el sector privado, la Ley Federal establece en su Capítulo V, "Transferencias nacionales e internacionales de datos de carácter personal", artículos 36 y 37, y su Reglamento en los artículos 37, 38 y 39, señalando:

> *Artículo 36. Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento. El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, de igual manera, el tercero receptor, asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos.*
> *Artículo 37. Las transferencias nacionales o internacionales de datos podrán llevarse a cabo sin el consentimiento del titular cuando se dé alguno de los siguientes supuestos:*
>
> *I. Cuando la transferencia esté prevista en una Ley o Tratado en los que México sea parte;*
> *II. Cuando la transferencia sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios;*
> *III. Cuando la transferencia sea efectuada a sociedades controladoras, subsidiarias o afiliadas bajo el control común del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable que opere bajo los mismos procesos y políticas internas;*
> *IV. Cuando la transferencia sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el responsable y un tercero;*
> *V. Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público, o para la procuración o administración de justicia;*
> *VI. Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial, y*

> *VII. Cuando la transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular.*

Para el sector público, de conformidad con la Ley General, el Capítulo Único "De las Transferencias y Remisiones de Datos Personales", artículo 65 al 71, señala:

> *Artículo 65. Toda transferencia de datos personales, sea ésta nacional o internacional, se encuentra sujeta al consentimiento de su titular, salvo las excepciones previstas en los artículos 22, 66 y 70 de esta Ley.*
> *Artículo 66. Toda transferencia deberá formalizarse mediante la suscripción de cláusulas contractuales, convenios de colaboración o cualquier otro instrumento jurídico, de conformidad con la normatividad que le resulte aplicable al responsable, que permita demostrar el alcance del tratamiento de los datos personales, así como las obligaciones y responsabilidades asumidas por las partes.*
> *Lo dispuesto en el párrafo anterior, no será aplicable en los siguientes casos:*
> *I. Cuando la transferencia sea nacional y se realice entre responsables en virtud del cumplimiento de una disposición legal o en el ejercicio de atribuciones expresamente conferidas a éstos, o*
> *II. Cuando la transferencia sea internacional y se encuentre prevista en una ley o tratado suscrito y ratificado por México, o bien, se realice a petición de una autoridad extranjera u organismo internacional competente en su carácter de receptor, siempre y cuando las facultades entre el responsable transferente y receptor sean homólogas, o bien, las finalidades que motivan la transferencia sean análogas o compatibles respecto de aquéllas que dieron origen al tratamiento del responsable transferente.*
> *Artículo 67. Cuando la transferencia sea nacional, el receptor de los datos personales deberá tratar los datos personales, comprometiéndose a garantizar su confidencialidad y únicamente los utilizará para los fines que fueron transferidos atendiendo a lo convenido en el aviso de privacidad que le será comunicado por el responsable transferente.*
> *Artículo 68. El responsable sólo podrá transferir o hacer remisión de datos personales fuera del territorio nacional cuando el tercero receptor o el encargado se obligue a proteger los datos personales*

conforme a los principios y deberes que establece la presente Ley y las disposiciones que resulten aplicables en la materia.

Artículo 69. En toda transferencia de datos personales, el responsable deberá comunicar al receptor de los datos personales el aviso de privacidad conforme al cual se tratan los datos personales frente al titular.

Artículo 70. El responsable podrá realizar transferencias de datos personales sin necesidad de requerir el consentimiento del titular, en los siguientes supuestos:

I. Cuando la transferencia esté prevista en esta Ley u otras leyes, convenios o Tratados Internacionales suscritos y ratificados por México;

II. Cuando la transferencia se realice entre responsables, siempre y cuando los datos personales se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales;

III. Cuando la transferencia sea legalmente exigida para la investigación y persecución de los delitos, así como la procuración o administración de justicia;

IV. Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho ante autoridad competente, siempre y cuando medie el requerimiento de esta última;

