TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES.

LAS CLÁUSULAS CONTRACTUALES DE LA RED IBEROAMERICANA DE PROTECCIÓN DE DATOS (RIPD) COMO ALTERNATIVA PARA FACILITAR LA EXPORTACIÓN DE INFORMACIÓN

NELSON REMOLINA ANGARITA

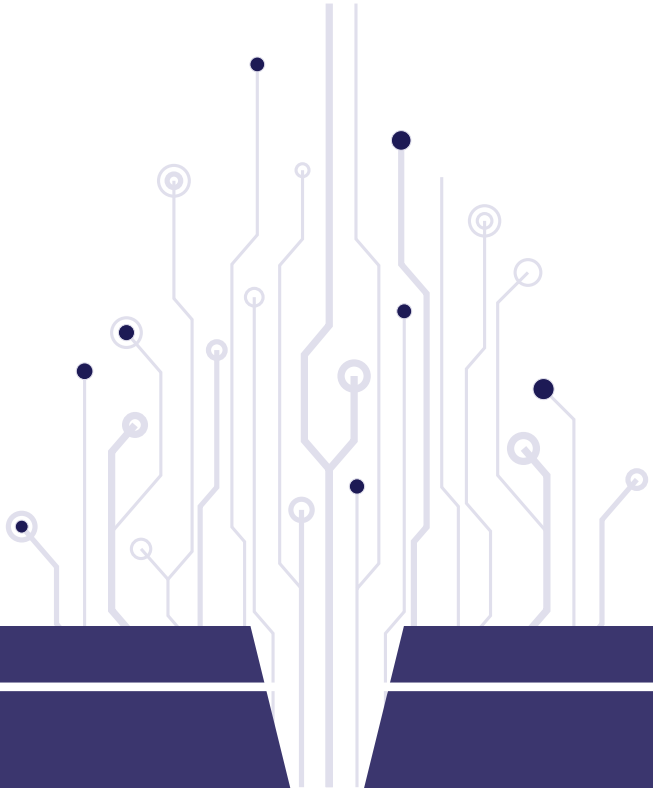
inai

Equipo Editorial

Edición: Edgar Samuel Rodríguez Ocampo, Kenya Soraya Martínez Ponce, Griselda Rubalcava Hernández y María Fernanda de León Canizalez.
Diseño editorial y portada: Diego González Hernández.

Primera edición digital, julio 2024.
ISBN: 978-607-5918-00-6
Hecho en México / Made in Mexico
Ejemplar de distribución gratuita
Tiraje: 1,500 ejemplares

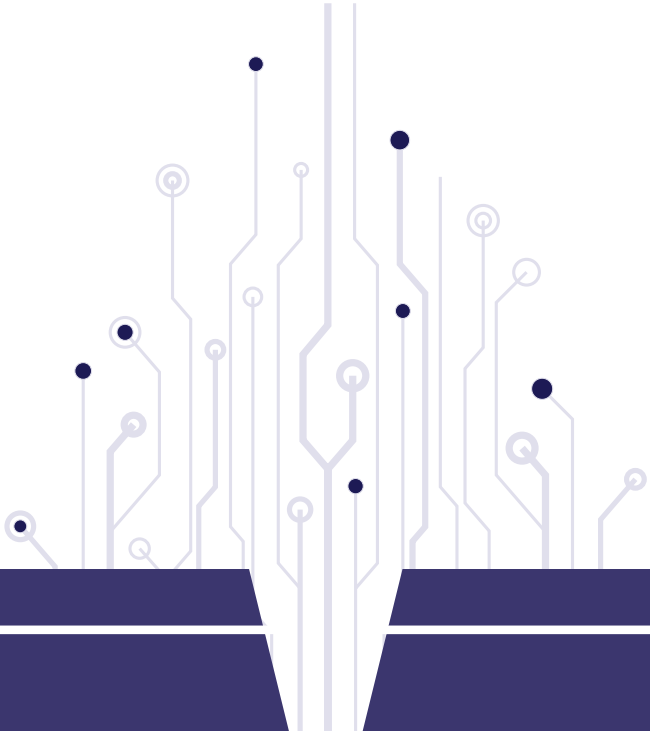
En memoria
de GILMA REMOLINA REMOLINA
por todo su amor y de PEDRO JOSÉ AVENDAÑO LIZARAZO
por recibirme como un hijo en su hogar y enseñarme muchas cosas
relevantes sobre el derecho y la vida.



ÍNDICE

PRESENTACIÓN

TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES: LAS CLÁUSULAS CONTRACTUALES DE LA RED IBEROAMERICANA DE PROTECCIÓN DE DATOS (RIPD) COMO ALTERNATIVA PARA FACILITAR LA EXPORTACIÓN DE INFORMACIÓN.



El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), fue creado con la finalidad de otorgar certeza y seguridad en el cumplimiento de los derechos que tutela; es decir, el acceso a la información pública y protección de datos personales. El INAI, a través de sus obras editoriales busca implementar y promover en la sociedad la importancia del combate en contra de la opacidad y la corrupción. Es por ello que busca originar la reflexión y difusión de conocimientos útiles que beneficien la protección de los derechos de la sociedad y su relación con las instituciones públicas.

El autor de la obra, Nelson Remolina Angarita, es Doctor y especialista en Derecho Comercial de la Universidad de los Andes, Master of Laws del London School of Economics and Political Sciences y Doctor summa cum laude en Ciencias Jurídicas de la Pontificia Universidad Javeriana, Ex presidente de la Red Iberoamericana de Protección de Datos. Ganó el Premio Internacional Protección de Datos Personales de Investigación 2014, conferido por la Agencia Española de Protección de Datos (AEPD) sobre Trabajos originales e inéditos que traten acerca del derecho a la protección de datos en países iberoamericanos.

El autor se remonta a los años setenta, donde el Comité de Ministros del Consejo de Europa, expresó la importancia de buscar soluciones para proteger la privacidad de las personas en el sector privado, esto con el fin de proteger datos electrónicos que se encontraban en los bancos. Asimismo, también se emitieron recomendaciones para el sector público. Resalta el escritor que, en los años ochenta, la Cooperación y el Desarrollo Económico (OCDE), remitió las directrices que desde su postura reconocían como relevantes, en la privacidad en la transferencia de datos internacionales, surge el primer instrumento jurídico internacional para proteger a los datos personales de los ciudadanos.

En los años noventa, la Organización de las Naciones Unidas (ONU), proyectó el inicio de los ejes rectores para implementar reglamento en los archivos de los datos personales. Posteriormente el Parlamento Europeo y el Consejo de la Unión Europea, se pronunciaron por la protección de los datos de personas físicas, así como por el tratamiento y la circulación de los mismos. Para los años dos mil, en Europa se priorizó el reforzamiento de la protección de los derechos fundamentales, con respecto a la vida privada y familiar. La **Red Iberoamericana de Protección de Datos (RIPD)**, ratificó las directrices sobre la importancia y tratamiento a nivel global de datos personales para la comunidad, reiterando la necesidad para el desarrollo comercial, para facilitar el intercambio de información.

Aunado a lo anterior, la **Corte Interamericana de Derechos Humanos (CIDH)**, menciona que el Estado debe proveer mecanismos eficaces, ca-

paces de administrar y supervisar la protección de los datos personales. De aquí la importancia de la importación y exportación de los datos personales y de la responsabilidad de proteger los datos de cada país. Como sabemos la preocupación de los ciudadanos es tener plena confianza sobre la seguridad de sus datos, saber que se encuentran protegidos, por ello deben existir procedimientos de transferencias que estén regulados para den certeza de ello. Si bien la Organización para la Cooperación y el Desarrollo Económico (OCDE), resalta a través de una declaración, la importancia acerca un futuro digital fiable, sostenible que sea de relevancia para la economía mundial, por este motivo se debe contar con un orden global que implemente y contribuya con las regulaciones necesarias para facilitar la protección de datos y la privacidad en conjunto con las innovaciones y tecnologías actuales.

Ahora bien, en la actualidad, el uso de las Tecnologías de Información (TIC), ha impactado en la necesidad de adecuar los tratamientos de datos personales, para materializar la integración económica que no es más que importación y exportación de datos personales entre países. En donde solo se podrá justificar la no transferencia internacional de datos en casos de inteligencia militar, seguridad nacional y terrorismo.

Bajo ese contexto, es importante tomar en consideración que, en cumplimiento de deberes, principios y obligaciones en materia de protección de datos personales en el marco normativo de cada país, pueden existir requerimientos complementarios, como en el caso de México, que existe la obligación de comunicar el aviso de privacidad. Asimismo, nuestro país regula la transferencia internacional de datos personales bajo los artículos 65 a 71 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y artículos 36 y 37 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

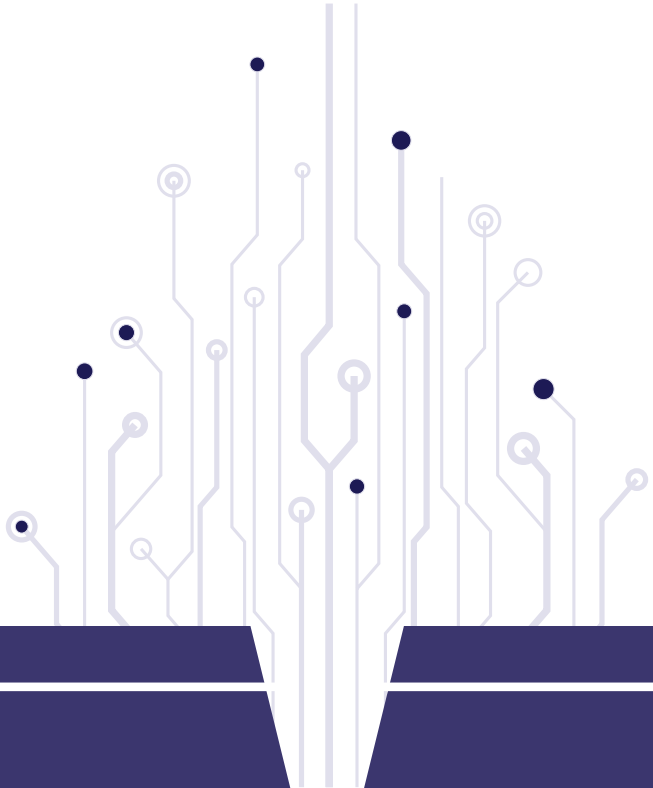
Es por ello, que las **Transferencias Internacionales de Datos Personales (TIDP)**, son los principales fundamentos de la regulación y la protección de los datos de la información que se remite a otros países. La finalidad de la **Recolección Internacional de Datos Personales (RIDP)**, conocer la regla para exportar datos de un país a otro, las disparidades nacionales impiden la correcta circulación fronteriza de la información.

Apreciados lectores, el Comité Editorial del INAI, a través de esta obra, reitera la búsqueda de temas que promuevan y difundan la importancia de la protección de datos personales. Así mismo brindar las herramientas que faciliten el uso de instrumentos que den certeza en la recolección y tratamiento de la transferencia de los datos personales.

Comité Editorial

ACERCA DEL AUTOR

NELSON REMOLINA ANGARITA



NELSON REMOLINA ANGARITA

Profesor Asociado de la Facultad de Derecho de la Universidad de los Andes (Bogotá, Colombia). Doctor -*Summa Cum Laude*- en Ciencias Jurídicas de la Pontificia Universidad Javeriana (2015). Master of Laws del London School of Economics and Political Sciences (2000). Especialista en Derecho Comercial (1995) y Abogado de la Universidad de los Andes (1994)

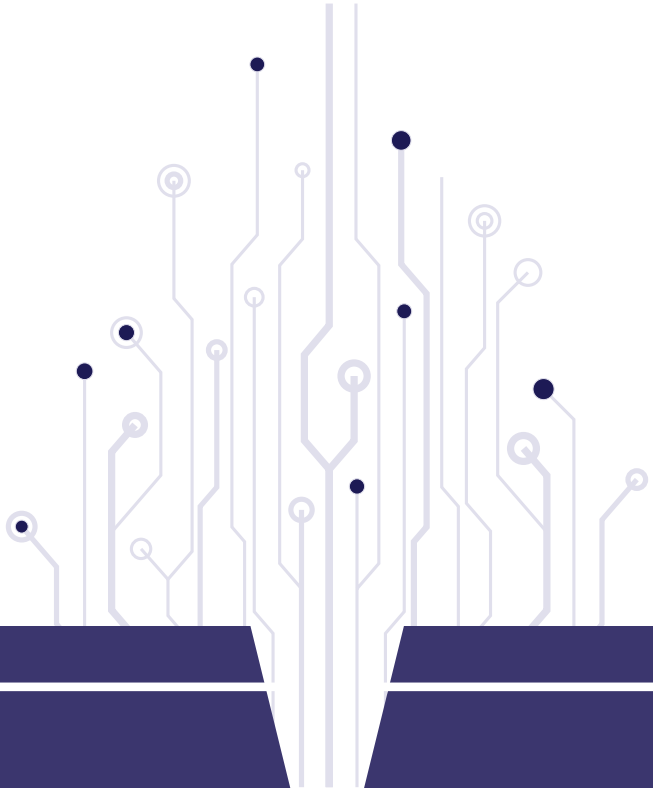
Cofundador (2001) y Director del GECTI -Grupo de Estudios en Internet, Comercio Electrónico, Telecomunicaciones & Informática"- http://gecti.uniandes.edu.co/ de la Facultad de Derecho de la Universidad de los Andes. Fundador (2008) y Director del Observatorio Ciro Angarita Barón Sobre La Protección De Datos Personales En Colombia http://habeasdata-colombia.uniandes.edu.co/.

Exsuperintendente Delegado para la protección de datos personales (octubre de 2018 – marzo 31 de 2022) de la Superintendencia de Industria y Comercio de la República de Colombia (Autoridad colombiana de protección de datos personales).

Ganador del *Premio Internacional Protección de Datos Personales de Investigación 2014*, conferido por la Agencia Española de Protección de Datos (AEPD) sobre trabajos originales e inéditos que traten acerca del derecho a la protección de datos en países iberoamericanos.

Autor y coautor de libros, artículos y diversas publicaciones sobre protección de datos personales, inteligencia artificial, neuroderechos, accountability, desmaterialización de títulos valores e instrumentos financieros y comercio electrónico. Conferencista nacional e internacional sobre dichos temas.

INTRODUCCIÓN



La Corte Interamericana de Derechos Humanos (CIDH) expresamente reconoció en octubre de 2023 la autodeterminación informativa como un derecho humano autónomo de obligatorio respeto y cumplimiento en el sistema interamericano de derechos humanos. En efecto, en la sentencia Serie C No. 506 de 18 de octubre de 2023 concluyó la CIDH:

> "586. A juicio de la Corte Interamericana, los elementos anteriores dan configuración a **un derecho humano autónomo: el derecho a la autodeterminación informativa**, reconocido en distintos ordenamientos jurídicos de la región 743, y que encuentra acogida en el contenido tutelar de la Convención Americana, en particular a partir de los derechos recogidos en los artículos 11 y 13, y, en la dimensión de su protección jurisdiccional, en el derecho que garantiza el artículo 25"[1].
>
> "588. En definitiva, **se trata de un derecho autónomo que sirve, a su vez, de garantía de otros derechos**, como los concernientes a la privacidad, a la protección de la honra, a la salvaguarda de la reputación y, en general, a la dignidad de la persona. Es preciso acotar que el derecho alcanza, con las limitaciones aplicables (infra párrs. 601 a 608), **a cualquier dato de carácter personal en poder de todo órgano público, y opera igualmente respecto de registros o bases de datos a cargo de particulares**, cuestiones sobre las que no se ahonda en razón del objeto de este proceso internacional"[2].

Se trata de un fallo icónico de enorme relevancia en el sistema interamericano de derechos humanos porque, entre otras cuestiones, impone deberes a los Estados y abre las puertas para que el mismo sea garantizado por tribunales de justicia internacionales.

1 Cfr. Corte Interamericana de Derechos Humanos Sentencia de 18 de octubre de 2023. Serie C No. 506. El texto oficial de la sentencia puede consultarse en: https://jurisprudencia.corteidh.or.cr/vid/953775991
2 Cfr. Corte Interamericana de Derechos Humanos Sentencia de 18 de octubre de 2023. Serie C No. 506. El texto oficial de la sentencia puede consultarse en: https://jurisprudencia.corteidh.or.cr/vid/953775991

Adoptar mecanismos para garantizar en la práctica (no en el papel o en la teoría) es, precisamente, uno de los deberes que deben cumplir los Estados tal y como se deriva de lo siguiente que enfatiza la CIDH:

> 599. En todo caso, la Corte Interamericana reitera que **la efectividad del derecho a la autodeterminación informativa exige que los Estados prevean mecanismos o procedimientos adecuados, ágiles, gratuitos y eficaces para dar trámite y atender, por parte de la misma autoridad que administra los datos o por otra institución competente en materia de protección de datos personales o de supervisión** (supra párr. 582)755, (...) **Esta exigencia, derivada del deber que establece el artículo 2 de la Convención Americana**, en cuanto abarca la expedición de normas y el desarrollo de prácticas conducentes a la observancia de los derechos humanos 757, incluidos procedimientos administrativos apropiados, constituye una garantía esencial para hacer valer y ejercer el derecho."[3].

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. Frente a la preocupación internacional de los Estados cuando los datos de sus ciudadanos circulan a través de sus fronteras, se ha establecido como regla general que no se deben enviar datos a países que no garanticen un nivel adecuado de protección.

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.

3 Cfr. Corte Interamericana de Derechos Humanos Sentencia de 18 de octubre de 2023. Serie C No. 506. El texto oficial de la sentencia puede consultarse en: https://jurisprudencia.corteidh.or.cr/vid/953775991

A finales de diciembre de 2022 la Organización para la Cooperación y el Desarrollo Económico (OCDE) emitió la Declaración sobre un futuro digital fiable, sostenible[4] en la cual se resalta, entre otros temas, "las conclusiones del Proyecto horizontal de la OCDE sobre gobernanza de datos para el crecimiento y el bienestar (fase III de Going Digital), que reconocen la importancia de los datos como motor de la economía mundial,(..)."

Dicha organización se comprometió a trabajar para, entre otras acciones: a) "Impulsar una transformación digital centrada en el ser humano y que promueva los derechos humanos, tanto en línea como fuera de ella, así como una sólida protección de los datos personales, leyes y normativas adecuadas a la era digital, y un uso fiable, seguro, responsable y sostenible de las tecnologías digitales emergentes y la inteligencia artificial." b) "Garantizar el bienestar de los consumidores capacitándolos para tomar decisiones informadas en el entorno digital y protegiéndolos de las prácticas comerciales engañosas, manipuladoras, fraudulentas, ilícitas y desleales, así como de los bienes y servicios inseguros"[5].

El 23 de enero de 2023, el Parlamento Europeo, el Consejo y la Comisión, por su parte, aprobaron la Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital[6]. Allí, en el CAPÍTULO III -titulado Libertad de elección- y bajo el subtítulo de "Un entorno digital justo" se comprometieron , entre otros puntos, a lo siguiente: " a) velar por un entorno digital seguro y protegido, basado en la competencia leal, en el que los derechos fundamentales estén protegidos, los derechos de los usuarios y la protección de los consumidores en el mercado único digital estén garantizados y las responsabilidades de las plataformas, especialmente los

4 Cfr. OCDE (2022) Declaration on a Trusted, Sustainable and Inclusive Digital Future. La declaración fue fruto de la reunión que se realizó en la Isla Gran Canaria (España) el 14-15 diciembre de 2022. El texto oficial puede consultarse en: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0488

5 Ídem.