V. Cuando la transferencia sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios, siempre y cuando dichos fines sean acreditados;

VI. Cuando la transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular;

VII. Cuando la transferencia sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el responsable y un tercero;

VIII. Cuando se trate de los casos en los que el responsable no esté obligado a recabar el consentimiento del titular para el tratamiento y transmisión de sus datos personales, conforme a lo dispuesto en el artículo 22 de la presente Ley, o

IX. Cuando la transferencia sea necesaria por razones de seguridad nacional.

La actualización de algunas de las excepciones previstas en este artículo, no exime al responsable de cumplir con las obligaciones previstas en el presente Capítulo que resulten aplicables.

> *Artículo 71. Las remisiones nacionales e internacionales de datos personales que se realicen entre responsable y encargado no requerirán ser informadas al titular, ni contar con su consentimiento*

8.5. CONCLUSIONES

México ha dado pasos importantes hacia la consolidación de su sistema jurídico de protección de datos personales, desde la óptica de los derechos humanos, cuestión que ha quedado patente con los diferentes procesos legislativos (como la existencia de dos leyes federales y las 31 leyes estatales) y la firma y ratificación del Convenio 108 del Consejo de Europa, por citar dos ejemplos al respecto.

La convicción bajo la cual se ha trabajado desde la reforma constitucional del artículo 16, para reconocer al derecho de protección de datos como un derecho fundamental, ha sido fortalecer el sistema de derechos humanos de este país bajo un pilar esencial, garantizar el adecuado y sano desarrollo de las personas en el contexto de la revolución tecnológica. Para ello, se deben buscar nuevos espacios que amplíen la protección de datos personales y brinden mayores fortalezas y beneficios para todos los mexicanos.

Trabajar en la búsqueda del reconocimiento de la Unión Europea, apunta a ser parte de un sistema de derechos humanos, específicamente en su componente de protección de datos, en el que se reconocen los estándares más exigentes en la materia a nivel global.

Para México, contar con la adecuación desde la óptica de terceros países, no solo está enfocado en cómo crear un mecanismo comercial que elimine barreras no arancelarias al comercio, sino que el énfasis está en determinar si nuestro país cuenta con las fortalezas suficientes para garantizar los derechos y libertades fundamentales con un marco normativo robusto, instituciones del Estado eficaces, garantías de los titulares, entre otros, sin dejar de tener en cuenta el potencial comercial que acompaña a este tipo de procesos.

En términos de lo antes planteado, consideramos que México debe seguir avanzando en el fortalecimiento de su sistema de derechos humanos, mediante el reconocimiento de un nivel de protección de datos personales adecuado, así México se sumaría al conjunto de democracias con el más alto nivel de exigencia en el espacio de uno de los derechos de la personalidad (protección de datos), con los múltiples efectos positivos que esto traería a la vida cotidiana de las personas, dada la transversalidad de esta medida.

9. URUGUAY

9.1. INTRODUCCIÓN AL SISTEMA URUGUAYO

El sistema jurídico uruguayo para las transferencias internacionales de datos, conforme el cual estas se encuentran en principio prohibidas, encuentra su inspiración en el Reglamento Europeo de Protección de Datos ((EU) 2016/679), así como en las normas que le precedieron. En tal sentido, es dable recordar que Uruguay fue declarado "adecuado" en el año 2012 (Resolución 2012/484/EU).

Conforme al sistema uruguayo de protección de datos personales, por tanto, en principio las transferencias internacionales de datos están prohibidas y su habilitación se produce como una excepción al mencionado principio general.

En este sentido, la ley madre de protección de datos (Ley N° 18.331, de agosto de 2008) sólo permite transferencias de datos personales a países que sean considerados "adecuados" por resolución de la autoridad de protección de datos uruguaya (la Unidad Reguladora y de Control de Datos Personales, en adelante, la URCDP), junto con otras varias excepciones establecidas en el artículo 23 de la mencionada Ley, conforme nos referiremos a continuación.

Entre las excepciones que admiten que se produzca la transferencia de datos personales a países que no se consideran adecuados podemos encontrar: el consentimiento expreso del interesado, que debe estar debidamente documentado; las transferencias que se realizan para cooperar con las autoridades públicas de otros países; la transferencia de datos sanitarios sensibles para el tratamiento médico de una persona en el extranjero o por razones de salud pública; la transferencia de datos personales financieros en caso de transacciones financieras internacionales; las transferencias de datos realizadas desde una fuente accesible al público ; las transferencias de datos realizadas en el ámbito de una convención o tratado internacional que Uruguay haya suscrito; las transferencias de datos realizadas en cooperación entre organismos de inteligencia contra la delincuencia organizada, el tráfico ilícito de drogas y la prevención del terrorismo. También, es posible realizar transferencias internacionales de datos si se realizan en cumplimiento de un contrato con el interesado (o para proteger los intereses del interesado), si es necesario u obligatorio para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial, o en el caso en que la transferencia sea necesaria para la salvaguardia del interés vital del interesado.

9.2. AUTORIZACIÓN A LA URCDP PARA REALIZAR LAS TRANSFERENCIAS INTERNACIONALES

Ahora bien, incluso si el país de destino no proporciona estándares de "adecuación" y la transferencia no se encuentra dentro de las excepciones legales, el responsable de la base de datos puede solicitar autorización a la URCDP para realizar las transferencias

internacionales de datos ofreciendo 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.

Para otorgar la autorización mencionada, que es potestad de la Unidad Reguladora, se tendrá en cuenta la adopción de cláusulas contractuales, la ubicación del responsable del tratamiento (y si el país en el que se encuentra ha adoptado alguna normativa de protección de datos), así como la auto certificación puesta a disposición por el organismo norteamericano de contralor FTC (Federal Trade Commission de los Estados Unidos de Norteamérica).

El régimen uruguayo de protección de datos recibió el impacto del caso "Schrems II" (C-311/18) y de la sentencia del TJUE de 16 de julio de 2020, como ocurrió en otras partes del mundo. Como consecuencia, la URCDP anunció algunos cambios en el régimen de protección de datos respecto a las transferencias internacionales de datos personales. Dichos cambios fueron realizados mediante la Resolución 23/2021, de 8 de junio de 2021, y la Resolución 41/2021, de 8 de septiembre de 2021.

9.3. IMPACTO DEL CASO "SCHREMS II": LA RESOLUCIÓN 23/2021

La Resolución 23/2021 realizó algunos ajustes con respecto a los países considerados "adecuados" para las transferencias internacionales de datos, eliminando de la lista las transferencias realizadas bajo el programa "Privacy Shield" entre la Unión Europea y los Estados Unidos de Norteamérica. La URCDP también tomó otras medidas complementarias, como establecer un plazo para la adecuación de los contratos existentes realizados bajo el programa "Privacy Shield".

A su vez estableció cuáles son los países considerados adecuados para las transferencias de datos personales, que son los países de la UE y el Acuerdo EEE, Andorra, Argentina, el sector privado de Canadá, Guernsey, Islas Man, Islas Feroe, Israel, Japón, Jersey, Nueva Zelanda, el Reino Unido, Irlanda del Norte y Suiza. La eliminación del "Privacy Shield" de la lista fue el cambio relevante realizado.

Un análisis realizado por la autoridad uruguaya concluyó que era necesario adaptar la lista de países adecuados frente al caso "Schrems II" y la sentencia del TJUE. Según lo declarado por la URCDP con respecto al "Privacy Shield", existen algunos elementos derivados del análisis realizado sobre el procesamiento de datos desde los Estados Unidos que resultaron en la invalidación de dicho marco de cooperación. La idea explícita detrás de esta decisión fue mantener al país actualizado para cumplir con los Estándares Internacionales de Protección de Datos de la Red Iberoamericana de Protección de Datos y el RGPD, permitiendo a Uruguay seguir siendo "adecuado" según los estándares europeos.