6 Cfr. El Parlamento Europeo, el Consejo y la Comisión (2023) Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital (2023/C 23/01). Publicada el 23 de enero de 2023 en el Diario Oficial de la Unión Europea. El texto oficial se puede consultar en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=OJ%3AJOC_2023_023_R_0001

grandes operadores y los guardianes de acceso, estén bien definidas; (...)".

La Global Privacy Assembly (GPA), por su parte, adoptó en octubre de 2023 la resolución "Achieving global data protection standards: Principles to ensure high levels of data protection and privacy worldwide" mediante la cual se insiste en una idea de hace décadas: contar con estándares globales con respecto a la protección de datos y la privacidad. Para ello, promovió en la declaración algunos principios, derechos y otros elementos como importantes para lograr altos estándares de protección de los citados derechos. En dicho, la GPA resolvió lo siguiente:[7]

- Abogar por, promulgar y promover los principios, derechos y otros elementos establecidos en esa resolución, para garantizar que puedan implementarse y aplicarse efectivamente en todos los contextos, particularmente en el procesamiento de datos con tecnologías e innovaciones nuevas y emergentes; y
- Solicitar a los legisladores y formuladores de políticas que consulten a las autoridades de protección de datos y privacidad como asesores expertos confiables al promulgar y modificar leyes de protección de datos, privacidad y leyes relacionadas.

En ese documento, GPA enfatizó la "importancia de brindar protección de datos personales a través de fronteras con una variedad de mecanismos de transferencia, como adecuación, cláusulas modelo, certificaciones y acuerdos adminis-

7 Lo anterior es parte de una traducción libre del autor del siguiente texto oficial en inglés: "The 45th Global Privacy Assembly therefore resolves to:

• Advocate for, promulgate and promote the principles, rights and other elements set out in this resolution, to ensure they can be effectively implemented and applied in all contexts, particularly in the processing of data with new and emerging technologies and innovations; and

• Call on law and policy makers to consult data protection and privacy authorities as trusted expert advisers when enacting and amending data protection, privacy and related laws".

Tomado de: Global Privacy Assembly (GPA). 45th Closed Session of the Global Privacy Assembly. October 2023. Achieving global data protection standards: Principles to ensure high levels of data protection and privacy worldwide. Pág 9. En: https://globalprivacyassembly.org/document-archive/adopted-resolutions/

trativos, para garantizar que la protección de los datos "viaje" con dicha información cuando la misma circula a través de las fronteras" y destacó "los beneficios de aprovechar los puntos comunes, las complementariedades y los elementos de convergencia para fomentar la interoperabilidad futura entre los enfoques y mecanismos regulatorios existentes que permitan flujos de datos transfronterizos seguros y confiables"[8].

La transferencia de información entre países con diferentes culturas jurídicas es una realidad que tiende a continuar creciendo a medida que se incrementan las relaciones sociales y económicas junto con el aumento de usuarios de internet y la inmersión masiva de las TIC en el mundo[9]. Vivimos en una sociedad globalizada e interconectada tecnológicamente en donde internet ha facilitado significativamente las posibilidades de intercambio de información[10].

Los aspectos jurídicos y económicos son dos dimensiones[11] o facetas[12] de la globalización que han sido impactadas

---

8 Lo anterior es parte de una traducción libre del autor del siguiente texto oficial en inglés:
"13. International transfers of personal data.
We emphasize the importance of providing for the protection of personal data across borders with a range of transfer mechanisms, such as adequacy, model clauses, certifications and administrative arrangements, to ensure that protection travels with the data. We note the benefits of building on commonalities, complementarities and elements of convergence in order to foster future interoperability between existing regulatory approaches and mechanisms enabling safe, trustworthy cross border data flows". Tomado de: Global Privacy Assembly (GPA). 45th Closed Session of the Global Privacy Assembly October 2023 Achieving global data protection standards: Principles to ensure high levels of data protection and privacy worldwide. En: https://globalprivacyassembly.org/document-archive/adopted-resolutions/

9 En 1980 la OCDE reconocía que la circulación de datos "se ha incrementado en gran medida en años recientes y que van a aumentarse aún más con la introducción generalizada de nuevas tecnologías de informática y de comunicaciones" (Parte tomada del prólogo del siguiente documento: OCDE. 1980. Recomendación del Consejo relativa a las directrices que rigen la protección de la intimidad y de la circulación transfronteriza de datos personales).

10 Cfr. DE TERWANGNE, Cécile. 2009. *Isa Global Data Protection Regulatory Model Possible?*, en Reinventing data protection?, editado por S. GUTWIRTH. Netherlands: Springer. P. 177. Esta autora denomina nuestra sociedad como "the globalized and networked society".

11 Según Bonilla, "Teubner defiende la idea de una globalización policéntrica que está compuesta por dimensiones culturales, jurídicas, sociales, políticas y económicas que interactúan y se transforman continuamente" (BONILLA MALDONADO, Daniel. 2010. *Estado-nación y globalización: soberanía absoluta, soberanía porosa y soberanía vacía. En Estado, soberanía y globalización*. Bogotá: Siglo del Hombre Editores, Universidad de los Andes y Pontificia Universidad Javeriana - Instituto Pensar, p 15-16).

12 En similar sentido a lo mencionado en la nota anterior, otros autores han señalado que la globalización es una realidad plurifacética [RODRÍGUEZ BENOT, Andrés. 2003. *La influencia de la globalización en la elaboración, aplicación e interpretación del sistema de derecho internacional privado: especial referencia al comercio electrónico y a la contratación internacional*. En Globalización y derecho, editado por A. L. Calvo Caravaca. Madrid: Editorial COLEX. p. 508].

por el uso de las TIC (tecnologías de información y comunicación) y la necesidad del tratamiento de datos personales. Afirma Rincón que "la globalización ha sido, sin lugar a duda, uno de los fenómenos que durante el último siglo más ha influido en la evolución de nuestros sistemas jurídicos y que con seguridad determinará el curso de su evolución en este siglo que comienza"[13]. Lo anterior puede constatarse, entre otros testimonios, con lo sucedido respecto de las regulaciones sobre las transferencias internacionales de datos personales necesarias para materializar la integración económica.

Los procesos de integración económica exponen la necesidad de exportar e importar[14] datos personales entre las empresas privadas, las personas o las autoridades de los diferentes países. De hecho, se ha reconocido que estos procesos han aumentado significativamente los flujos transfronterizos de datos[15] y que fue necesario expedir normas sobre el tratamiento de estos para que se conciliara la protección de la privacidad y la transferencia internacional de los mismos.

Diversas son las razones por las cuales las empresas, las personas físicas y los gobiernos requieren transferir datos personales a otros países[16] o recibir esa información proveniente de otras partes del mundo. En el caso de los Estados, es recurrente justificar la transferencia internacional de datos por motivos de seguridad pública, seguridad nacional, investigaciones contra el terrorismo, labores de inteligencia militar o policial, cooperación judicial, colaboración internacional en general, protección de un interés del titular del dato, controles de inmigración, entre otros.

13 Cfr. RINCÓN SALCEDO, Javier. 2010. *La globalización y el derecho. En Realidades y tendencias del derecho en el siglo XXI*. Bogotá: Pontificia Universidad Javeriana y Editorial Temis. P 90.

14 En este sentido señala la doctrina que la globalización de las actividades económicas ha intensificado los procesos transfronterizos de intercambio y circulación de información. [DE TERWANGNE, op. cit., p. 17.]

15 Cfr. Numeral 4 de los considerandos de la Directiva 95/46/CE.

16 Sobre diversos aspectos de las transferencias internacionales de datos, véase entre otros: ACED FELEZ, Emilio. 2005. T*ransferencias internacionales de datos. En Protección de datos de carácter personal en Iberoamérica*, editado por José Luis Piñar. Valencia: Tirant Lo Blanch; BARCELÓ, Rosa. PÉREZ ASINARI, María Verónica. 2008. *Transferencia internacional de datos personales. En Protección de datos. Comentarios al Reglamento de desarrollo de la LOPD.* Valencia, España: Tirant Lo Blanch.; PALAZZI, Pablo. 2003. *Comercio electrónico, transferencia internacional de datos personales y armonización de leyes en un mundo globalizado*. En Derecho de internet & telecomunicaciones, editado por GECTI. Bogotá: Legis.

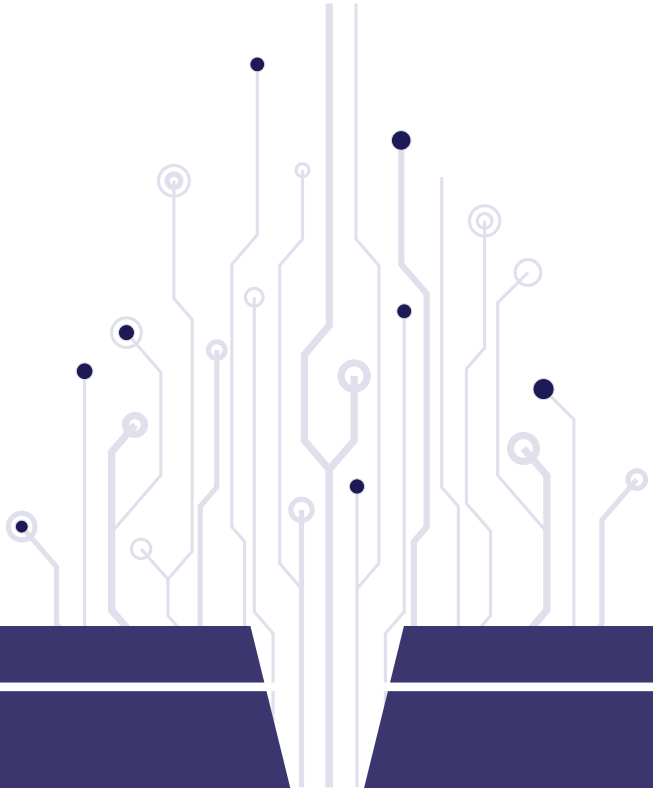
En el plano empresarial, las multinacionales requieren circular información entre las diferentes sucursales o establecimientos que poseen a lo largo del planeta[17]. Otras empresas necesitan de la misma para brindar atención telefónica a los clientes a través de call centers internacionales, realizar acciones de marketing, administrar, proveer y dar soporte técnico a las bases de datos de clientes y proveedores, tener un perfil lo más completo posible sobre un potencial cliente[18] y realizar procesos de big data.

El valor y la utilidad de los datos personales dependen, en muchos casos, de su posibilidad de circulación internacional en la medida que puedan ser entregados o remitidos a terceros para diversos propósitos. Una de las situaciones originarias que abordaron las normas sobre tratamiento de datos personales fue la transferencia de naturaleza transfronteriza o internacional. Se establecieron pautas para permitir que los datos tratados en un país pudieran ser enviados a otro. Este es uno de los tópicos centrales del contexto internacional sobre la materia que analizaremos a continuación.

17 Sobre la necesidad de exportar información para diferentes fines véase: PÉREZ ASINARI, María Verónica. 2003. *The WTO and the Protection of Personal Data. Do EU Measures Fall within GATS Exception? Which Future for Data Protection within the WTO e-commerce Context?*. Conferencia presentada en el 18th BILETA Conference: Controlling Information in the Online Environment. Londres, Reino Unido: Queen Mary & Westfield College, University of London.

18 La gran mayoría de los ejemplos fueron tomados de la presentación titulada "*Globalización de la privacidad: hacía unos estándares comunes -transferencias internacionales de datos*"de María José BLANCO, Subdirectora General del Registro General de Protección de Datos de la Agencia Española de Protección de Datos. La conferencia tuvo lugar durante el VI encuentro Iberoamericano de protección de datos realizado en Cartagena de Indias (Colombia) del 27 al 30 de mayo de 2008.

DEL CIBERESPACIO Y LOS DATOS PERSONALES



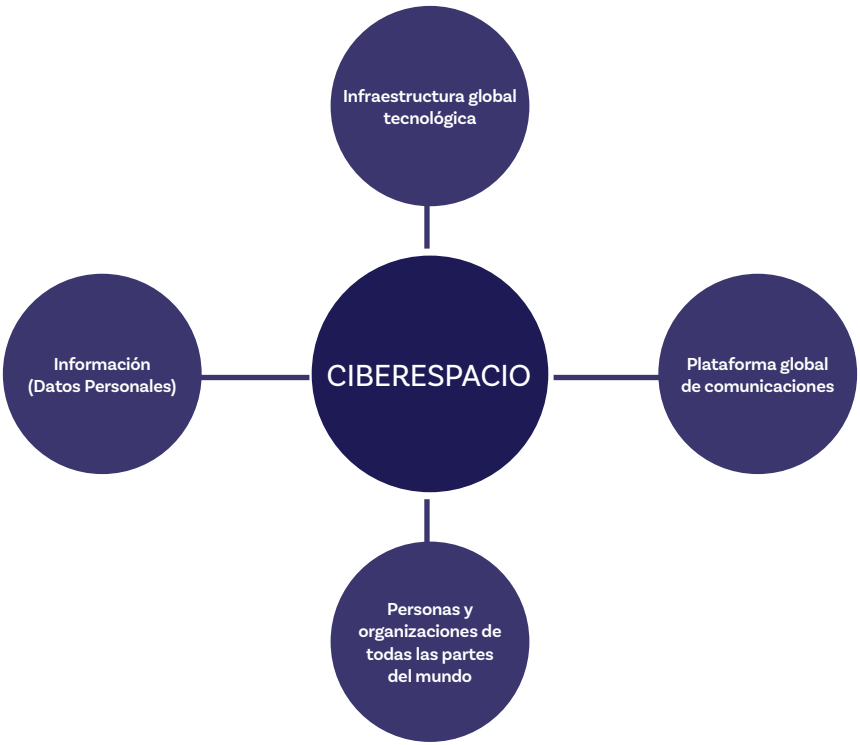
Los datos personales circulan diariamente en el ciberespacio. No obstante, la regulación sobre el tratamiento de datos surgió en un escenario en donde aún no se hablaba del ciberespacio. En otras palabras, la realidad socio tecnológica actual no era la que existía cuando se emitieron las primeras regulaciones sobre protección de datos personales.

Al margen de lo anterior, la información (y los datos personales) son una pieza clave e imprescindible del ciberespacio. Aunque existen diferentes acepciones sobre el ciberespacio, consideramos relevante tener presente que el mismo está integrado por los siguientes elementos:[19]

- Una infraestructura tecnológica (elementos como el hardware, el software, y los diferentes servicios que hacen falta para optimizar la gestión interna y la seguridad de la información para el almacenamiento de los datos) conformada por un sinnúmero de equipos (servidores, computadoras, teléfonos móviles, tabletas, entre otros) que se encuentran ubicados en muchas partes del mundo.
- Una plataforma de comunicaciones (red global de comunicaciones), información y redes interconectadas (internet) de alcance mundial denominada "infraestructura global de información"[20].
- Millones de personas y organizaciones de diversas nacionalidades, domiciliadas en países con sistemas jurídicos disímiles que desde cualquier parte del mundo hacen uso de la tecnología, las comunicaciones y la información para interactuar con otras personas o utilizar los servicios disponibles en internet.
- Enormes cantidades de información (incluidos los datos personales) que circulan de manera permanente local y transfronterizamente.

19 Sobre algunas características del ciberespacio y los retos que genera al Derecho véase: JOHNSON, David y POST, David. 1995-1996. *Law and borders: the rise of law in cyberspace*. Stanford Law Review 48:1367-1402.
20 Reidenberg se refiere a ella como "the global information infrastructure -GII-" (REIDENBERG, Joel R. 1996. Governing networks and cyberspace rule-making. Emory Law Journal 45. p. 912).

Lo anterior puede graficarse de la siguiente manera:



Gráfica 1. Elementos del ciberespacio. Elaboración del autor.

Poco a poco somos testigos de la migración del mundo físico y fronterizo al ciberespacio tecnológico y sin fronteras geográficas.[21] Vivimos en un planeta fraccionado en territorios cuyas actividades se rigen en su mayoría por regulaciones nacionales y autoridades con competencia territorial[22] (no transfronteriza). Al mismo tiempo, somos testigos de un proceso de erosión y desintegración de las fronteras territoriales y de la aparición de un

21 Para la redacción de este apartado sobre el ciberespacio se tomaron fragmentos de los siguientes libros del autor de esta obra: **(1)** *Recolección internacional de datos: un reto del mundo postinternet.* BOE - Boletín Oficial del Estado. Madrid, España, abril de 2015. ISBN 978-84-340-2196-9. **(2)** *Tratamiento de datos personales. Aproximación internacional y comentarios a la ley 1581 de 2012* (Ed Legis. Bogotá, noviembre de 2013). ISBN: 978-958-767-086-8, y **(3)** *De la responsabilidad demostrada en las funciones misionales de la Registraduría Nacional del Estado Civil: hacia un programa de gestión de datos personales y la consolidación de un buen gobierno corporativo en el tratamiento de esa información* (2018). Ed Temis. ISBN: 978-958-35-1183-7 (Coautoría con Gustavo Quintero y Manuel Tenorio).

22 Puede afirmarse que el mundo jurídico actualmente es una amalgama de: **(I)** reguladores locales con campo de acción definido por un territorio; **(II)** regulación fundada en bases territoriales; y **(III)** soluciones de controversias normalmente a cargo de jueces o autoridades con competencia delimitada por un territorio.

espacio de enorme magnitud donde aumenta progresivamente el número de personas que interactúan en el ciberespacio.

El mundo es, entre otras acepciones, un gran territorio delimitado por fronteras físicas, dentro de las cuales viven personas sujetas a normas jurídicas locales (territoriales) y autoridades de la misma naturaleza. Unas y otras hacen parte del marco jurídico nacional vinculante a los sujetos dentro de determinado espacio. En este contexto, el ámbito de aplicación de las normas, las autoridades, así como la competencia jurídica de éstas, los efectos de sus decisiones y los mecanismos de solución de controversias fueron creados por los reguladores de un territorio para ser aplicados en ese territorio[23]. Tratándose de ciertas cuestiones transfronterizas se ha procurado dar respuesta a las mismas mediante las reglas del derecho internacional. Ese ha sido, grosso modo, el escenario jurídico en que hemos vivido durante varios siglos.

Si aplicamos lo anterior a la arena del derecho, al debido tratamiento de datos personales encontramos el siguiente escenario: varios países tienen normas generales y locales obligatorias en relación con los tratamientos que se realizan en cada uno de sus territorios. El ámbito de aplicación es definido, normalmente, en las normas locales sobre TDP (Tratamiento de Datos Personales). Para hacer cumplir dichas normas crearon autoridades nacionales de protección de datos cuya competencia es territorial.

Actualmente no contamos con un instrumento jurídico internacional sobre TDP que sea vinculante a todos los países. Sólo existe un convenio internacional regional vinculante, en materia de protección de datos, aplicable a los países europeos. El punto para determinar es, si dichas reglas e instituciones, nacionales e internacionales, son suficientes, pertinentes y eficientes para dar respuesta a los retos que cada día se evidencian en un mundo denominado “ciberespacio”, en donde

23 En este sentido véase: REIDENBERG, Joel R. 1996. *Governing networks and cyberspace rule-making.* Emory Law Journal 45. p. 914.

las actividades pueden involucrar personas provenientes de diversos sistemas jurídicos y/o áreas geopolíticas del mundo. En el ciberespacio los límites geográficos no son barreras para interactuar y las actividades pueden tener lugar sin necesidad de tener contacto físico-territorial.