Para poner al día al sector público y privado en materia de privacidad y protección de datos, la URCDP dio a los responsables y encargados del tratamiento seis meses desde

la publicación de la Resolución (16 de septiembre de 2021) para ajustarse a las nuevas condiciones para las transferencias de datos realizadas previamente en el marco del programa “Privacy Shield”.

9.4. LA RESOLUCIÓN DE LA URCDP 41/21

La Resolución de la URCDP 41/2021 amplía aún más las modificaciones del régimen iniciadas con la Resolución 23/2021, poniendo a disposición de los responsables y encargados del tratamiento una guía sobre las cláusulas de redacción de un contrato de transferencia de datos, que sirve como ejemplo de buenas prácticas y como prueba del cumplimiento exigido por el artículo 23 de la Ley N° 18.331 para los casos en los que la autorización de la URCDP para realizar la transferencia internacional de datos se torna necesaria.

Las transferencias internacionales de datos a países considerados "no adecuados" por la URCDP (Resolución 23/021) deben ir precedidas de un análisis del riesgo e impacto de esta transferencia.

La guía contiene algunas estipulaciones consideradas de suma importancia y como contenido mínimo de cada contrato de transferencia de datos.

Cuenta con Cláusulas Generales y Cláusulas Específicas, las primeras establecen las disposiciones que deben estar en todo contrato internacional de transferencia de datos; las segundas, el contenido necesario en función de las partes que suscriben dicho contrato (Responsable-Responsable, Responsable-Encargado, Encargado-Encargado).

Las Cláusulas Generales constituyen requerimientos que se fundan en la necesidad de que cierta información sea explícitamente indicada en los términos del contrato, aunque algunas soluciones particulares también son obligatorias.

Si bien el texto de la Resolución no posee carácter obligatorio para quienes lo suscriben, algunos términos de la misma denotan obligatoriedad.

Este es el caso de la finalidad de la cesión, que debe estar claramente establecida en el contrato.

Asimismo, el derecho de información del interesado, según lo establecido en el artículo 13 de la Ley N° 18.331, que establece la información que debe facilitarse al interesado cuando se recopilan los datos, incluida la identidad del encargado del tratamiento y de los sub procesadores (si procede). Esta información debe estar disponible de forma permanente o debe facilitarse a petición del interesado.

En todo caso, el contrato deberá estipular que -- en caso de incumplimiento -- la autoridad administrativa competente deberá ser la uruguaya, con excepción de los casos en que el importador esté sujeto a una autoridad reguladora homónima en el país de destino.

El análisis de impacto obligatorio (artículo 6 f) del Decreto Nº 64/020) debe adjuntarse al contrato como demostración de la debida diligencia en materia de seguridad y privacidad de los datos.

Con respecto a la información que debe indicarse explícitamente en el contrato, los datos específicos transferidos al tercer país deben enumerarse en detalle. En caso de que haya datos sensibles, se debe detallar el contenido y el propósito para la transferencia de cada dato.

Se deben indicar los métodos de procesamiento aplicados a los datos, así como las medidas operativas y de seguridad, que deben ser explicitadas en las cláusulas para cumplir con los requisitos de seguridad de datos y enfoque proactivo de la privacidad de los datos de los artículos 10 y 12 (nueva redacción del artículo 39 de la Ley N° 19.670 y Decreto N° 64/020) de la Ley N° 18.331.

Si se opera una transferencia de datos con posterioridad, el controlador también debe establecer las condiciones bajo las cuales los datos se transferirán a otra parte.

Sobre la resolución de disputas, las partes pueden estipular cualquier mecanismo siempre que no altere los derechos del interesado, no incumpla con las leyes aplicables, modifique de alguna manera las operaciones de procesamiento en interés del interesado, ni establezca una retención indebida de información, que debe eliminarse de acuerdo con la ley aplicable.