En ausencia de una definición jurídica, oficial o unívoca sobre lo que debe entenderse por ciberespacio, encontramos diversas referencias para tener una idea de qué se trata. En el Diccionario de la Real Academia Española se incluyó la palabra "ciberespacio" para hacer referencia a un "ámbito artificial creado por medios informáticos". Destacamos de lo anterior, la connotación inmaterial y artificial que desde un principio se ha asociado al ciberespacio para contrastarlo con las actividades materiales y reales que acontecen en el mundo territorial y, especialmente, antes del surgimiento de internet.

Para el Profesor Lessig, el ciberespacio hace alusión a una "nueva sociedad" que surgió en los países occidentales en la "mitad de la década de los años noventa", en un principio en "las universidades y centros de investigación" y luego en la sociedad en general. Internet es esa nueva sociedad a la que se refiere dicho autor, la cual gira en torno a una "estructura abierta y de finalidad múltiple de las redes basadas en la transferencia de paquetes de datos (...) en la que cada persona podría ejercer como su propio redactor-jefe y publicar lo que desease"[24].

El ciberespacio ha sido caracterizado por ser un escenario global no delimitado por fronteras geográficas[25] en donde las actividades suceden dentro de la arquitectura tecnológica de Internet que, como vimos, está en plena eclosión de crecimiento desde la perspectiva del número de usuarios. Acá no existe un espacio físico definido (como nuestra casa o el territorio de nuestro país) sino un campo artificial o virtual e indeterminado en

24 Las expresiones y frases entre comillas son tomadas de: LESSIG, Lawrence. 2001. *El código y otras leyes del ciberespacio*. Traducción de E. Alberola, Colección taurusesdigital. Madrid, España: Grupo Santillana de Ediciones S.A. p. 21. Este mismo autor previamente analizó otros aspectos sobre el ciberespacio en: LESSIG, Lawrence. 1996. *The zones of cyberspace*. Stanford Law Review 48:1403-1411.

25 Cfr. GILDEN, Michael. 2000. *Jurisdiction and the internet: the real world meets cyberspace*. ILSA Journal of International & Comparative Law 7 (1). P 150

donde las personas interactúan. En palabras del citado profesor, "las personas se ´conectan´ a estos espacios virtuales y actúan en ellos"[26]. Buena parte de esas actuaciones en el mundo virtual tienen implicaciones y consecuencias jurídicas en el mundo real.

En suma, el ciberespacio hace alusión a un escenario tecnológico e intangible - en contraposición al mundo territorial o físico- en donde tienen lugar una serie de acontecimientos que afectan cotidianamente a las personas, las empresas y los Estados. Aunque se trata de un "mundo virtual", sus ciudadanos son miles de millones de personas reales ubicadas en prácticamente cualquier lugar del "mundo físico" cuyas actividades tienen impacto o consecuencias en el "mundo real"[27].

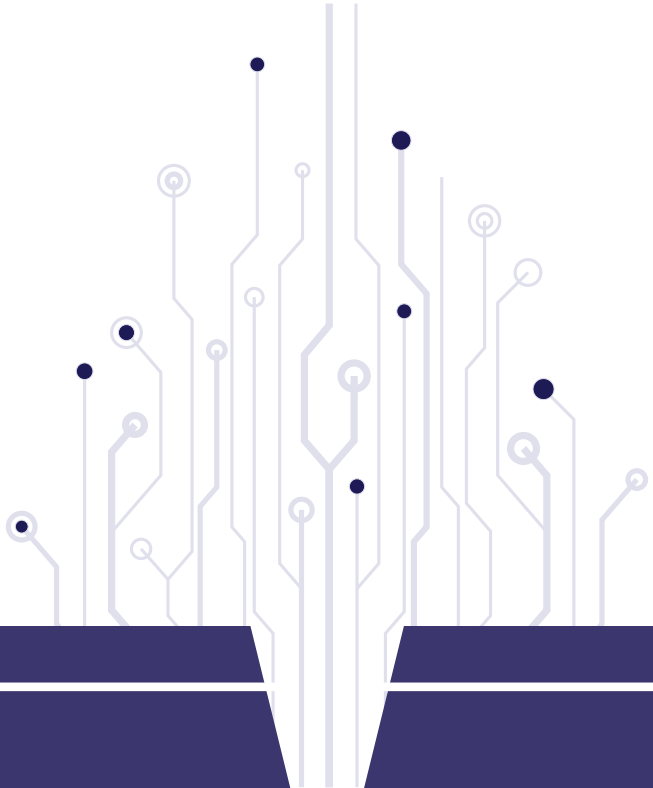
Si bien las actividades en internet tienen, en parte, vocación de ser transfronterizas, ello no significa que las fronteras físicas que demarcan los límites geográficos de los Estados hayan desaparecido. Dichas fronteras siguen existiendo, aunque en la práctica la tecnología permite que se realicen muchas actividades sin que las autoridades locales puedan evitarlo o tratar de controlarlo como lo hacen, por el ejemplo, en el caso de la inmigración de personas o en los controles de aduanas de mercancías que circulan de un país a otro.

Es transfronteriza en la medida que cualquier actividad en internet puede involucrar el uso de una red tecnológica cuyos componentes están distribuidos en lugares físicos establecidos en muchas partes del mundo. También es transfronterizo porque, supone que un sujeto desde cualquier parte del mundo realiza actividades que afectan a los sujetos ubicados en otro y otros países del mundo. En internet, lo que sucede en un país (por ejemplo, el país del recolector internacional) puede afectar a personas ubicadas en otros países (como el titular del dato ubicado en un país diferente al del recolector).

26 Cfr. LESSIG, 2001, op. cit. p. 35.

27 De hecho, autores como Baronti, han afirmado que el ciberespacio es en última "una proyección simbólica del mundo real" (Cfr. BARONTI, Hugo. 2014. *¿Qué es el ciberespacio?*). En: http://baronti.net/textos/292-¿que-es-el-ciberespacio.html (Última consulta: octubre 22 de 2014).

CONTEXTO INTERNACIONAL DE LA CIRCULACIÓN TRANSFRONTERIZA DE DATOS



Las transferencias internacionales de datos personales (en adelante TIDP) fueron una de las principales razones que motivaron la regulación sobre tratamiento de datos personales. En otras palabras, las transferencias internacionales de datos forman parte del ¿qué? y del ¿por qué? se querían regular y armonizar ciertas cuestiones. Más allá de conocer la razón de regular las TIDP resulta pertinente analizar el ¿cómo? dichas regulaciones procuran proteger los derechos de los titulares de los datos cuando su información se remite a otros países.

Es trascendente determinar lo anterior para poder establecer si las herramientas regulatorias previstas para las TIDP son útiles en el caso de la recolección internacional de datos personales (en adelante RIDP). En otras palabras, es importante establecer las reglas para exportar datos de un país a otro con miras a determinar si las mismas pueden reproducirse en el caso de la recolección de datos desde otro país. De ser así, las reglas sobre TIDP podrían ser una buena práctica[28] que sería conveniente replicar al caso de la RIDP. Previo a lo anterior, nos parece pertinente recalcar que las transferencias internacionales junto con la privacidad fueron los principales motivos que dieron origen a la regulación sobre tratamiento de datos personales, como veremos a continuación:

28 La expresión "buena práctica" usualmente se refiere a experiencias que han producido resultados positivos, demostrando su eficacia y utilidad en un contexto concreto. Señala Beatriz Boza que una buena práctica es "una actividad o proceso que ha producido destacados resultados en el manejo de una organización y que puede ser replicada en otras organizaciones para mejorar la efectividad, eficiencia e innovación de las mismas" [BOZA, Beatriz. 2004. *Acceso a la información del Estado: marco legal y buenas prácticas*. Lima, Perú: Konrad Adenauer Stiftung. p. 71].
No obstante, señala el International Bureau of Education (IBE) de la UNESCO que definir el concepto de "buena práctica" no es fácil, pues este concepto se aplica en varios contextos. "Se puede considerar que las "buenas prácticas" corresponden a casos en los cuales los procesos y comportamientos han obtenido resultados positivos, es decir, que las "buenas prácticas" son comparables a las "mejores prácticas". Otros definen una "buena práctica" de manera más general, "considerándola como un enfoque que frecuentemente es innovador, que ha sido probado y evaluado y que tiende a tener éxito en otros contextos. Una buena práctica es la innovación que permite mejorar el presente y por lo tanto es o puede ser un modelo o norma para determinado sistema". Publicado en: http://www.ibe.unesco.org/Spanish/AIDS/BPractices/BPratiques_home.htm

TRANSFERENCIAS INTERNACIONALES DE DATOS Y PRIVACIDAD COMO MOTORES DE LA ARMONIZACIÓN REGULATORIA SOBRE TRATAMIENTO DE DATOS PERSONALES

El tratamiento de datos personales se ha caracterizado por su internacionalidad, gracias al carácter transfronterizo de buena parte de su recolección, uso y circulación. Las TIC han facilitado que las actividades comerciales y el tratamiento de datos tiendan a ser transnacionales. En efecto, quien utiliza una página electrónica en Internet puede llegar a personas de cualquier parte del mundo y le da a su actividad connotaciones de alcance internacional. A su vez, también podría recolectar datos de las personas que visitan su página web.

La naturaleza global, internacional y transfronteriza de muchas actividades como, entre otras, el comercio electrónico realizado a través de Internet[29] ha sido un elemento determinante de la necesidad de contar con una regulación apropiada. El uso de las TIC en las actividades comerciales cuestiona la función y la eficacia de las instituciones de ámbito de aplicación local en el comercio internacional y contribuye a acelerar el fenómeno de la globalización[30].

El comercio internacional y el comercio electrónico requieren de la circulación global de datos personales[31]. En adición a la libre circulación de mercancías, personas y capitales, el tráfico de datos personales entre Estados es un insumo importante para el funcionamiento del mercado y el éxito de varios negocios. Las disparidades entre legislaciones nacionales sobre

29 La naturaleza global de Internet fue destacada mediante resolución del 24 de octubre de 1995 de la Federal Networking Council de los Estados Unidos, a saber: "Entendemos por Internet un sistema global de información que: **1)** Está relacionado lógicamente por un único espacio global de direcciones basado en el protocolo IP o en sus extensiones; **2)** Es capaz de soportar comunicaciones usando el conjunto de protocolos TCP/IP o sus extensiones y/o otros protocolos compatibles con IP; 3) Proporciona, usa o hace accesible, de manera pública o privada, servicios de alto nivel en capas de comunicaciones y otras infraestructuras relacionadas".

30 Un análisis de la incidencia de las tecnologías en la globalización puede consultarse en: GUIDDENS, Anthony. 2003. *Runaway world: How globalization is reshaping our lives*. New York Routledge.

31 Esto luego lo corroboraremos con lo que varias organizaciones internacionales expresan al respecto.

privacidad y tratamiento de datos personales son barreras para el desarrollo de estas actividades porque impiden la circulación transfronteriza de la información en comento.

Desde los años setenta se resaltaba la necesidad de "adoptar medidas tendentes a evitar que se originen nuevas divergencias"[32] sobre la privacidad y el tratamiento de datos entre el derecho de los países europeos. Una concepción común del derecho a la protección de datos es importante para garantizar globalmente el cumplimiento de este y eliminar barreras injustificadas para su circulación. Por eso se han promovido un conjunto de principios generales, de instituciones y de reglas especiales que progresivamente nutren y oxigenan las estructuras y el funcionamiento jurídico propio de las actividades sobre los datos personales en los ámbitos nacional e internacional. Dicho conjunto ha inspirado y ha sido el referente para la expedición de regulaciones en varios países como Colombia, tal y como lo veremos posteriormente.

Así pues, desde hace tiempo existe la tendencia de unificar o por lo menos de armonizar internacionalmente la regulación sobre tratamiento de datos personales con miras a evitar que las diferencias entre las regulaciones nacionales, los modelos de protección de datos y las tradiciones jurídicas, no se conviertan en un obstáculo[33] para su uso en el comercio internacional y a su vez se protejan adecuadamente los derechos de las personas titulares de los datos. En línea con lo anterior, la Red Iberoamericana de Protección de Datos (en adelante RIPD)

32 Cfr. Párrafo cuarto de la exposición de motivos de la Resolución (73) 22 relativa a la protección de la privacidad de las personas físicas respecto de los bancos de datos electrónicos en el sector privado expedida por el Comité de Ministros del Consejo de Europa el 26 de septiembre de 1973. El texto de la Resolución puede consultarse en: AGENCIA DE PROTECCIÓN DE DATOS, ed. 1997. *El Consejo de Europa y la protección de datos personales.* 1 ed. Madrid, España: Agencia de Protección de Datos. Págs. 31-33.

33 En efecto, en la Resolución de Estrasburgo las Autoridades de Protección de Datos y Privacidad dieron a conocer que "Las diferencias persistentes en materia de protección de datos y respeto de la privacidad en el mundo, y especialmente la ausencia de garantías en muchos Estados, perjudican los intercambios de datos personales y la puesta en práctica de una protección de datos efectiva y global". Por eso, "el desarrollo de reglas internacionales que garanticen, de un modo uniforme, el respeto a la protección de datos y a la privacidad, resulta prioritario" [AUTORIDADES DE PROTECCIÓN DE DATOS Y PRIVACIDAD. 2008. Resolución relativa a la urgente necesidad de proteger la privacidad en un mundo sin fronteras, y de alcanzar una propuesta conjunta para el establecimiento de estándares internacionales sobre privacidad y protección de datos personales].

ha manifestado que el "establecimiento de un marco armonizado de protección de datos a nivel global ha sido el principal fundamento de la adopción de los distintos instrumentos internacionales actualmente existentes en materia de protección de datos. Se trata así de garantizar que el desarrollo del comercio a nivel mundial resulte compatible con la protección de los derechos de las personas, especialmente en lo que se refiere a la protección de la información que les concierne"[34].

Las respuestas normativas mediante las TIC se caracterizan por tener enfoque internacional y ser armonizadas. Por eso, la recolección, el almacenamiento, el uso, la circulación y demás actividades sobre los datos personales han sido objeto de una labor de armonización internacional regulatoria con miras a lograr un consenso jurídico coherente sobre temas cardinales de dicha materia[35].

Durante el siglo XX se inició este proceso de armonización regulatoria internacional en donde los principales protagonistas han sido el Consejo de Europa (en adelante CE), la Organización para la Cooperación y el Desarrollo Económico (OCDE), la Organización de las Naciones Unidas (en adelante ONU), el Parlamento Europeo (en adelante PE), el Consejo de la Unión Europea (en adelante CUE). En el siglo XXI se sumaron a dicha gestión el Foro de Cooperación Económica Asia Pacífico (APEC por sus siglas en inglés), la Red Iberoamericana de Protección de Datos (en adelante RIPD) y las Autoridades de Protección de Datos y Privacidad (en adelante APDPr) que conforman hoy la Global Privacy Assembly (GPA).

34 Cfr. RED IBEROMERICANA DE PROTECCIÓN DE DATOS. 2007. *Directrices para la armonización de la protección de datos en la comunidad Iberoamericana*. p. 1. Continúa la RIPD señalando que de este modo, el establecimiento de un marco homogéneo de regulación del derecho a la protección de datos, bien mediante la adopción de instrumentos supranacionales de carácter vinculante, bien mediante la adopción de Leyes nacionales que consagren el contenido esencial de este derecho, garantizará el desarrollo del comercio en la zona, facilitando el intercambio de información entre los distintos operadores ubicados en los Estados Iberoamericanos y de éstos con terceros países, en particular los Estados miembros de la Unión Europea, en condiciones que no se vean restringidas como consecuencia del distinto nivel de protección del derecho fundamental a la protección de datos de carácter personal.

35 En la citada declaración de UE-EEUU sobre comercio electrónico se puntualizó que "el papel de los gobiernos es proporcionar un marco legal claro y consistente, promover un entorno competitivo en el que el comercio electrónico pueda florecer y asegurar la protección adecuada de objetivos de interés público como la intimidad, los derechos de propiedad intelectual, la prevención del fraude, la protección del consumidor y la seguridad nacional".

Los instrumentos de armonización utilizados por dichas organizaciones son de diversa naturaleza y efecto jurídico vinculante. Muy poco se ha recurrido a los tratados internacionales y en su lugar se han utilizado directrices, recomendaciones, principios o estándares. Independientemente de que más adelante nos refiramos a ellos, a continuación nos centraremos en establecer cuáles son los motivos que han dado origen a los mismos.

En las siguientes líneas destacaremos cronológicamente algunas cuestiones relevantes sobre los documentos más emblemáticos que han emitido el CE, la OCDE, la ONU, el PE, el CUE, el APEC, la RIPD y las APDPr o GPA sobre tratamiento de datos personales (en adelante TDP). Nuestro objetivo es establecer que, entre otros, la circulación trasfronteriza de datos es el otro gran motivo –en adición a la privacidad– de la regulación sobre tratamiento de datos personales.

Es necesario realizar varias aclaraciones sobre la revisión cronológica de fuentes primarias de información: En primer lugar, consideramos relevante tener presente las fechas de emisión de cada documento porque los mismos procuraron dar respuestas regulatorias a escenarios sociales impactados en diversos grados por las TIC. En segundo lugar, las mencionadas entidades han proferido muchos otros documentos sobre tratamiento de datos personales, no obstante en este espacio sólo consideraremos los principales textos y dentro de ellos nos enfocaremos en revisar la exposición de motivos, los considerandos o sus objetivos con miras a establecer las razones primordiales que dieron origen a los mismos. Finalmente, algunos de estos textos han sido modificados recientemente o se encuentran en período de revisión, razón por la cual nos referiremos a los mismos en lo pertinente.

PRINCIPALES DOCUMENTOS DEL SIGLO XX

La década de los años setenta marcó el inicio de la expedición de documentos sobre tratamiento de datos personales. La protección de la privacidad de las personas fue el motivo inicial que estuvo en la mira de los procesos de armonización de esa época. En efecto, el 26 de septiembre de 1973 el Comité de Ministros del Consejo de Europa expidió una resolución con recomendaciones para proteger "la vida privada de las personas físicas respecto de los bancos de datos electrónicos en el sector privado"[36] en cuyos considerandos se alertó sobre la necesidad de proteger dicho derecho frente al "desarrollo creciente de la introducción en ordenador de datos de carácter personal"[37].

El 20 de septiembre de 1974 la misma organización emitió una recomendación similar pero aplicable a los bancos de datos del sector público[38] donde se puso de relieve la importancia de proteger la privacidad respecto del tratamiento de datos por parte de las autoridades[39]. Ninguno de los documentos anteriores hizo referencia a la circulación transfronteriza de datos personales.

Entrada la década de los años ochenta las transferencias internacionales se sumaron a la privacidad como factores importantes que se querían armonizar. En efecto, el 23 de septiembre de 1980 la OCDE expidió unas directrices que desde su encabezado fueron explícitas en reconocer la protección de la intimidad y las transferencias internacionales de datos como las principales razones que motivaron la redacción de las recomendaciones de dicha organización[40]. Las directrices

36 Cfr. CONSEJO DE EUROPA, Comité de Ministros. 1973. Resolución (73) 22 relativa a la protección de la privacidad de las personas físicas respecto de los bancos de datos electrónicos en el sector privado.
37 Cfr. Párrafo quinto de la exposición de motivos de la Resolución (73) 22 relativa a la protección de la privacidad de las personas físicas respecto de los bancos de datos electrónicos en el sector privado expedida por el Comité de Ministros del Consejo de Europa el 26 de septiembre de 1973.
38 Cfr. CONSEJO DE EUROPA, Comité de Ministros. 1974. Recomendación No. R (74) 29 relativa a la protección de la vida privada de las personas físicas respecto a los bancos de datos electrónicos en el sector público.
39 El texto completo de la Recomendación No. R (74) 29 puede consultarse en: AGENCIA DE PROTECCION DE DATOS, ed. 1997. *El Consejo de Europa y la protección de datos personales*. 1 ed. Madrid, España: Agencia de Protección de Datos. p. 45-48.
40 Cfr. Organización para la Cooperación y el Desarrollo Económico, OCDE. 1980. Recomendación del Consejo relativa a las directrices que rigen la protección de la intimidad y de la circulación transfronteriza de datos personales.

mencionadas son aplicables al tratamiento de cualquier tipo de datos personales en el sector público o privado que puedan representar un peligro para la intimidad y las libertades personales[41].

Las directrices declaran la necesidad de proteger el derecho de la intimidad[42] para facilitar la transferencia internacional de datos con miras a favorecer, entre otros, el desarrollo social, económico[43] y los negocios que requieren tratar este tipo de información. El documento reconoce explícitamente que "los países miembros tienen un interés común en proteger la intimidad y las libertades individuales, y en reconciliar los valores fundamentales en oposición, tales como la intimidad y la libre circulación de información"[44].

Las directrices recalcan que el tratamiento automatizado de información facilita la circulación transfronteriza de grandes cantidades de datos, razón por la cual es necesario "considerar la protección de la intimidad en relación a los datos personales"[45] y armonizar algunos aspectos para impedir que "las disparidades en las legislaciones nacionales pudieran obstaculizar la libre circulación transfronteriza de datos personales"[46] ya que las "restricciones a esta circulación podrían

41 Cfr. Numeral 2 de las directrices de la OCDE (1980) que rigen la protección de la intimidad y de la circulación transfronteriza de datos personales. En el numeral 3 se advierte que esas "Directrices no debieran interpretarse en el sentido de que impiden: **a)** la aplicación, a diferentes categorías de datos personales, de distintas medidas de protección según su índole y el contexto en el cual se recojan, almacenen, traten o divulguen; **b)** la exclusión, respecto a la aplicación de las Directrices, de datos personales que evidentemente no contienen ningún riesgo para la intimidad ni para las libertades individuales, o **c)** la aplicación de las Directrices sólo al tratamiento automático de datos personales".

42 Dentro de los reconocimientos de las directrices se establece que "la legislación nacional relativa a la protección de la intimidad y de la circulación transfronteriza de datos personales puede obstaculizar tal circulación transfronteriza" por eso, dentro de las recomendaciones, la OCDE solicita a los Estados miembros que "procuren retirar o evitar la creación, en aras de la protección de la intimidad, los obstáculos injustificados a la circulación transfronteriza de datos personales".

43 Cfr. En la parte de reconocimientos de las directrices se indica que "la circulación transfronteriza de datos personales contribuye al desarrollo económico y social".

44 Cfr. Sección de reconocimientos de las directrices de la OCDE, 1980, op. cit.

45 Prólogo de las directrices de la OECD,1980, op. cit. Allí se señala que "los países miembros de la OCDE han considerado necesario elaborar Directrices que ayuden a armonizar la legislación nacional relativa a la intimidad y que, a la vez que defiendan tales derechos, impidan interrupciones en la circulación internacional de datos".

46 Loc. cit. En la sección de reconocimientos se establece que "el tratamiento automático y la circulación transfronteriza de datos personales crean nuevas formas de relación entre los países y precisan la elaboración de normas y prácticas compatibles".

ocasionar graves trastornos en importantes sectores de la economía, tales como la banca y los seguros"[47].

Unos meses después, el 28 de enero de 1981, el Consejo de Europa aprobó el primer instrumento jurídico internacional de carácter vinculante con miras a proteger a las personas cuando sus datos personales son tratados[48]. En la parte introductoria del Convenio, el CE no sólo reconoce "la necesidad de conciliar los valores fundamentales del respeto a la vida privada y de la libre circulación de la información entre los pueblos" sino que subraya la importancia de que sus países miembros respeten los derechos humanos y las libertades fundamentales. Dada la "intensificación de la circulación a través de las fronteras de los datos de carácter personal que son objeto de tratamientos automatizados", el CE estimó necesario "ampliar la protección" de los mismos con especial referencia al derecho a la vida privada.

En línea con lo anterior, el artículo primero estableció que el objeto del Convenio era "garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona (protección de datos)"[49]. Nótese cómo, la protección del Convenio cobija a cualquier persona sin distinción de su nacionalidad o lugar de residencia lo cual es importante porque cualquier individuo que resida fuera del territorio de las partes del Convenio puede solicitar a las mismas la protección de sus derechos.

Posteriormente, la Asamblea General de la ONU expidió el 14 de diciembre de 1990 la Resolución 45/95 mediante la cual propuso unos principios rectores para que los Estados

47 Loc. cit.

48 Cfr. CONSEJO DE EUROPA. 1981. Convenio 108 para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal.

49 Desde 2010 se inició un proceso de modernización de este Convenio para adaptarlo a los retos que genera el desarrollo tecnológico en un mundo globalizado y definir herramientas para la efectividad del mismo. Toda la información sobre esta cuestión se encuentra publicada en la página web del Consejo de Europa: http://www.coe.int/t/dghl/standardsetting/dataprotection/modernisation_en.asp

las tuviesen en cuenta a la hora de reglamentar archivos de datos personales[50]. Dicho documento no contiene una exposición de motivos en su versión oficial que nos permita determinar las razones que dieron origen a la resolución precitada[51]. No obstante lo anterior, en el contenido de la Resolución existe una disposición referente a los flujos de datos a través de sus fronteras que relacionan con la protección de la vida privada[52].

Más adelante, el Parlamento Europeo y el Consejo de la Unión Europea emitieron el 24 de octubre de 1995 la Directiva 95/46/CE[53] sobre la protección de las personas físicas cuando sus datos son objeto de tratamiento y la libre circulación de dichos datos[54]. La Directiva precisa y amplía lo dispuesto en el Convenio del 28 de enero de 1981 del Consejo de Europa[55].

En el encabezado de la Directiva sobresalen los dos principales motivos que dieron origen a la misma, a saber: la libre circulación de los datos personales y la protección de los derechos de la persona cuando sus datos son tratados Estos fueron recogidos en el artículo 1 de la Directiva al establecer como objetivos de la misma "la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales" y la no restricción ni prohibición de la "la libre circulación de datos personales entre los Estados miembros".

50 Cfr. ORGANIZACIÓN DE LAS NACIONES UNIDAS, ONU. 1990. Resolución 45/95 de la Asamblea General "Principios rectores para la reglamentación de ficheros de datos personales".

51 Sólo existen como antecedentes: la Resolución 1990/42 del 6 de marzo de 1990 de la Comisión de Derechos Humanos de la ONU y la Resolución 1990/38 del 25 de mayo de 1990 del Consejo Económico y Social de la organización en comento.

52 Cfr. Numeral 9 de la Resolución 45/95 de la Asamblea General de la ONU.

53 Aunque esta directiva se encuentra derogada, haremos referencia a la misma por su importancia histórica y pertinencia temática con este texto.

54 Cfr. PARLAMENTO EUROPEO Y CONSEJO DE LA UNIÓN EUROPEA. 1995. Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

55 Cfr. Considerando número 11 de la Directiva 95/46/CE.

En los considerandos se reconoce que las TIC facilitan enormemente el tratamiento, intercambio y circulación transfronteriza de datos personales[56] y se afirma que las diferencias regulatorias de los Estados y los disímiles niveles locales de protección de los derechos y libertades de las personas (en especial la intimidad) pueden ser un obstáculo para la transmisión de datos de un Estado a otro, lo cual tal vez sea una barrera para la realización de actividades económicas[57]. Para eliminar dichos obstáculos fue necesario regular y armonizar lo atinente al tratamiento de datos personales entre los Estados miembros con miras a alcanzar una protección equivalente en todos ellos[58].

Por otro lado, también se ponen de relieve otras cuestiones en los considerandos de la Directiva. En primer lugar, que las transferencias internacionales de datos son importantes para el desarrollo del comercio mundial[59] así como para la integración económica y social. Por eso, desde ese entonces se vaticinaba que la circulación de datos a nivel global crecería notablemente[60]. Esto que se decía en ese entonces respecto de las transferencias podría decirse hoy de la recolección internacional de datos.

En segundo lugar, se precisó que los sistemas de tratamiento de datos no solo deben "contribuir al progreso económico y social, al desarrollo de los intercambios, así como al bienestar de los individuos"[61] sino que deben "respetar las libertades y derechos fundamentales de las personas físicas y, en particular, la intimidad"[62] con independencia de la nacionalidad o residencia de estas. Finalmente, que el funcionamiento de los mercados internacionales no sólo demanda la circulación transfronteriza de datos sino la protección de los derechos de las personas[63].

56 Cfr. Considerandos número 4 y 6 de la Directiva 95/46/CE.
57 Cfr. Considerando número 7 de la Directiva 95/46/CE.
58 Cfr. Considerandos número 8 y 9 de la Directiva 95/46/CE.
59 Cfr. Considerandos número 56, 3 de la Directiva 95/46/CE.
60 Cfr. Considerando número 5 de la Directiva 95/46/CE.
61 Cfr. Considerando número 2 de la Directiva 95/46/CE.
62 Cfr. Considerando número 2 de la Directiva 95/46/CE.
63 Cfr. Considerando número 3 de la Directiva 95/46/CE.

PRINCIPALES DOCUMENTOS DEL SIGLO XXI

El 7 de diciembre del año 2000 el Parlamento Europeo, el Consejo de la Unión Europea y la Comisión Europea proclamaron la Carta de los Derechos Fundamentales de la Unión Europea[64], la cual tiene igual valor jurídico que los tratados internacionales tal y como lo señala el artículo 6 del tratado de la Unión Europea. En el preámbulo de dicho documento se destacó la necesidad de "reforzar la protección de los derechos fundamentales a tenor de la evolución de la sociedad, del progreso social y de los avances científicos y tecnológicos"[65].

En dicha Carta se consagran por separado el derecho al "respeto a la vida privada y familiar"[66] (artículo 7) y el derecho a la "protección de datos de carácter personal"[67] (artículo 8). Con lo anterior se subraya el carácter autónomo e independiente de la protección de datos frente al derecho a la intimidad.

El 8 de noviembre de 2001 el Consejo de Europa aprueba un protocolo adicional al Convenio 108 de 1981[68]. En esta ocasión, las transferencias internacionales de datos siguen siendo la gran preocupación, especialmente las que se realizan a países que no son parte del citado Convenio[69]. En el preámbulo se recalcó que frente al aumento de transferencias internacionales de datos es necesario "asegurar la efectiva protección de los derechos humanos y libertades

64 Cfr. PARLAMENTO EUROPEO, CONSEJO DE LA UNIÓN EUROPEA, COMISIÓN EUROPEA. 2000. *Carta de los derechos fundamentales de la Unión Europea.* El texto oficial fue publicado en el Diario Oficial de las Comunidades Europeas C 364/7 del 18 de diciembre de 2000.

65 En el preámbulo también se precisa que la Carta reafirma "los derechos reconocidos especialmente por las tradiciones constitucionales y las obligaciones internacionales comunes de los Estados miembros, el Tratado de la Unión Europea y los Tratados comunitarios, el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, las Cartas Sociales adoptadas por la Comunidad y por el Consejo de Europa, así como por la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas y del Tribunal Europeo de Derechos Humanos".

66 "Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones" (Artículo 7 de la Carta de los derechos fundamentales de la Unión Europea).

67 "1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.

68 CONSEJO DE EUROPA. 2001. Protocolo adicional del convenio No 108 para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal y relativo a transferencias de datos.

69 El otro tema central del protocolo fueron las autoridades de control como elemento de protección de los derechos de las personas cuando sus datos son objeto de tratamiento.

fundamentales, y, en especial, el derecho a la privacidad, en relación con tales intercambios".

El 12 de julio de 2002 el Parlamento Europeo y el Consejo de la Unión Europea emitieron una Directiva sobre privacidad y las comunicaciones electrónicas[70] cuyo objeto fue armonizar las regulaciones locales con miras a "garantizar un nivel equivalente de protección de las libertades y los derechos fundamentales y, en particular, del derecho a la intimidad y la confidencialidad, en lo que respecta al tratamiento de los datos personales en el sector de las comunicaciones electrónicas, así como la libre circulación de tales datos y de los equipos y servicios de comunicaciones electrónicas en la Comunidad"[71]. Esta directiva precisa y complementa algunas cuestiones de la Directiva 95/46/CE pero aplicadas al sector de las comunicaciones.

Dentro de los aspectos relevantes nos parece oportuno mencionar que en los considerandos se hizo referencia explícita a internet como una red mundial de comunicaciones que está revolucionando los mercados y generando nuevas alternativas a las personas y las empresas. Internet, precisa el documento, también genera nuevos riesgos respecto de la protección de los datos personales y la vida privada de los ciudadanos[72].

El Foro de Cooperación Económica Asia Pacífico (APEC por sus siglas en inglés) emitió en 2004 el Marco de Privacidad APEC (APEC Privacy Framework), el cual enfatiza sobre la necesidad de las transferencias internacionales de datos para aprovechar las posibilidades que ofrece el comercio electrónico y el comercio global. Su propósito es lograr una protección apropiada a la privacidad que permita "asegurar el libre flujo de información en la región Asia Pacífico"[73] para promover el comercio electrónico[74].

70 Cfr. PARLAMENTO EUROPEO Y CONSEJO DE LA UNIÓN EUROPEA. 2002. Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas).
71 Cfr. Artículo 1 de la Directiva 2002/58/CE.
72 Cfr. Considerando número 6 de la Directiva 2002/58/CE.
73 Cfr. Numeral 4 del Preámbulo del Marco de Privacidad APEC.
74 Cfr. Numeral 5 del Preámbulo del Marco de Privacidad APEC.

Ese documento reconoce la importancia de "desarrollar protecciones efectivas para la privacidad que eviten barreras a los flujos de información" y "asegurar el intercambio continuo y el crecimiento económico en la región APEC"[75]. Concluye el documento que, entre otros, los "sistemas reguladores que restringen innecesariamente este flujo o le imponen cargas, tienen implicaciones adversas para el comercio global y para las Economías"[76].

En el preámbulo se recalca que las TIC, "incluyendo tecnologías móviles que se conectan a Internet y a otras redes de información, han hecho posible recopilar, almacenar y acceder a la información desde cualquier parte del mundo"[77]. Señala APEC que dicho Marco de Privacidad fue elaborado para destacar la importancia de "reconocer el libre flujo de información como algo esencial para Economías de mercado desarrolladas y en desarrollo, para sustentar el crecimiento económico y social"[78] así como de "promover y hacer cumplir la privacidad de la información, y mantener la continuidad de los flujos de información entre Economías de APEC y sus socios comerciales"[79].

El 9 de noviembre de 2007 la **Red Iberoamericana de Protección de Datos (en adelante RIPD) aprobó en Lisboa unas directrices de armonización sobre tratamiento de datos personales para la comunidad Iberoamericana**[80]. Señala la RIPD que la armonización sobre tratamiento de datos a nivel global ha sido necesaria para que el desarrollo del comercio internacional sea compatible con la protección de los derechos de las personas[81].

---

75 Cfr. Prólogo del Marco de Privacidad APEC. En el mismo sentido véase el numeral 1 del preámbulo de dicho documento.

76 Cfr. Numeral 3 del Preámbulo del Marco de Privacidad APEC.

77 Cfr. Numeral 2 del Preámbulo del Marco de Privacidad APEC.

78 Cfr. Numeral 8 del Preámbulo del Marco de Privacidad APEC.

79 Cfr. Numeral 8 del Preámbulo del Marco de Privacidad APEC. Otras cuestiones importantes que se indican en el precitado numeral son: **(I)** "Desarrollar protecciones apropiadas para la información personal, particularmente contra las dañinas consecuencias de intrusiones no deseadas y del uso incorrecto de la información personal" y **(II)** "Posibilitar organizaciones globales que recopilen, accedan, usen o procesen información en Economías de APEC para desarrollar e implementar acercamientos uniformes dentro de sus organizaciones para tener acceso global y uso de la información personal".

80 Cfr. RED IBEROMERICANA DE PROTECCIÓN DE DATOS. 2007. *Directrices para la armonización de la protección de datos en la comunidad Iberoamericana.*

81 Cfr. Red Iberoamericana de Protección de Datos, 2007, op. cit., p. 1.

Con lo anterior en mente, el principal objetivo de las directrices es "ofrecer a los poderes públicos de los Estados Iberoamericanos unos criterios orientativos que puedan resultar de utilidad en el desarrollo de las iniciativas normativas que puedan adoptarse, facilitando así el establecimiento de un marco homogéneo de protección que facilite el intercambio de los flujos de información entre todos ellos y desde y hacia terceros Estados que han adoptado estándares similares de protección"[82].

El 5 de noviembre de 2009, las Autoridades de Protección de Datos y Privacidad (en adelante APDPr) aprobaron durante su trigésima primera Conferencia Internacional realizada en Madrid unos estándares para la protección de la privacidad, en relación con el tratamiento de datos de carácter personal[83] (denominada Resolución de Madrid)[84]. El antecedente inmediato de este documento tuvo lugar en octubre de 2008 durante la 30a Conferencia de las APDPr[85] realizada en Estrasburgo en donde se reiteró la necesidad de emitir un "Convenio universal para la protección de las personas con respecto al tratamiento de datos personales"[86] y se creó un Grupo de Trabajo, coordinado por la Agencia Española de Protección de Datos para que, junto con otras autoridades en la materia, elaborara una propuesta conjunta para la redacción de estándares internacionales sobre la protección de la privacidad y de los datos de carácter personal[87].

82 Cfr. Red Iberoamericana de Protección de Datos, 2007, op. cit., p. 4.
83 Cfr. AUTORIDADES DE PROTECCIÓN DE DATOS Y PRIVACIDAD. 2009. Estándares internacionales sobre protección de datos personales y privacidad (Resolución de Madrid) -Propuesta Conjunta para la Redacción de Estándares Internacionales para la protección de la Privacidad en relación con el Tratamiento de Datos de carácter personal- Madrid, España.
84 Más información sobre los antecedentes de la Resolución de Madrid puede consultarse en la página web de la Agencia Española de Protección de Datos: http://www.agpd.es/portalwebAGPD/internacional/Estandares_Internacionales/proceso-ides-idphp.php
85 Cfr. AUTORIDADES DE PROTECCIÓN DE DATOS Y PRIVACIDAD. 2008. Resolución relativa a la urgente necesidad de proteger la privacidad en un mundo sin fronteras, y de alcanzar una propuesta conjunta para el establecimiento de estándares internacionales sobre privacidad y protección de datos personales.
86 Esta es una idea que se gestó en otras Conferencias de las APDP como la declaración adoptada en Venecia (22ª Conferencia), Breslavia (26ª Conferencia), Montreux (27ª Conferencia), Londres (28ª Conferencia) y Montreal (29ª Conferencia). De hecho, en 2005 en la Declaración de Montreaux se hizo un "llamamiento a la Organización de las Naciones Unidas para la redacción de un instrumento jurídico vinculante que enuncie detalladamente el derecho a la protección de datos y a la privacidad, habida cuenta de su carácter de derecho fundamental" [Autoridades de Protección de Datos y Privacidad, 2008, op. cit.].
87 Cfr. Autoridades de Protección de Datos y Privacidad, 2008, op. cit.

El objetivo dual de la Resolución de Madrid quedó plasmado en el numeral primero de la misma en los siguientes términos: "**a.** Definir un conjunto de principios y derechos que garanticen la efectiva y uniforme protección de la privacidad a nivel internacional, en relación con el tratamiento de datos de carácter personal; y **b.** Facilitar los flujos internacionales de datos de carácter personal, necesarios en un mundo globalizado".