Las condiciones bajo las cuales se conservarán los datos (por el exportador, el importador y terceros) también deben indicarse en las cláusulas. Los datos deben estar siempre a disposición de la URCDP, cumpliendo con lo establecido en el artículo 34 D) de la Ley 18.331.

La guía también exige que el contrato establezca el contenido de las obligaciones de confidencialidad asumidas por el personal del importador y del exportador, así como el hecho de que sólo las autoridades de control del país de destino pueden acceder a la base de datos con una orden judicial y siempre garantizando la seguridad y confidencialidad de los datos, accediendo sólo a aquellos que sean estrictamente necesarios para cumplir con dicha orden judicial.

Las Cláusulas Específicas, por su parte, versan sobre las bases legales para esa transferencia en particular y todas las posteriores, con especial atención a la responsabilidad de cada parte por los daños causados sobre los derechos del titular de los datos.

A pesar de que las cláusulas son obligatorias para las transferencias de datos realizadas a países que “no son adecuados” según la autoridad uruguaya, la Resolución exhorta a todos los responsables a tener en cuenta estas cláusulas en todo tipo de transferencia internacional de datos, en lo pertinente.

9.5. CONCLUSIONES

Las nuevas resoluciones de Uruguay marcan nuevas obligaciones para los sujetos involucrados en las transferencias internacionales de datos, estructurándose un sistema más complejo y con más cargas especialmente para las empresas, pero que tiene por ventaja para el país el poder continuar en la línea del sistema europeo de protección de datos personales. A su vez, la adaptación a los estándares pre acordados en materia de protección de datos personales por parte del estado uruguayo nos marca una conducta en pro de la cooperación internacional, lo cual es aceptado y especialmente valorado por los distintos actores con diferentes intereses en juego involucrados.

10. CONSIDERACIONES FINALES

10.1. DESAFÍOS ACTUALES EN AMÉRICA LATINA

Las transferencias internacionales de datos enfrentan varios desafíos, considerando su importancia en la economía digital se convierten en prácticas imprescindibles, que deben cumplir con los estándares de calidad y seguridad para los usuarios, tomando en consideración que en algunos casos su implementación es compleja a causa de la diferencia de las regulaciones que existe en cada país y a la imparable innovación tecnológica que ofrece día con día nuevas formas de comercializar y productos y servicios que ofrecer.

Enlisto algunos desafíos que se presentan como áreas de oportunidad para la efectiva y segura transferencia de datos:

1. Protección de datos y privacidad: uno de los principales desafíos es garantizar la protección y privacidad de los datos durante las transferencias internacionales de datos. Los datos pueden estar sujetos a diferentes leyes y reglamentos en cada país, lo que genera discrepancias en el nivel de protección y dificulta la garantía de la privacidad de las personas.
2. Jurisdicción y marcos regulatorios: Las transferencias internacionales de datos están influenciadas por diferentes jurisdicciones y marcos regulatorios en diferentes países. Cada país puede tener diferentes leyes y regulaciones con respecto a la protección de datos, lo que puede crear desafíos para cumplir con los requisitos legales y respetar los derechos de privacidad en diferentes contextos.
3. Seguridad de los datos: las transferencias internacionales de datos pueden presentar riesgos de seguridad, ya que los datos pueden estar expuestos a amenazas de seguridad cibernética, piratería o intercepción no autorizada durante el proceso de transferencia. La implementación de medidas de seguridad sólidas es esencial para proteger los datos durante la transferencia y el almacenamiento.
4. Consentimiento informado: Obtener el consentimiento informado de las personas para transferir sus datos personales a nivel internacional puede ser un desafío. Es posible que las personas no sean plenamente conscientes de cómo se utilizarán sus datos en otros países o de los riesgos asociados. Garantizar un consentimiento válido y claro se convierte en un desafío importante.
5. Transferencias a países con niveles de protección inadecuados: algunos países pueden tener niveles de protección de datos considerados inadecuados en comparación con los estándares internacionales. La transferencia de datos personales a estos países puede presentar riesgos adicionales para la privacidad y la seguridad de los datos.