Como se observa, el propósito armonizador de la Resolución no sólo es evidente, sino que se mantiene la privacidad como principal derecho protegido y el tratamiento de los datos (no la protección de datos) como una actividad en la que dicho derecho puede ser afectado si la misma se realiza indebidamente. En cuanto a lo primero vale la pena mencionar que el texto se ha catalogado como un precedente muy importante para la expedición de un futuro instrumento jurídico internacional vinculante sobre tratamiento de datos[88].

La transferencia internacional de datos sigue siendo el otro gran motivo de este tipo de iniciativas. Es decir, la circulación transfronteriza de datos continúa impactando las regulaciones, aunque el contexto inicial de los años ochenta y particularmente hasta finales del siglo XX ha cambiado.

El año 2012 marcó el inicio formal de la reforma en Europa de la protección de datos[89]. En efecto, el 25 de enero

88 En efecto, Artemi Rallo, director de la Agencia Española de Protección de Datos en la época que se aprobó la Resolución de Madrid, manifiesta lo siguiente en la presentación de dicho texto: "La labor conjunta de los garantes de la privacidad de casi cincuenta países, bajo coordinación de la Agencia Española de Protección de Datos, ha desembocado en un texto que trata de plasmar los múltiples enfoques que admite la protección de este derecho, integrando legislaciones de los cinco continentes. Su carácter consensuado aporta dos valores añadidos esencialmente novedosos: de un lado, enfatiza la vocación universal de los principios y garantías que configuran este derecho; del otro, reafirma la factibilidad de avanzar hacia un documento internacionalmente vinculante, que contribuya a una mayor protección de los derechos y libertades individuales en un mundo globalizado, y por ello, caracterizado por las transferencias internacionales de información". Lo anterior se ratifica en la parte resolutiva de la 31a Conferencia de APDP en donde se dice que "La Propuesta Conjunta demuestra la viabilidad de tales estándares, como un nuevo paso hacia la elaboración, en el momento oportuno, de un instrumento internacional vinculante".

89 En la página web del Supervisor Europeo se detallan todos los aspectos sobre la reforma a la protección de datos en Europa. Particularmente se destacan los documentos que han emitido las siguientes organizaciones: El Supervisor Europeo de Protección de Datos, la Comisión Europea, el Parlamento Europeo, el Consejo de Europa, el Grupo del artículo 29 de la Directiva 95/46/CE. https://secure.edps.europa.eu/EDPSWEB/edps/Consultation/Reform_package

la Comisión Europea presentó una propuesta[90] para emitir un Reglamento[91] general sobre el derecho fundamental de la protección de las personas en relación con el tratamiento de datos personales[92]. Esta reconoce en la exposición de motivos el efecto transformador de las TIC sobre la economía y la vida social[93]. Al mismo tiempo, subraya que "la rápida evolución tecnológica ha supuesto nuevos retos para la protección de los datos personales" porque, entre otros desafíos, no sólo se ha "incrementado enormemente la magnitud del intercambio y la recogida de datos" sino que las TIC facilitan que en los sectores público y privado se "utilicen datos personales en una escala sin precedentes a la hora de desarrollar sus actividades". Adicionalmente, menciona que las personas físicas "difunden un volumen cada vez mayor de información personal a escala mundial"[94].

En la propuesta de Reglamento[95] se reconoce la vigencia

90 Cfr. COMISIÓN EUROPEA. 2012. Propuesta de reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos). (COM(2012) 11 final. 2012/0011 (COD)). La versión oficial del texto puede consultarse en http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:ES:PDF Todos los detalles sobre la propuesta pueden consultarse en la página web de la Comisión Europea http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

91 En la propuesta se explica que el Reglamento es un instrumento más favorable que las Directivas. Los reglamentos son actos legislativos directamente vinculantes en toda la UE a partir de la fecha fijada en el Diario Oficial mientras que las Directivas no son de aplicación directa sino establecen un objetivo que todos los países de la UE deben cumplir y cada país debe decidir cómo hacerlo: "la aplicabilidad directa de un reglamento, de conformidad con el artículo 288 del TFUE, reducirá la fragmentación jurídica y ofrecerá una mayor seguridad jurídica merced a la introducción de un conjunto armonizado de normas básicas, la mejora de la protección de los derechos fundamentales de las personas y la contribución al funcionamiento del mercado interior" [Cfr. Comisión Europea, 2012, op. cit.] También léase el numeral 11 de los considerandos de la propuesta.

92 En el considerando primero de la propuesta se reconoce la naturaleza de este derecho en los siguientes términos: "La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental. El artículo 8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea y el artículo 16, apartado 1, del Tratado establecen que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan".

93 En el texto de la propuesta se documentan detalladamente los principales aspectos, antecedentes, elementos jurídicos y demás información sobre la misma. [Cfr. Comisión Europea, 2012, op. cit., p. 1-18.].

94 Todas las frases citadas entre comillas son tomadas de la parte denominada "contexto de la propuesta" incluida en la exposición de motivos presentada por la Comisión Europea. Dichos aspectos señalados entre comillas también se recalcan en el considerando número 5 de la propuesta.

95 Los principales antecedentes de la propuesta fueron publicados por la Comisión Europea en su página web http://ec.europa.eu/justice/data-protection/review/actions/index_en.htm

de los motivos que dieron origen a la Directiva 95/46/CE pero se plantea la necesidad de mitigar riesgos para las personas respecto del tratamiento de sus datos en el contexto digital o las actividades en línea[96]. Y es que el contexto actual difiere del escenario existen en la época en que se gestó y expidió la Directiva 95/46/CE. En este sentido, Viviane Reding[97] sostiene que "hace 17 años, menos de un 1% de los europeos usaba Internet. Hoy en día se transfieren e intercambian enormes cantidades de datos personales entre continentes y de una punta a otra del mundo en fracciones de segundos"[98].

En síntesis, aunque el contexto tecnológico de la década de los años 90 es sustancialmente diferente al actual, la protección de los derechos y libertades de las personas (especialmente la privacidad) y la necesidad de facilitar la transferencia internacional de datos continúan siendo los principales motivos que originaron la propuesta.

La OCDE, por su parte, aprobó el 11 de julio de 2013 una versión revisada[99] de sus recomendaciones de 1980. El Working Party on Information Security and Privacy (en adelante WPISP) de la OCDE estuvo a cargo de liderar el proceso de revisión y actualización dentro del cual destacó los cambios significativos de la sociedad actual junto con el rol de los datos personales en el mercado, la sociedad y nuestra cotidianeidad respecto del escenario existente hace 30 años. Dentro de los mismos se destacaron los siguientes: i) el aumento del volumen de datos personales que son recolectados, usados y almacenados; ii) los análisis que se realizan sobre grandes cantidades de información (big data) y los usos que se dan a las conclusiones que se derivan de los mismos; iii) el valor social y económico de las TIC y el uso responsable de los datos personales; iv) el aumento de

96 Cfr. Considerando número 7 de la propuesta de Reglamento.

97 Comisaria de Justicia de la UE y Vicepresidenta de la Comisión Europea.

98 Cfr. Comunicado de prensa de la Comisión Europea titulado "La Comisión propone una reforma general de las normas de protección de datos para aumentar el control de los usuarios sobre sus propios datos y reducir los costes para las empresas" (European Commission - IP/12/46 25/01/2012) publicado el 25 de enero de 2012 en http://europa.eu/rapid/press-release_IP-12-46_es.htm

99 Cfr. Organización para la Cooperación y el Desarrollo Económico, OCDE. 2013. Recomendación del Consejo relativa a las directrices que rigen la protección de la intimidad y de la circulación transfronteriza de datos personales.

amenazas para para la privacidad; v) el número y la variedad de actores involucrados en el tratamiento de datos capaces de poner en riesgo o de proteger la privacidad; vi) la frecuencia y la complejidad de las interacciones o actividades que requieren datos personales y vii) la disponibilidad global de datos personales facilitada por redes de comunicación y plataformas tecnológicas que facilitan la transferencia de esa información a o desde muchas partes del mundo[100].

Nótese cómo la recolección de datos empieza a ser una razón explícita que la OCDE reconoce como un cambio importante, aunque no se haga mención a la captura internacional de datos por parte de personas de cualquier parte del mundo con acceso a internet. No obstante, lo anterior, los motivos de la versión de 2013 coinciden con los de las de 1980 en la medida que la OCDE sigue reconociendo el interés de dicha organización de proteger la privacidad y las libertades de las personas junto con la libre circulación global de los datos personales.

La OCDE registra en la exposición de motivos de la versión 2013 de sus recomendaciones otros aspectos pertinentes para esta investigación que resumimos a continuación: **I)** el aumento de riesgos a la privacidad junto con los grandes beneficios económicos y sociales que genera el más amplio e innovador uso de los datos personales; **II)** la necesidad de fortalecer la cooperación entre las APDP y de consolidar la interoperabilidad de los sistemas de protección de datos para facilitar la circulación transfronteriza de los mismos a través de redes globales de comunicación; **III)** Los retos a la seguridad de la información que genera un ambiente abierto, global e interconectado de tratamiento de datos.

Los principios de las directrices de 1980 se mantienen intactos[101] pero la nueva versión gira en torno a dos grandes aspectos. Por una parte, la necesidad de realizar mayores esfuerzos para abordar la dimensión global de la privacidad a través de una

100 Cfr. Organización para la Cooperación y el Desarrollo Económico, OCDE. 2013. The OCDE privacy framework: OCDE Publishing. p. 3 y 19-20.
101 Cfr. OCDE, 2013, op. cit., p. 4.

mejor interoperabilidad (*improved interoperability*) y por otra parte, el establecimiento de herramientas para alcanzar la aplicación práctica de la protección de la privacidad a través de un enfoque basado en la gestión del riesgo (*risk management*)[102].

Dentro de las novedades que reconoce la OCDE se destacan las siguientes: Necesidad de establecer e implementar estrategias nacionales de privacidad (*National privacy strategies*) coordinadas al más alto nivel gubernamental para establecer los caminos apropiados para cumplir correctamente las normas sobre privacidad y tratamiento de datos. Junto a lo anterior también son relevantes los programas de gestión de Privacidad (*Privacy management programmes*) como mecanismo operativo a través del cual las organizaciones implementan la protección de ese derecho. Finalmente, también son útiles las notificaciones de violación de la seguridad de datos (*Data security breach notification*) que se deben realizar tanto a la APDP como a la persona afectada por una falla de seguridad respecto de los datos personales[103].

Finalmente, se expidieron los siguientes documentos a los que nos referiremos posteriormente:

- REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO (27 de abril de 2016) relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
- Estándares de protección de datos personales para los países Iberoamericanos de la Red Iberoamericana de Protección de Datos[104] (RIPD) aprobados en 2017.
- El Convenio 108+ de 2018[105] para la protección de las personas con respecto al tratamiento de datos de carácter personal.

102 Loc. cit.
103 Loc. cit.
104 Estándares aprobados en el XV Encuentro de la RIPD, que tuvo lugar en Santiago de Chile, el 22 de junio de 2017.
105 Respecto del convenio 108+ o convenio 108 modernizado consulte: https://www.coe.int/es/web/data-protection/convention108/modernised

- Principios actualizados sobre la privacidad y la protección de datos personales, con anotaciones[106] expedidos el 9 de abril de 2021 por el l Comité Jurídico Interamericano (CJI), órgano consultivo de la Organización de Estados Americanos (OEA). Estos principios fueron aprobados por la Asamblea General de la OEA en noviembre de 2021.
- La Decisión Andina 897[107] del 14 de julio de 2022 de la Comunidad Andina de Naciones (CAN).

Visto lo anterior nos parece pertinente realizar algunas reflexiones en torno a la denominación y concepto de las transferencias internacionales para determinar en qué consisten y poderlas diferenciar de la recolección internacional de datos.

DENOMINACIÓN Y CONCEPTO DE LAS TIDP

En los documentos internacionales se evidencia la pluralidad terminológica y conceptual sobre las transferencias internacionales. Aunque se trata de una cuestión presente en todos ellos, existen diversos grados de desarrollo del tema. Veamos cronológicamente lo que se refleja en dichos textos teniendo en cuenta las referencias existentes en los siglos XX y XXI. Esto es importante para tener claro a qué se refiere la transferencia internacional de datos y poder diferenciarla de la recolección internacional de datos personales.

Durante el siglo XX la OCDE, el Parlamento y el Consejo Europeo así como la ONU se refirieron al tema en los siguientes términos: Inicialmente las Directrices OCDE de 1980 las denominó “circulación transfronteriza de datos personales” para hacer referencia a “los movimientos de datos personales a través de fronteras nacionales”[108]. Desde un principio se estableció la necesidad de traspasar las fronteras territoria-

106 El texto puede consultarse en: https://www.redipd.org/sites/default/files/2021-05/CJI-doc_638-21.pdf
107 Publicada en la Gaceta Oficial del Acuerdo de Cartagena No. 4499 del 14 de julio de 2022. El texto oficial está disponible en: https://www.comunidadandina.org/DocOficialesFiles/Gacetas/GACETA%204499.pdf
108 Cfr. Directrices OCDE de 1980, Literal –c– del numeral 1.

les como un requisito distintivo de las TIDP. Posteriormente, el Convenio 108 de 1981 las llamó "Flujos transfronterizos de datos de carácter personal" refiriéndose a las "transmisiones a través de las fronteras nacionales, por cualquier medio que fuere, de datos de carácter personal"[109].

Más adelante, en la Resolución 45/95 de la ONU (1990) fueron denominados "Flujo de datos a través de las fronteras"[110] sin precisar definición alguna aunque puede derivarse que dicha situación se da cuando los datos pasan los límites territoriales de un país. Finalmente, en la Directiva 95/46/CE se denominan "transferencia a un país tercero"[111] sin que exista una definición[112] que precise el alcance de dicha expresión.

En el siglo XXI el tema es abordado nuevamente en documentos y propuestas del Parlamento y el Consejo Europeo y la OCDE, pero ingresan en la escena otras organizaciones como APEC, las Autoridades de Protección de Datos, la RIPD y la CAN. El primer documento de este siglo fue el Protocolo adicional de 2001 al Convenio 108 en donde se regulan la "Transferencia de datos personales a destinatarios no sometidos a la competencia de las Partes del Convenio" para hacer referencia a la "transferencia de datos personales a un destinatario

109 Convenio 108 de 1981, artículo 12.

110 Resolución 45/95 de la ONU (1990), numeral 9.

111 Directiva 95/46/CE, Capítulo IV titulado "Transferencia de datos personales a países terceros" (artículos 25 y 26).

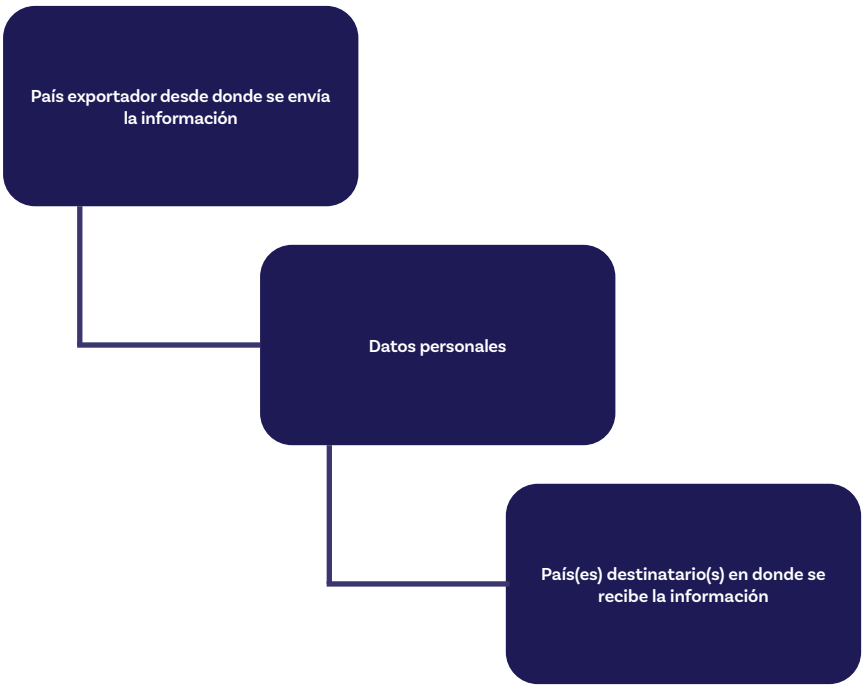
112 Esto fue reconocido por el TJUE en el siguiente caso: TRIBUNAL DE JUSTICIA DE LA UNION EUROPEA. 2003. Göta hovrätt - Suecia y Bodil Lindqvist. Asunto C-101/01. En dicha sentencia, el tribunal señala algunas cuestiones sobre la publicación de datos personales en Internet y las transferencias de datos personales a terceros países. Estos planteamientos –dice la sentencia– "se suscitaron en el marco de un proceso penal seguido ante dicho órgano jurisdiccional contra la Sra. Lindqvist, acusada de haber infringido la normativa sueca relativa a la protección de datos personales al publicar en su sitio de Internet diversos datos de carácter personal sobre varias personas que, como ella, colaboraban voluntariamente con una parroquia de la Iglesia protestante de Suecia". Estas fueron algunas de las conclusiones del TJUE: En primer lugar, "la conducta que consiste en hacer referencia, en una página web, a diversas personas y en identificarlas por su nombre o por otros medios, como su número de teléfono o información relativa a sus condiciones de trabajo y a sus aficiones, constituye un «tratamiento total o parcialmente automatizado de datos personales» en el sentido del artículo 3, apartado 1, de la Directiva 95/46. (Apartado 27). En segundo lugar, "no existe una «transferencia a un país tercero de datos» en el sentido del artículo 25 de la Directiva 95/46 cuando una persona que se encuentra en un Estado miembro difunde datos personales en una página web, almacenada por su proveedor de servicios de alojamiento de páginas web que tiene su domicilio en el mismo Estado o en otro Estado miembro, de modo que dichos datos resultan accesibles a cualquier persona que se conecte a Internet, incluidas aquéllas que se encuentren en países terceros" (Apartado 71).

sometido a la competencia de un Estado u organización que no es Parte del Convenio"[113]. En otras palabras, fija reglas para transferir datos a países donde dicho convenio no es jurídicamente vinculante.

Posteriormente, en el Marco de Privacidad APEC de 2004 no se hace referencia explícita a la transferencia internacional de datos o a una expresión similar pero dentro del principio de "Responsabilidad" (*Accountability*) se hace alusión a la situación en que la información vaya a ser transferida a otra persona u organización, nacional o internacional[114]. Posteriormente, en las Directrices de la Red Iberoamericana de Protección de Datos (RIPD) se utiliza la expresión "transferencia internacional de datos"[115] sin definición alguna. En 2009, la Resolución de Madrid incorpora la expresión "Transferencias Internacionales"[116]. En la Propuesta de 2012 del Reglamento general de protección de datos del Parlamento Europeo y del Consejo, siguiendo lo planteado en la Directiva 95/46/CE se les denomina como "Transferencia de datos personales a terceros países u organizaciones internacionales"[117]. La versión de 2013 de las directrices OCDE no refleja ningún cambio en este aspecto respecto de los dispuesto en 1980.

En síntesis, las transferencias internacionales de datos personales se presentan cuando un tercero diferente del titular del dato envía esa información desde un país hacia otro (s) país (es). Implica, por tanto, que los datos salen del territorio de un país. Ahora bien, las reglas sobre transferencias internacionales buscan, entre otros, prevenir que los datos de los ciudadanos de un país se envíen a otro país sin niveles adecuados de protección o a paraísos informáticos como lo señalaremos enseguida.

113 Protocolo adicional de 2001 al Convenio 108, artículo 2.
114 Marco de Privacidad APEC de 2004, numeral 26.
115 Directrices de la Red Iberoamericana de Protección de Datos, numeral 8.
116 Resolución de Madrid (2009), numeral 15.
117 Propuesta de Reglamento general de protección de datos del Parlamento Europeo y del Consejo (2012), capítulo V.



Esquema simple de transferencia internacional de datos personales. Elaboración del autor.

DE LOS PARAÍSOS INFORMÁTICOS AL PRINCIPIO DE CONTINUIDAD DE PROTECCIÓN DE DATOS EN LAS TIDP

Algunos países carecen de normas sobre tratamiento de datos lo cual significa que en esas partes del planeta no existe certeza sobre la forma de proteger los derechos de los titulares de los datos o simplemente no se protege a las personas frente al tratamiento indebido de los datos personales. En la nota explicativa[118] del Convenio 108 del Consejo de Europa[119], del 28 de enero

118 El texto de la nota (explanatory report) puede consultarse en: http://conventions.coe.int/Treaty/EN/Reports/HTML/108.htm

119 La versión oficial del Convenio se encuentra publicada en: http://conventions.coe.int/Treaty/EN/Treaties/Html/108.htm. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Strasbourg, 28.I.1981.

de 1981, se reconoció la existencia de países que no tienen leyes de protección de datos o que las tienen pero con niveles bajos de protección denominados "paraísos informáticos" (data havens) en donde la protección de los derechos de los titulares de los datos es débil o inexistente[120].

Palazzi, refiriéndose al artículo 25 de la Directiva 95/46/CE comenta que la finalidad de la misma es "evitar la creación de paraísos informáticos (*data havens*), es decir, jurisdicciones donde la carencia de leyes de protección de datos, las transforme en sitios atractivos para realizar tratamientos de datos personales que pueden ser violatorios de otras leyes de privacidad"[121]. Los "paraísos informáticos" no sólo comprenden países sin regulación sobre tratamiento de datos personales sino que también cobijan otros temas como, entre otros, los delitos informáticos. Para la ONU, por ejemplo, los "paraísos informáticos" son "Estados que no dan prioridad a la reducción o prevención del uso ilícito de las redes de computadoras, o donde no se han elaborado leyes de procedimiento eficaces"[122].

Las TIC e Internet[123] permiten a las personas realizar muchas actividades desde cualquier parte del mundo. Así las cosas, para ellas puede ser conveniente, en ciertos casos, seleccionar países en donde no exista legislación sobre la actividad lo cual les permite obrar libremente y mitigar cualquier riesgo jurídico de ser investigados o sancionados por incumplir la ley del país que escogieron como domicilio[124]. En este sentido, la ONU

120 El texto original completo dice lo siguiente: "In practice, however, protection of persons grows weaker when the geographic area is widened. Concern has been expressed that data users might seek to avoid data protection controls by moving their operations, in whole or in part, to "data havens", i.e. countries which have less strict data protection laws, or none at all." Cfr. http://conventions.coe.int/Treaty/EN/Reports/HTML/108.htm

121 Cfr. PALAZZI, Pablo. 2003. *Comercio electrónico, transferencia internacional de datos personales y armonización de leyes en un mundo globalizado.* En Derecho de internet & telecomunicaciones, editado por GECTI. Bogotá: Legis. p 299.

122 Cfr. ORGANIZACIÓN DE LAS NACIONES UNIDAS. 2000. Delitos relacionados con las redes informáticas. Documento A/CONF.187/10 sobre antecedentes para el curso práctico sobre delitos relacionados con las redes informáticas. En Décimo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente. Viena: ONU. p 3.

123 Señala Palazzi que "no es necesario aclarar que con el explosivo desarrollo de Internet y la velocidad y la facilidad de las comunicaciones actuales, la posibilidad de encontrar data havens es cada vez más alta" [Cfr. PALAZZI, 2003, op. cit., p. 299].

124 Para la ONU, en el campo de los delitos informáticos, "los delincuentes cibernéticos pueden encau-

destaca que "las estructuras abiertas de las redes informáticas internacionales ofrecen a los usuarios la oportunidad de elegir el entorno jurídico que mejor se ajuste a sus propósitos. Los usuarios pueden elegir un país en el que determinadas formas de comportamiento que puedan desarrollarse en un entorno electrónico no se hayan tipificado como delitos. Esto puede atraer la actividad de personas de otros Estados en cuyos ordenamientos jurídicos esas mismas actividades constituyan un delito"[125].

En los medios de comunicación se ha puesto de manifiesto la problemática que generan a las autoridades dichos paraísos. En efecto, según las autoridades españolas, "las unidades de policías especializadas en perseguir los delitos informáticos consideran que el principal problema para luchar contra este tipo de criminalidad son los "paraísos informáticos", países donde la falta de legislación y de control en ese campo sirve de "punta de lanza" a estos delincuentes"[126]. Particularmente se recalca que "el delincuente sabe que ´hay países donde hay una legislación muy laxa´ en esta materia y que le permite ´ampararse y acudir a estos paraísos informáticos como punta de lanza o camino´ para cometer sus delitos, y ha precisado que este problema es "muy preocupante" en países de Europa del Este y Asia. De este modo, y después de una investigación minuciosa, ´cuando llegamos a ese país, no hay nada que hacer"[127]. Este panorama en materia de delitos informáticos puede replicarse al caso del tratamiento de datos personales.

Vista la gravedad potencial de esta realidad, en materia de tratamiento de datos se han establecido reglas para evitar que los datos objeto de transferencias internacionales lleguen a "paraísos informáticos". En efecto, a partir de los documentos analizados puede establecerse que, como regla, para que

zar sus actividades electrónicas a través de un determinado Estado en el que ese comportamiento no esté tipificado como delito y por lo tanto quedar amparados por las leyes de ese país" [Cfr. ONU, 2000, op. cit., p. 5.]

125 Ibíd., p. 3.

126 Cfr. Los 'paraísos informáticos', la mayor pesadilla de los 'ciberpolicías'. Los países sin legislación ni control sirven de 'punta de lanza' a estos delincuentes. Noticia publicada por el diario el mundo.es el 22 de octubre de 2007 en su página web http://www.elmundo.es/navegante/2007/10/22/tecnologia/1193064956.html (última consulta junio 15 de 2014).

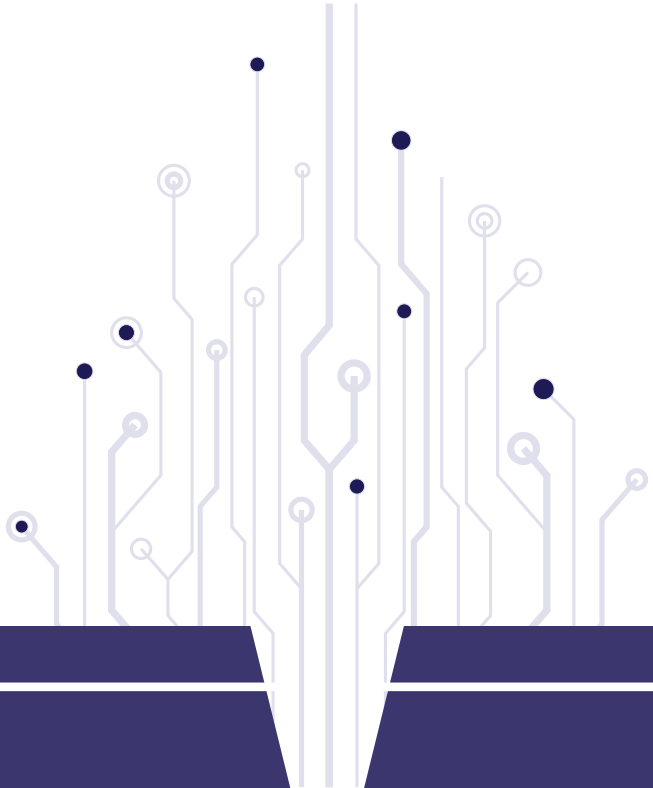
127 Loc. cit.

se permita transferir datos de un país a otro se debe verificar que el país receptor de los mismos garantice un nivel "adecuado" de protección de los datos personales. "Adecuado" inicialmente se refiere a que en el país en donde se reciban los datos exista un grado de protección superior, igual, similar o equivalente al del país desde donde se remiten los mismos.

Con lo anterior se busca evitar que con ocasión de una operación de exportación de datos personales se disminuya el nivel de protección que se le garantiza al titular del dato en el país exportador. En otros términos, se quiere que el nivel de protección del país exportador se garantice en el país importador. Esta regla es conocida como el principio de continuidad de la protección de datos y se fundamenta en que "la transferencia internacional de datos no debe afectar la protección de los interesados por lo que respecta al tratamiento de sus datos personales"[128]. Así las cosas, en diversos documentos internacionales se han establecido reglas y mecanismos para procurar garantizar el citado principio de continuidad. Este aspecto será analizado en las próximas líneas.

128 Cfr. DE FRUTOS, JOSÉ MANUEL, "Globalización de la privacidad: hacia unos estándares comunes", Conferencia presentada dentro del marco del VI Encuentro Iberoamericano de Protección de Datos realizado en Cartagena de Indias (Colombia) del 27 al 30 de mayo de 2008.

LA TRANSFERENCIA INTERNACIONAL DE DATOS EN LOS DOCUMENTOS INTERNACIONALES



A continuación nos referiremos a las principales pautas que sobre transferencia internacional de datos han desarrollado algunas entidades internacionales. Para el efecto utilizaremos como fuentes primarias los textos originales de los documentos y citaremos la labor de las organizaciones en orden cronológico para establecer las ideas centrales sobre la materia sin importar que al mismo tiempo estudiemos las recientes reformas o proyectos de reformas surgidas sobre los primeros textos internacionales.

ORGANIZACIÓN PARA LA COOPERACIÓN Y EL DESARROLLO ECONÓMICO (OCDE)

Esta entidad fue denominada en 1948 como "Organización Europea de Cooperación Económica (OECE)" con el propósito inicial de implementar el Plan Marshall financiado por Estados Unidos para procurar reconstruir Europa luego de la Segunda Guerra Mundial. Su nombre cambió a Organización para la Cooperación y el Desarrollo Económico (OCDE) cuando Canadá y los Estados Unidos de América se unieron a los miembros de la OECE con la firma del nuevo convenio de la OCDE el 14 de diciembre de 1960. La OCDE nació oficialmente el 30 de septiembre de 1961, cuando la Convención entró en vigor[129].

Dentro de los principales objetivos de la OCDE se encuentra la promoción de políticas: "**(A)** para lograr el máximo crecimiento económico sostenible y el empleo y la elevación del nivel de vida en los países miembros, manteniendo la estabilidad financiera, y así contribuir al desarrollo de la economía mundial; **(B)** contribuir a una sana expansión económica en los Estados miembros, así como los países no miembros en el proceso de desarrollo económico, y **(C)** contribuir a la expansión del comercio mundial sobre una base multilateral y no discriminatoria conforme a las obligaciones internacionales"[130]. Para materializar esos ob-

129 Toda esta información fue tomada de la página web de la OCDE http://www.oecd.org/about/history/
130 Cfr. Artículo 1 de la Convención sobre la Organización para la Cooperación y el Desarrollo suscrita el 14 de diciembre de 1960 en París. El texto oficial de la Convención puede consultarse en http://www.oecd.org/general/conventionontheorganisationforeconomicco-operationanddevelopment.htm

jetivos la OCDE puede emitir recomendaciones que no son de obligatorio cumplimiento[131].

Las directrices OCDE de 1980, actualizadas en 2013, son los principales documentos[132] que contienen aspectos sobre transferencias internacionales de datos, razón por la cual las analizaremos a continuación. Vale la pena aclarar que estas recomendaciones no son un instrumento jurídico vinculante o de obligatorio cumplimiento entre los miembros de la OCDE. Se trata de directrices para que los mismos las tengan en cuenta en sus regulaciones internas y procuren eliminar barreras injustificadas a la circulación transfronteriza de datos personales[133].

131 Cfr. Literal b) del artículo 5 de la Convención sobre la Organización para la Cooperación y el Desarrollo suscrita el 14 de diciembre de 1960 en París. De conformidad con el numeral 3 del artículo 6 de la Convención, "Ninguna decisión será vinculante para cada Miembro, hasta que haya cumplido con los requisitos de sus propios procedimientos constitucionales".

132 Existen otros documentos importantes de la OCDE pero los más relevantes para efectos de esta investigación son las directrices de privacidad de 1980 y 2013. No obstante, a título referencial citamos otros textos de dicha organización que son mencionados en el preámbulo de la versión 2013 a saber: Ministerial Declaration on the Protection of Privacy on Global Networks [C(98)177]; the Recommendation of the Council concerning Guidelines for the Security of Information Systems and Networks [C(2002)131/FINAL], the Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy [C(2007)67], the Declaration for the Future of the Internet Economy (The Seoul Declaration) [C(2008)99], the Recommendation of the Council on Principles for Internet Policy Making [C(2011)154], the Recommendation of the Council on the Protection of Children Online [C(2011)155] and the Recommendation of the Council on Regulatory Policy and Governance [C(2012)37].

133 En la nota explicativa de las recomendaciones de la OCDE se destaca que "a principios de 1978 se creó dentro de la OCDE un nuevo Grupo de Expertos ad hoc sobre las Trabas a la Circulación Transfronteriza de Datos y Protección de la Intimidad, al que se encargó la elaboración de directrices sobre normas básicas que rijan la circulación transfronteriza y la protección de datos personales y de la intimidad, a fin de facilitar la armonización de las legislaciones nacionales, sin perjuicio de que se establezca en fecha posterior un Convenio internacional".

DIRECTRICES DE PRIVACIDAD OCDE DE 1980

El 23 de septiembre de 1980[134] el Consejo de la OCDE aprobó una serie de recomendaciones[135] con miras a "fomentar la libre circulación de información entre los países miembros y a evitar la creación de obstáculos injustificados al desarrollo de las relaciones económicas y sociales entre los países miembros"[136]. Preocupaba a la OCDE que las restricciones injustificadas a la circulación transfronteriza "podrían ocasionar graves trastornos en importantes sectores de la economía, tales como la banca y los seguros"[137].

En la parte tercera de las recomendaciones se establecieron ciertos principios de aplicación internacional centrados en la libre circulación de información entre los países miembros de la OCDE. Por eso se enfatizó en el numeral 16 de las Recomendaciones, la necesidad de que los "países miembros deberían adoptar todas las medidas razonables y oportunas para garantizar la circulación transfronteriza, ininterrumpida y segura, de los datos personales, incluso el tránsito a través de algún país miembro".

Las Recomendaciones permiten que los países miembros establezcan limitaciones a la circulación de determinada

134 La actividad de la OCDE en lo referente al tema en estudio inició desde 1969 tal y como lo destaca esa organización en la nota explicativa de las Recomendaciones de 1980:" El programa de la OCDE acerca de la circulación transfronteriza de datos se deriva de unos estudios de utilización de la informática en el sector público que se iniciaron en 1969. Un Grupo de Expertos, el Data Bank Panel, analizó y estudió diferentes aspectos de la cuestión de la intimidad, verbigracia, en relación a la información digital, la administración pública, la circulación transfronteriza de datos y los resultados implícitos de la política en general. A fin de recabar pruebas de la índole de los problemas, el Data Bank Panel organizó un Simposio en Viena en 1977, que proporcionó opiniones y experiencia procedentes de una diversidad de sectores interesados, incluidos gobiernos, industria, usuarios de redes internacionales de comunicación de datos, servicios de tratamiento y organismos intergubernamentales".

135 OCDE. 1980. Recomendación del Consejo relativa a las directrices que rigen la protección de la intimidad y de la circulación transfronteriza de datos personales.

136 Parte final de los considerandos de: OCDE, 1980, op. cit. En la nota explicativa de las Recomendaciones se recalca el énfasis de promover la circulación internacional, pero respetando el derecho a la intimidad: "Tal y como se manifiesta en el Preámbulo, hay implicados dos valores básicos imprescindibles: la protección de la intimidad y de las libertades individuales y el fomento de la libre circulación de datos personales. Con las Directrices se intenta equilibrar ambos valores entre sí. En tanto que se aceptan ciertas restricciones a la libre circulación transfronteriza de datos personales, se pretende reducir la necesidad de tales restricciones y, por tanto, reforzar la idea de la libre circulación de información entre los países".

137 Parte del prólogo de: OCDE, 1980, op.cit.

clase de datos. En todo caso, en el numeral 18 de las mismas se recomendaba a los países "evitar la elaboración de leyes, políticas y prácticas en aras de la protección de la intimidad y de las libertades individuales, que creen obstáculos a la circulación transfronteriza de datos personales que superarían las necesidades de tal protección".

En el numeral 17 de las Recomendaciones se establecieron las pautas para permitir la transferencia internacional de datos entre países miembro de la OCDE. La regla general es la libre circulación[138] entre los mismos, salvo dos casos: **(I)** El país de destino de la información "no haya observado sustancialmente estas Directrices" o **(II)** "la reexportación de tales datos soslayase su legislación nacional sobre la intimidad".

Como se observa, el cumplimiento de las directrices por parte del país destinatario de la circulación transfronteriza de datos es el factor para establecer que el mismo garantiza un nivel de protección equivalente. Estas reglas prevén la hipótesis de la circulación entre países miembros[139]. Es decir, se trata de un modelo de reglas de transferencia para operar en un escenario cerrado (intergrupal) al interior de los países que conforman la OCDE[140].

Las Recomendaciones no fijan pautas para aplicar cuando la transferencia se hace a un país no miembro de la OCDE[141].

138 Según la parte inicial del numeral 17 de los principios OCDE, "la circulación transfronteriza de datos personales entre dos países miembro no debería restringirse".

139 De hecho, en el acápite sobre cooperación internacional (V Parte) se establece que "los países miembros deberían también asegurar que los procedimientos para la circulación transfronteriza de datos personales y para la protección de la intimidad y de las libertades individuales, sean sencillos y compatibles con los de los demás países miembro que cumplan estas Directrices".

140 A diciembre 31 de 2023 los siguientes países son miembros de la OCDE: Australia, Austria, Belgium, Canada, Chile, Colombia, Costa Rica, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Korea, Lituania, Luxembourg, México, Netherlands, New Zealand, Norway, Poland, Portugal, Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, United Kingdom, United States. Información tomada el 16 de enero de 2024 de la página web de la OCDE: http://www.oecd.org/about/membersandpartners/

141 En la nota explicativa de los principios de la OCDE se reconoció que "la Recomendación va dirigida a los países miembros, lo cual se hace ver en varias disposiciones que están restringidas expresamente a las relaciones entre los países miembros (véanse los Apartados 15, 17 y 20 de las Directrices). Sin embargo, el reconocimiento generalizado de las Directrices es conveniente y nada de lo que se exponga en ellas debería interpretarse en el sentido de que se impide la aplicación de las Disposiciones oportunas a los países que no sean miembros. En vista del incremento en la circulación transfronteriza de datos y de

Asumimos que la regla será la de no enviar datos a ese país salvo que garantice un "nivel de protección equivalente" al que se obtiene con las Recomendaciones de la OCDE.

DIRECTRICES DE PRIVACIDAD OCDE DE 2013

A partir de un proceso de revisión y actualización[142] de las directrices de 1980 para ajustarlas a los retos[143] actuales, el 11 de julio de 2013 el Consejo de la OCDE adoptó la nueva versión de las directrices que rigen la protección de la privacidad y de la circulación transfronteriza de datos personales (Directrices de privacidad)[144].