6. Transparencia y rendición de cuentas: las organizaciones deben ser transparentes sobre cómo se transfieren, almacenan y utilizan los datos personales en el contexto de las transferencias internacionales. Adicionalmente, deben asumir la responsabilidad de asegurar el cumplimiento de las normas y estándares aplicables.

Para hacer frente a estos desafíos, se han establecido marcos legales y mecanismos de autorregulación, como acuerdos de transferencia de datos y estándares de seguridad, para garantizar una protección adecuada de los datos y el respeto de los derechos de privacidad en las transferencias internacionales de datos, una práctica que debemos alentar es la adopción de esquemas de autorregulación vinculante, así como la adopción de instrumentos jurídicos específicos como cláusulas modelo o Normas Corporativas Vinculantes (BCR por sus siglas en inglés), entre otras.

10.2. ALGUNAS IDEAS PARA EL DESARROLLO DE MECANISMOS DE ADECUACIÓN "LATINOAMERICANOS"

En América Latina resulta necesario desarrollar un marco regional adecuado para reconocimiento de adecuación de las jurisdicciones locales, a los fines de permitir el libre flujo de datos dentro de un marco protectorio de los derechos de protección de datos personales.

Esto podría darse de diferentes maneras, entre otras, las siguientes situaciones que describimos seguidamente:

a) Reconocimiento en base a legislaciones de datos personales vigentes en cada jurisdicción mediante un "checklist" que tenga como base a los Estándares Iberoamericanos desarrollados por la RelPD como una suerte de "marco general" para reconocimiento de adecuación. Este checklist podría ser elaborado por la Red Iberoamericana o mediante un acuerdo conjunto entre varias agencias de datos personales de la región (e ir sumando a las que quieran sumarse).
b) Tener en cuenta asimismo la existencia y aplicación de tratados vigentes sobre derechos humanos (la Convención Americana sobre Derechos humanos) y sobre protección de datos personales tales como el Convenio 108 original o el Convenio 108+ en la jurisdicción de destino de la transferencia de los datos.
c) Elaborar un tratado regional de protección de datos personales a nivel latinoamericano (por ej. en el marco de la OEA y siguiendo los Principios aprobados en 2021) que establezca como principio general que los países miembros poseen un nivel adecuado de protección de datos personales a los fines del libre flujo de datos personales dentro de la región y que fomente la cooperación directa entre las agencias de datos personales.

d) Desarrollar y promover el uso de cláusulas contractuales modelo para toda la región. En este sentido, la ReIPD elaboró una primera versión de las cláusulas contractuales modelo para transferencias a responsables y a encargados de datos y una Guía de implementación de las mismas. Por ahora solo Perú y Uruguay han adoptado este modelo y otros países lo están analizando. Pero aún queda mucho por hacer, por ejemplo, generar más módulos alternativos como hizo la UE al aprobar cuatro modelos y no solo dos, o redactar un modelo de cláusula contractual más compatible con la UE.
e) Desarrollar y promover el uso de "binding corporate rules" para toda la región a través la ReIPD o a través de un acuerdo de reconocimiento mutuo entre agencias de datos personales.
f) Puentes: Pensar en la posibilidad de reconocimiento con otras modelos vigentes en regiones (BRICs, Mercosur, Comunidad Andina, APEC, ASEAN, EU, APAs) a través de "puentes" o acuerdos regionales donde un bloque reconócelas herramientas de transferencia internacional usadas por otro bloque. Esto evitaría los reconocimientos unilaterales que terminan creando un "campo minado" para el libre flujo de datos personales.