Respecto de la TIDP se destaca el cambio sustancial del contexto de 1980 vs. el actual. En la nota explicativa se pone de manifiesto que cuando se redactaron las Directrices de 1980, los flujos de datos principalmente eran transmisiones punto a punto entre empresas o gobiernos. Hoy, señala la OCDE, los datos se pueden procesar de forma simultánea en múltiples ubicaciones; se pueden almacenar en diversos puntos ubicados en diferentes partes del mundo y es sencillo recombinarlos instantáneamente. Adicionalmente, los datos pueden ser movidos a través de las fronteras por cualquier persona mediante dispositivos móviles[145].

En la versión de 2013 se ratifica la postura de 1980 en el sentido de que los miembros de la OCDE están decididos a

la necesidad de garantizar soluciones concertadas, se hará todo lo posible para poner las Directrices en conocimiento de los países que no sean miembros y de los organismos internacionales competentes".

142 Según la OCDE este proceso inició en 2010 en el contexto del décimo tercer aniversario de las recomendaciones de 1980. Puede consultarse mayor detalle en el siguiente libro de dicha organización: ORGANISATION FOR ECONOMIC COOPERATION AND DEVELOPMENT. 2013. The OECD privacy framework, OECD. P 21-22.

143 Sobre los retos vale la pena mencionar los que surgen para la protección de las personas en escenarios como el big data. En este sentido en noviembre de 2012 se publicó un documento contentivo de algunas reflexiones y propuestas preliminares para tener presente en la nueva versión de las directrices de la OCDE. Ver: CATE y MAYER-SHÖNBERGER, 2012, op. cit.

144 Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data ("Privacy Guidelines").

145 "When the 1980 Guidelines were drafted, data flows largely constituted discrete point-to-point transmissions between businesses or governments. Today, data can be processed simultaneously in multiple locations; dispersed for storage around the globe; re-combined instantaneously; and moved across borders by individuals carrying mobile devices." [OCDE, 2013, op. cit., p. 29.]

"promover aún más el libre flujo de información entre los países miembros y evitar la creación de obstáculos injustificados al desarrollo de las relaciones económicas y sociales entre ellos".

Dentro de los motivos esenciales de la nueva versión y pertinentes para efectos de esta investigación se destaca que los países miembros de la OCDE tienen un interés en promover y proteger "valores fundamentales de la vida privada, las libertades individuales y el libre flujo global de información". Se suma a lo anterior el reconocimiento de la OCDE de que "los usos más amplios e innovadores de datos personales generan mayores beneficios económicos y sociales, pero también aumentan los riesgos a la privacidad"[146].

Según la OCDE dos aspectos relevantes se destacan en las directrices de 2013. En primer lugar, alcanzar mayores niveles de privacidad mediante la implementación de un enfoque basado en la gestión del riesgo (*risk management*), acompañado de programas de gestión de privacidad (*Privacy management programmes*) mediante el cual las organizaciones implementan la protección de privacidad. En segundo lugar, realizar más y mejores esfuerzos para abordar la dimensión global de la privacidad a través de una mejor interoperabilidad[147] (*improved interoperability*)[148].

Respecto de las TIDP se establece lo siguiente:

Conserva la definición de la versión de 1980, en el sentido que "circulación transfronteriza de datos personales" se refiere a los movimientos de datos personales a través de fronte-

146 La versión original en inglés de los considerandos dice lo siguiente: "RECOGNISING that Member countries have a common interest in promoting and protecting the fundamental values of privacy, individual liberties and the global free flow of information; RECOGNISING that more extensive and innovative uses of personal data bring greater economic and social benefits, but also increase privacy risks.

147 En los considerandos de la versión 2013 se establece que "RECONOCIENDO que los flujos continuos de datos de carácter personal a través de redes mundiales amplifican la necesidad de mejorar la interoperabilidad entre marcos de privacidad, así como la cooperación transfronteriza reforzada entre las autoridades de aplicación de la privacidad". En el numeral 21 se invita a los países miembros para que fomenten y apoyen el desarrollo de acuerdos internacionales que promueven interoperabilidad entre diversas regulaciones sobre privacidad para dar aplicación práctica a las directrices.

148 Cfr. http://www.oecd.org/sti/ieconomy/privacy.htm

ras nacionales"[149] y establece –en la parte IV, numerales 16 a 18– las siguientes reglas sobre las TIDP:

Por una parte, se precisa que el responsable del tratamiento o controlador (data controller) responde por el tratamiento de los datos sin que sea relevante el lugar donde estos se encuentren[150]. Adicionalmente, se promueve la libre transferencia de datos entre países que **(a)** observen sustancialmente las directrices o **(b)** proporcionen garantías suficientes incluyendo, entre otros, los mecanismos de cumplimiento efectivo o medidas apropiadas que utilice el responsable del tratamiento para asegurar un nivel constante de protección en consonancia con las directrices 2013 de la OCDE[151]. Por otra parte, se recalca que las eventuales restricciones que creen los Estados a las TIDP deben ser "proporcionales a los riesgos presentados, teniendo en cuenta la sensibilidad de los datos, así como el propósito y contexto del tratamiento"[152].

En síntesis, la OCDE condiciona el envío de datos a otros Estados siempre y cuando en el país destinatario se garantice un nivel de protección igual o muy similar al brindado por la directriz de 2013.

CONSEJO DE EUROPA (CE)

Los tres principales textos internacionales jurídicamente vinculantes son el Convenio 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal (en

149 "Transborder flows of personal data" means movements of personal data across national borders". (Literal e) del numeral 1 –Definitions- de "Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013)".

150 La versión original en inglés dice lo siguiente: "16. A data controller remains.

151 La versión original en inglés dice lo siguiente: "17. A Member country should refrain from restricting transborder flows of personal data between itself and another country where (a) the other country substantially observes these Guidelines or (b) sufficient safeguards exist, including effective enforcement mechanisms and appropriate measures put in place by the data controller, to ensure a continuing level of protection consistent with these Guidelines".

152 El texto original en inglés dice lo siguiente: "18. Any restrictions to transborder flows of personal data should be proportionate to the risks presented, taking into account the sensitivity of the data, and the purpose and context of the processing".

adelante el Convenio 108 de 1981), el Protocolo 181+ de 2001 del Consejo de Europa, adicional al Convenio para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal, a las autoridades de control y los flujos trasfronterizos de datos (en adelante el Protocolo 181 de 2001) y el Convenio 108+.

A continuación, nos referiremos a los principales aspectos de estos respecto a las transferencias internacionales.

EL CONVENIO 108 DE 1981

Este convenio[153] establece las pautas para proteger las personas respecto al tratamiento automatizado de datos de carácter personal. Es el primer tratado internacional sobre protección de datos que es jurídicamente vinculante a 46 países[154].

En la nota explicativa del Convenio[155] se reconoció que las computadoras y las telecomunicaciones facilitan nuevas formas de tratar datos a escala internacional superando barreras de distancia, tiempo, lenguaje y costos; particularmente en algunos sectores (banca, turismo, tarjetas de crédito) en donde en aquella época la trasferencia internacional de datos era algo cotidiano[156]. Frente a dicho escenario se preguntaban,

153 La versión oficial del Convenio se encuentra publicada en: http://conventions.coe.int/Treaty/EN/Treaties/Html/108.htm Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Strasbourg, 28.I.,1981.

154 Esta es la información existente a abril 20 de 2014 en la "Treaty Office" del Consejo de Europa. El convenio entró en vigencia el 1 de octubre de 1985 (Cfr. http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=108&CM=8&DF=20/04/2014&CL=ENG). En el sitio oficial del Consejo de Europa se encuentra el listado de países que han ratificado el convenio. Uruguay es el único país latinoamericano que ha ratificado dicho convenio Ver: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=8&DF=20/04/2014&CL=ENG

155 El texto de la nota (explanatory report) puede consultarse en: http://conventions.coe.int/Treaty/EN/Reports/HTML/108.htm

156 Tel texto original de la parte pertinente de la nota explicativa dice lo siguiente: "Transborder flows of personal data.

8. The question has arisen to what extent national data protection laws afford adequate protection to individuals when data concerning them flow across borders. Computers, in combination with telecommunications, are opening new prospects for data processing on an international scale. They help to overcome several types of barrier to communication between nations: distance, time, language and cost. Distributed processing enables users to disperse an information system or data base over several countries. Networks help users to have access to or link information systems in distant countries. In several sectors (for example banking, travel, credit cards, etc.) such transfrontier data processing applications

los redactores del Convenio, qué tanto las normas locales o regulaciones nacionales protegen los derechos de sus ciudadanos cuando sus datos son enviados a otros países. En el caso de los flujos transfronterizos de datos personales, dice la nota explicativa, "las mismas reglas fundamentales deben aplicarse y los interesados deben disponer de las mismas garantías para la protección de sus derechos e intereses"[157].

Desde aquella época se reconoció la existencia de países en donde la protección de los derechos de los titulares de los datos es débil o inexistente. Por eso, en algunas naciones, se crearon figuras como las licencias de exportación de datos, pero las mismas podrían "interferir con la libre circulación internacional de la información, que es un principio de fundamental importancia para los individuos, así como de naciones"[158].

Teniendo en cuenta lo anterior, el artículo 12 del Convenio, titulado Flujos transfronterizos de datos de carácter personal y el derecho interno, fijó las siguientes pautas dependiendo de si los datos se envían a países que forman o no parte del Convenio[159]. Para el CE el flujo internacional de datos es libre entre Estados parte del Convenio y prohibido o condicionado cuando se realiza a un Estado no parte del mismo. Veamos:

En primer lugar, si el país destinatario de los datos hace parte del Convenio no existe inconveniente en que se le envíen los datos porque un Estado parte del Convenio no puede, "con el fin de proteger la vida privada, prohibir o someter a una autorización especial los flujos transfronterizos de datos de carácter

are already commonplace" Cfr. http://conventions.coe.int/Treaty/EN/Reports/HTML/108.htm

157 El texto original dice lo siguiente: "The same fundamental rules should apply and data subjects should be given the same safeguards for the protection of their rights and interests" Cfr. http://conventions.coe.int/Treaty/EN/Reports/HTML/108.htm

158 El texto original completo dice lo siguiente: "(...) In order to counter this risk some countries have built into their domestic law special controls, for example in the form of a licence for export. However, such controls may interfere with the free international flow of information which is a principle of fundamental importance for individuals as well as nations. A formula had to be found to make sure that data protection at the international level does not prejudice this principle." Cfr. http://conventions.coe.int/Treaty/EN/Reports/HTML/108.htm

159 Según el numeral 1 del artículo 12 las reglas de dicho artículo se aplican a "las transmisiones a través de las fronteras nacionales, por cualquier medio que fuere, de datos de carácter personal que sean objeto de un tratamiento automatizado o reunidos con el fin de someterlos a ese tratamiento".

personal con destino al territorio de otra Parte"[160]. No obstante, lo anterior, es factible que un país parte establezca excepciones a la anterior regla para categorías especiales de datos personales o de ficheros, "a menos que la reglamentación de la otra Parte establezca una protección equivalente"[161]. Nótese como "la protección equivalente" del país de destino es un habilitante jurídico para que se pueda realizar la transferencia internacional y, con ello, se busca garantizar el principio de continuidad de la protección de datos. Esta expresión (protección equivalente) es quizá el precedente de lo que luego se quiso buscar al amparo del término "nivel adecuado de protección" a que se refiere la Directiva 95/46/CE.

En segundo lugar, se puede prohibir o someter a autorización especial el flujo internacional de datos a países que no hacen parte del Convenio"[162]. Lo anterior es así porque se asume que los Estados no contratantes del Convenio carecen de un nivel de protección equivalente al que se deriva del Convenio 108 de 1981.

EL PROTOCOLO 181 DE 2001

Dos décadas después se expidió el Protocolo 181[163] de 2001 del Consejo de Europa, adicional al Convenio para la protección de las personas respecto al tratamiento automatizado de datos

160 Cfr. Numeral 2 del artículo 12 del Convenio 108 de 1981 del Consejo de Europa.

161 Cfr. Literal a) del numeral 3 del artículo 12 del Convenio 108 del Consejo de Europa. El texto completo es el siguiente: "3. Sin embargo, cualquier Parte tendrá la facultad de establecer una excepción a las disposiciones del párrafo 2: a) En la medida en que su legislación prevea una reglamentación específica para determinadas categorías de datos de carácter personal o de ficheros automatizados de datos de carácter personal, por razón de la naturaleza de dichos datos o ficheros, a menos que la reglamentación de la otra Parte establezca una protección equivalente".

162 Cfr. Literal b) del numeral 3 del artículo 12 del Convenio 108 del Consejo de Europa. El texto de la norma dice lo siguiente: "3. Sin embargo, cualquier Parte tendrá la facultad de establecer una excepción a las disposiciones del párrafo 2: b) cuando la transmisión se lleve a cabo a partir de su territorio hacia el territorio de un Estado no contratante por intermedio del territorio de otra Parte, con el fin de evitar que dichas transmisiones tengan como resultado burlar la legislación de la Parte a que se refiere el comienzo del presente párrafo".

163 Protocolo 181+ de 2001 del Consejo de Europa adicional al Convenio para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal, a las autoridades de control y los flujos trasfronterizos de datos, adoptado en Estrasburgo del 8 de noviembre de 2001. (Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows. Strasbourg,8.XI.2001).

de carácter personal, a las autoridades de control y los flujos trasfronterizos de datos, adoptado en Estrasburgo del 8 de noviembre de 2001. Este convenio entró en vigor el 1 de julio de 2004 y es jurídicamente vinculante a los 35 países que lo han ratificado[164]. Su finalidad fue la de mejorar la aplicación de los principios contenidos en el convenio 108.

De conformidad con la nota explicativa del protocolo, se incluyó la creación de la autoridad de control por cada Parte y se matizaron y ampliaron las reglas sobre los flujos transfronterizos de datos personales a países u organizaciones que no son parte del convenio. En dicha nota se recalcó que cada día aumenta el volumen de transferencias a nivel mundial debido a los avances tecnológicos, razón por la cual es necesario un esfuerzo constante para mejorar la protección efectiva de los derechos garantizados por la Convención. Se puso de manifiesto que "la protección efectiva de la vida privada y los datos personales también significa que no debe haber flujos transfronterizos de datos personales a países u organizaciones en los que no se garantiza la protección de dichos datos".

Con el Protocolo 181 de 2001 se modificó el lenguaje de prohibición del flujo internacional a un país no contratante a uno de permisión siempre y cuando el Estado receptor de la información garantice un nivel adecuado de protección tal y como se deriva del numeral del artículo 2.

De conformidad con la nota explicativa, el nivel de protección debe ser evaluado caso por caso, para la transferencia o categoría de transferencias. Señala dicha nota que "así, las circunstancias de la transferencia deberán ser examinadas y, en particular, el tipo de datos, la finalidad y duración del tratamiento al que se transfieren los datos, el país de origen y el país de destino final, las normas generales y sectoriales de la ley aplicable en el Estado u organización de que se trate y las

164 Esta es la información existente al 20 de abril de 2014 y fue tomada de la "Treaty office" del Consejo de Europa: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=181 El listado de países que lo han ratificado puede consultarse en: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=181&CM=8&DF=20/04/2014&CL=ENG

normas profesionales y de seguridad que obtienen allí". Adicionalmente, la evaluación para establecer el nivel adecuado de protección debe tener en cuenta los principios del Capítulo II del Convenio 108 y del Protocolo 181, así como el nivel en que, efectivamente, se cumplen en el lugar receptor de los datos y los mecanismos con que cuenta el titular para defender sus derechos en el país destinatario de la transferencia de los datos.

No obstante lo anterior, el Convenio permite que las partes autoricen las transferencias a países u organizaciones que no tengan un nivel adecuado de protección cuando el derecho interno lo permite para proteger intereses específicos del titular de los datos o intereses legítimos como aquellos de interés público. También es factible que se autorice la transferencia cuando existan garantías suficientes que pueden resultar de cláusulas contractuales suscritas por el responsable del tratamiento para efectos de la transferencia, siempre y cuando dichas garantías (cláusulas contractuales) se consideren adecuadas por parte de la autoridad de protección de datos del país donde se exportará la información. Mediante dichas cláusulas se vincula al responsable del tratamiento y al destinatario de la transferencia que está ubicado en un país que no está sujeto a la jurisdicción de un Estado parte del convenio.

En síntesis, en un documento internacional vinculante —como el protocolo— se introdujo la expresión "nivel adecuado de protección" y al mismo tiempo se dio la posibilidad de permitir la transferencia internacional si existen otras garantías o alternativas como las cláusulas contractuales que utilice el Responsable del tratamiento, las cuales deben ser aprobadas por parte de las autoridades competentes del país exportador de los datos.

EL CONVENIO 108+ DE 2018

La versión "actualizada" o "modernizada" de convenio 108[165] fue adoptada el 18 de mayo de 2018 y se conoce como el con-

165 Sobre el convenio 108, sus protocolos y el convenio 108+ consulte la página Consejo de Europa del en: https://www.coe.int/es/web/data-protection/convention108-and-protocol

venio 108+[166] para la protección de las personas con respecto al tratamiento de datos de carácter personal. A noviembre 12 de 2023 este convenio ha sido ratificado por 30 Estados, dentro de los cuales se encuentran los siguientes países latinoamericanos: Argentina y Uruguay[167].

Respecto del tema objeto de estudio de este texto, se señaló en el preámbulo que para contribuir al libre flujo de información es "necesario promover a nivel mundial los valores fundamentales de respeto de la privacidad y de la protección de datos personales".

En el capítulo III sobre flujos transfronterizos de datos se estableció lo siguiente en el artículo 14:

En primer lugar, se reiteró la regla general de no prohibir o condicionar la libre circulación de datos personales entre países miembros del convenio. En otras palabras, existe libre circulación transfronteriza de la citada información entre las partes del convenido[168].

En segundo lugar, se precisa que la transferencia internacional de datos, a países que no hacen parte del convenio únicamente, podrá realizarse si ese tercer país asegura un nivel adecuado de protección de datos de conformidad con los parámetros establecidos en el convenio 108+[169]. Señala el convenio que el nivel adecuado puede garantizarse mediante: "a. La ley de ese Estado u organización internacional, incluidos los tratados o acuerdos internacionales aplicables; o b. Salvaguardias o garantías ad hoc o estandarizadas aprobadas o establecidas en instrumentos legalmente vinculantes y ejecutables, adoptados e implementados por las personas involucradas en la transferencia o en el tratamiento posterior"[170].

166 Respecto del convenio 108+ o convenio 108 modernizado consulte: https://www.coe.int/es/web/data-protection/convention108/modernised

167 Sobre el estado de firma y ratificación del convenio 108+ consúltese: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=223 (Última consulta: 12/XI/2023).

168 Cfr. Numeral 1 del artículo 14 del Convenio 108+.

169 Cfr. Numeral 2 del artículo 14 del Convenio 108+.

170 Cfr. Numeral 3 del artículo 14 de Convenio 108+.

En tercer lugar, y sin perjuicio de lo anterior, los Estados también permiten las transferencias internacionales en los siguientes casos:

a. El titular de los datos ha dado su consentimiento explícito, específico y libre, después de ser informado de los riesgos derivados de la falta de salvaguardias adecuadas; o
b. Se requiere la transferencia para la protección de los intereses específicos del titular del dato; o
c. Existen intereses legítimos predominantes, en particular, los intereses públicos señalados en la ley, y dicha transferencia constituye una medida necesaria y proporcionada en una sociedad democrática; o
d. Constituye una medida necesaria y proporcionada en una sociedad democrática para la libertad de expresión"[171].

ORGANIZACIÓN DE LAS NACIONES UNIDAS (ONU)

En la Carta de las Naciones Unidas (ONU), suscrita el 26 de junio de 1945[172], se estableció como uno de los cometidos de la ONU el de "realizar la cooperación internacional (...) en el desarrollo y estímulo del respeto a los derechos humanos y a las libertades fundamentales de todos, sin hacer distinción por motivos de raza, sexo, idioma o religión"[173]. Por consiguiente, los derechos de las personas respecto del tratamiento de sus datos personales también han estado en la agenda de la ONU.

171 Cfr. Numeral 4 del artículo 14 del Convenio 108+.
172 El texto oficial de la Carta de las Naciones Unidas puede consultarse en la página web de dicha organización: http://www.un.org/es/documents/charter/index.shtml
173 Cfr. Numeral 3 del artículo 1 de la Carta de las Naciones Unidas. Otros propósitos de las Naciones Unidas enunciadas en dicho artículo son: "1. Mantener la paz y la seguridad internacionales (...) 2. Fomentar entre las naciones relaciones de amistad basadas en el respeto al principio de la igualdad de derechos y al de la libre determinación de los pueblos, y tomar otras medidas adecuadas para fortalecer la paz universal. 3. Realizar la cooperación internacional en la solución de problemas internacionales de carácter económico, social, cultural o humanitario, y en el desarrollo y estímulo del respeto a los derechos humanos y a las libertades fundamentales de todos, sin hacer distinción por motivos de raza, sexo, idioma o religión; y 4. Servir de centro que armonice los esfuerzos de las naciones por alcanzar estos propósitos comunes".

En efecto, la Asamblea General[174] de la ONU, mediante resolución 45/95 del 14 de diciembre de 1990, adoptó los "principios rectores para la reglamentación de los ficheros computadorizados de datos personales"[175]. Este documento fue precedido de las resoluciones 1990/42 del 6 de marzo de 1990 de la Comisión de Derechos Humanos de la ONU y 1990/38 del 25 de mayo de 1990 del Consejo Económico y Social de dicha organización, titulada "Guidelines on the use of computerized personal files". Estas directrices no son jurídicamente vinculantes, razón por la cual en el texto de la resolución se sugiere a los gobiernos tomar en cuenta las directrices en sus regulaciones internas[176].

Para la ONU la transferencia internacional de datos es viable si se establece que el país destinatario de los datos ofrece garantías comparables de protección a las ofrecidas por el país exportador. En efecto, el principio 9 denominado "Flujo de datos a través de las fronteras", dice que "cuando la legislación de dos o más países afectados por un flujo de datos a través de sus fronteras ofrezca garantías comparables de protección de la vida privada, la información debe poder circular tan libremente como en el interior de cada uno de los territorios respectivos"[177].

Dicha resolución no precisa qué se entiende por "garantías comparables" ni determina criterios o procedimientos para establecer cuándo dichas garantías son "comparables". Consideramos que el objetivo es circular datos a territorios donde las garantías de protección sean equiparables, semejantes, similares o análogas a las de país exportador.

174 "La Asamblea General ocupa un lugar central como principal órgano deliberativo, de formulación de políticas y representativo de las Naciones Unidas". Tomado de la página web de la ONU: http://www.un.org/es/ga/

175 Los principios aplican a los ficheros computadorizados de entidades públicas y privadas. También pueden aplicarse, con ciertas adaptaciones, a los ficheros manuales (Cfr. Numeral 10 de las directrices).

176 Cfr. Numeral 4 de los considerandos de la resolución 45/95 del 14 de diciembre de 1990 de la Asamblea General de la ONU.

177 El texto original en inglés dice lo siguiente: "9. Transborder data flows. When the legislation of two or more countries concerned by a transborder data flow offers comparable safeguards for the protection of privacy, information should be able to circulate as freely as inside each of the territories concerned. If there are no reciprocal safeguards, limitations on such circulation may not be imposed unduly and only in so far as the protection of privacy demands".

FORO DE COOPERACIÓN ECONÓMICA ASIA-PACÍFICO (APEC)

El Foro de Cooperación Económica Asia-Pacífico (APEC) es una comunidad de países que tiene como principal objetivo apoyar el crecimiento económico sostenible y la prosperidad en la región Asia-Pacífico basada en la defensa del comercio libre, la inversión, la promoción y la aceleración de la integración económica y, en general, facilitar un entorno empresarial favorable y sostenible[178].

APEC está integrado por 21 países[179] que representan el 55% del producto interno bruto mundial y el 44% por ciento del comercio global[180].

Inicialmente ciertos aspectos de las transferencias internacionales se incorporaron dentro del contenido del principio de Responsabilidad en el marco de privacidad APEC 2004. Allí se establece que, cuando los datos van a ser transferidos nacional o internacionalmente, el responsable tiene dos opciones: **(I)** Tener autorización del titular para la transferencia, o **(II)** Actuar con la debida diligencia y tomar las medidas razonables para asegurar que la persona u organización receptora, protegerá la información consistentemente con principios en comento. Se quiere que el país receptor garantice un nivel similar al que se deriva del citado marco de privacidad, lo cual es una manifesta-

178 Cfr. Página web oficial de APEC. http://www.apec.org/About-Us/About-APEC/Mission-Statement.aspx . La versión original en inglés sobre la misión (Mission Statement) de APEC dice lo siguiente: "APEC is the premier Asia-Pacific economic forum. Our primary goal is to support sustainable economic growth and prosperity in the Asia-Pacific region.
We are united in our drive to build a dynamic and harmonious Asia-Pacific community by championing free and open trade and investment, promoting and accelerating regional economic integration, encouraging economic and technical cooperation, enhancing human security, and facilitating a favorable and sustainable business environment. Our initiatives turn policy goals into concrete results and agreements into tangible benefits." http://www.apec.org/About-Us/About-APEC/Mission-Statement.aspx

179 A enero de 2024, los siguientes países forman parte de APEC: Australia, Brunéi Darussalam, Canadá, Chile, China, Hong Kong, Indonesia, Japón, Corea, Malasia, México, Nueva Zelanda, Papua Nueva Guinea, Perú, Filipinas, Rusia, Singapur, China Taipéi, Tailandia, Estados Unidos y Vietnam. Ver: http://www.apec.org/About-Us/About-APEC/Member-Economies.aspx (Última consulta: enero 8 de 2024).

180 Estos datos son publicados por APEC en su página web http://www.apec.org/press/news-releases/2012/0731_cbpr.aspx: "APEC's 21 member economies account for 55 percent of world real gross domestic product as well as 44 percent of world trade, comprising a large market of 2.7 billion consumers" (Última consulta: enero 8 de 2024).

ción del mencionado principio de continuidad de protección de datos personales.

Como se observa, la autorización no es obligatoria y el responsable debe velar porque la organización o empresa receptora de la información garantice un nivel de protección coherente con los principios APEC de 2004. Ahora bien, esto es lo que se exige en dichos principios, pero ello no significa que se modifiquen las normas internas de cada nación sobre transferencias internacionales. Por eso, el responsable debe cumplir las leyes del país desde donde se van a exportar los datos. Es factible que la ley local permita que la transferencia internacional sea posible cuando se utilicen mecanismos de autorregulación como, entre otros, las normas corporativas vinculantes.

Posteriormente, los principales aspectos de la transferencia internacional entre los países que hacen parte de APEC se plasmaron en el APEC Cross Border Privacy Rules[181] (CBPR). Con esto, las transferencias internacionales en las economías APEC se basan en un sistema voluntario de certificación de buenas prácticas en tratamiento de datos personales que son vinculantes para las organizaciones que las adoptan.

En términos generales la operatividad de estas reglas implica que tanto los gobiernos como las empresas u organizaciones exportadoras de datos cumplan los siguientes pasos[182]:

En primer lugar, la autoridad local gubernamental debe aplicar para formar parte del "Cross Border Privacy Enforcement Arrangement" (CPEA) con miras a lograr ayuda y asistencia mutua entre las autoridades de los países miembros de APEC. EL CPEA[183] tiene como objetivo crear un marco de cooperación

181 En la parte introductoria del documento titulado APEC CROSS-BORDER PRIVACY RULES SYSTEM: POLICIES, RULES AND GUIDELINES se advierte que el los CBPR no están destinados para crear obligaciones internacionales vinculantes o afectar a las obligaciones existentes en el marco internacional o ley, o crear obligaciones nacionales en virtud de las leyes y reglamentos de las Economías de APEC.

182 Algunos de ellos son de competencia de las autoridades de cada país y otros de las empresas que deseen transferir desde un país APEC.

183 El CPEA comenzó a funcionar en julio de 2010 con cuatro autoridades. A julio de 2012 hace parte más de 22 autoridades de diferentes países. Es factible que de un país participen varias autoridades.

transfronteriza en la aplicación de las leyes sobre protección de datos y en las eventuales investigaciones de infracciones a las normas sobre dicho tema.

En segundo lugar, las autoridades locales competentes de cada país deben presentar una solicitud para participar en el CBPR System[184]. Actualmente participan los Estados Unidos de Norteamérica, la República Federal de México y Japón[185]. Se espera que, progresivamente, muchos otros países hagan parte del CBPR System. Una vez que el país forma parte del anterior sistema entonces la empresa de cada país que desee participar en el sistema debe acreditarse ante un "Accountability Agent" (AA) reconocido por APEC[186]. Las organizaciones solicitantes serán responsables de la elaboración de sus políticas y prácticas de tratamiento de datos. Sólo podrán participar en el Sistema CBPR si sus políticas y prácticas están certificadas por el AA.

El AA verifica que la empresa u organización que quiera exportar datos reúne los requisitos mínimos que exige APEC[187]. Una vez que la organización ha sido certificada, por un AA, para participar en el Sistema CBPR, sus políticas y prácticas de tratamiento de datos son de obligatorio cumplimiento. La inobservancia de estas puede ser sancionada por las AA o por las autoridades de cada país según el caso.

Para conocer qué empresas están acreditadas por las AA, se creará un directorio de acceso público con los datos de contacto de cada organización. Con esto se da publicidad a las empresas acreditadas ante las AA las cuales quedan habilitadas para transferir datos. Adicionalmente, para que las personas (titulares de los datos), si lo estiman necesario, eleven consultas o reclamos y, eventualmente, se quejen ante las au-

184 Esta es una carta que se remite al Electronic Commerce Steering Group, el Data Privacy Subgroup, y el Joint Oversight Panel de APEC.

185 Japón se unió en abril de 2014 al CBPR. El estudio de los requisitos de Japón y demás cuestiones para hacer parte de dicho sistema puede consultarse en: APEC. 2014. Cross border privacy rules system participation of Japan. Findings report. http://www.apec.org/~/media/Files/Groups/ECSG/CBPR/20140430_CBPR_Japan_Final_Report.pdf (Última consulta: Enero 8 de 2024).

186 "APEC-recognized Accountability Agent."

187 Sobre el particular existe una guía de referencia para la verificación denominada APEC cross-border privacy rules system program requirements.

toridades de control (*Privacy Enforcement Authorities*) si consideran que existe alguna irregularidad.

Debe precisarse que el sistema CBPR no desplaza o deja sin efectos las leyes nacionales ni elimina las responsabilidades de los reguladores nacionales y las autoridades de protección de datos locales. Tampoco exime a una empresa de cumplir con las normas sobre tratamiento de datos personales de cada país. De hecho, es necesario establecer en la regulación nacional si es factible acudir a esta alternativa para transferir datos a otros países. En otras palabras, la aplicación del CBPR en una nación queda condicionada a su permisibilidad o viabilidad jurídica a la luz de las normas locales.

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA

La Directiva 95/46/CE[188] del Parlamento Europeo y del Consejo, de 24 de octubre de 1995 (en adelante Directiva 95/46/CE), fue, antes del actual Reglamento General Europeo de Protección de Datos, el principal documento que fija reglas sobre transferencia internacional de datos. La misma ha impactado mucho en países no europeos en la medida que ha sido el detonador (particularmente el artículo 25) de un proceso de reglamentación en varios países latinoamericanos para alcanzar un nivel adecuado de protección de datos y poder ser receptores de datos personales provenientes de Europa. En enero de 2012 la Comisión Europea presentó al Parlamento Europeo y al Consejo una propuesta de Reglamento sobre la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a su libre circulación, en adelante Reglamento General de Protección de Datos (RGEPD).

188 "relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos". Publicada en el Diario Oficial n° L 281 de 23/11/1995 P. 0031 – 0050.

A continuación, nos referiremos a los aspectos relevantes de la citada Directiva y del RGEPD respecto de las transferencias internacionales con particular énfasis en todo aquello que demuestra el interés de que se garantice el principio de continuidad de datos cuando los datos son transferidos desde un país europeo a un tercer país no europeo.

LA LEGENDARIA Y DEROGADA DIRECTIVA 95/46/CE

Esta Directiva reconoció la necesidad e importancia del flujo internacional de datos personales para diversas actividades como, entre otras, el comercio internacional[189]. Por eso, es libre la circulación transfronteriza entre Estados miembros[190]. Para el caso de transferencias internacionales a Estados no miembros o terceros países, es permitido el envío de datos personales siempre y cuando se cumplan algunos requisitos[191]. El capítulo IV (artículos 25 y 26) de dicha Directiva estableció las principales reglas aplicables sobre el particular, a saber:

En primer lugar, la transferencia de datos personales a un país tercero "únicamente pueda efectuarse cuando, (...), el país tercero de que se trate garantice un nivel de protección adecuado"[192]. En otras palabras, la Directiva no permite la transferencia de datos a terceros países que carezcan de una serie de requisitos para garantizar el debido tratamiento de datos personales[193]. Sobre el nivel adecuado de protección el mismo artículo 25 establece las pautas y factores para evaluar si el país de destino de la transferencia internacional cuenta con dicho grado de protección[194]. Posteriormente nos referiremos un poco más a este tema.

189 En este sentido, en el numeral 56 de los considerandos de la Directiva se reconoce que "los flujos transfronterizos de datos personales son necesarios para el desarrollo del comercio internacional; (...)".
190 El numeral 2 del artículo 1 de la Directiva establece que "Los Estados miembros no podrán restringir ni prohibir la libre circulación de datos personales entre los Estados miembros".
191 En el numeral 56 de los considerandos de la Directiva se afirma que "(...) la protección de las personas garantizada en la Comunidad por la presente Directiva no se opone a la transferencia de datos personales a terceros países que garanticen un nivel de protección adecuado".
192 Numeral 1 del artículo 25 de la Directiva 95/46/CE.
193 En el numeral 57 de los considerandos de la Directiva se establece que "cuando un país tercero no ofrezca un nivel de protección adecuado debe prohibirse la transferencia al mismo de datos personales".
194 En efecto, el numeral 2 del dice que "El carácter adecuado del nivel de protección que ofrece un país ter-

En segundo lugar, tal y como sucede con otros documentos internacionales, existe una serie de casos excepcionales en los que se puede enviar información a países que no tengan nivel adecuado de protección, siempre y cuando se cumplan ciertas circunstancias enunciadas en el artículo 26[195] de la Directiva 95/46/CE.

Finalmente, en el numeral 2 del artículo 26 se da cabida a otras situaciones en las que son permitidos los envíos de datos personales a un país tercero que no garantice un nivel de protección adecuado cuando, entre otras: "el Responsable del tratamiento ofrezca garantías suficientes respecto de la protección de la vida privada, de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los respectivos derechos; dichas garantías podrán derivarse, en particular, de cláusulas contractuales apropiadas"[196]. Sobre esta alternativa nos referiremos más adelante previas las siguientes consideraciones respecto del nivel adecuado de protección de datos.

cero se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos; en particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, así como las normas profesionales y las medidas de seguridad en vigor en dichos países".

195 En efecto, se puede enviar datos a terceros países sin nivel adecuado de protección siempre y cuando: "a) el interesado haya dado su consentimiento inequívocamente a la transferencia prevista, o b) la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales tomadas a petición del interesado, o c) la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar en favor del interesado, entre el responsable del tratamiento y un tercero, o d) La transferencia sea necesaria o legalmente exigida para la salvaguardia de un interés público importante, o para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial, o e) la transferencia sea necesaria para la salvaguardia del interés vital del interesado, o f) la transferencia tenga lugar desde un registro público que, en virtud de disposiciones legales o reglamentarias, esté concebido para facilitar información al público y esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo, siempre que se cumplan, en cada caso particular, las condiciones que establece la ley para la consulta". (numeral 1 del artículo 26 de la Directiva 95/46/CE).

196 Numeral 2 del artículo 26 de la Directiva 95/46/CE.

REGLAMENTO GENERAL EUROPEO DE PROTECCIÓN DE DATOS (RGEPD)

El 25 de enero de 2012 se presentó una propuesta de Reglamento[197] para actualizar la Directiva 95/46/CE la cual fue concebida en una época donde no era masivo el uso de internet ni alta la tasa de penetración de este en el mundo[198]. El proceso culminó con la expedición de REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO (27 de abril de 2016) relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

En los considerandos del Reglamento General Europeo de Protección de Datos (en adelante RGEPD) se resumen las ideas generales del enfoque europeo sobre las transferencias internacionales en la medida que, de una parte, destacan que "los flujos transfronterizos de datos personales a, y desde, países no pertenecientes a la Unión y organizaciones internacionales son necesarios para la expansión del comercio y la cooperación internacionales", pero, de otra parte, son enfáticos en recalcar que, "si los datos personales se transfieren de la Unión a responsables, encargados u otros destinatarios en terceros países o a organizaciones internacionales, esto no debe menoscabar el nivel de protección de las personas físicas garantizado en la Unión por el presente Reglamento, ni siquiera en las transferencias ulteriores de datos personales desde el tercer

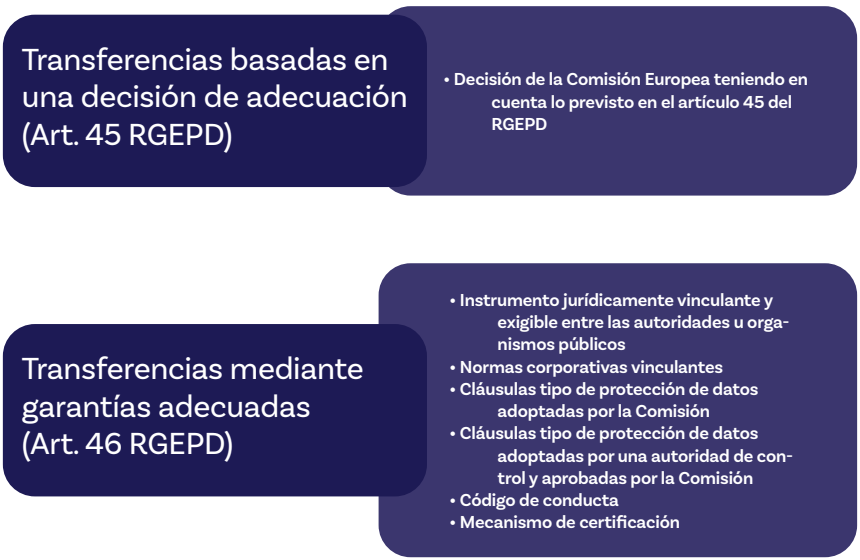
197 Cfr. COMISIÓN EUROPEA. 2012. Propuesta de reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos). (COM(2012) 11 final. 2012/0011 (COD)). El texto de la propuesta puede consultarse en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:ES:PDF

198 Según la Internet World Stats y la Unión Internacional de Telecomunicaciones (UIT), la tasa de penetración de internet en 1995 era del 0.4% de la población mundial. El TJUE, por su parte, señaló en su momento que "el capítulo IV de la Directiva 95/46 no contiene ninguna disposición relativa al uso de Internet. En concreto, no precisa los criterios que permiten determinar si, por lo que se refiere a las operaciones efectuadas a través de proveedores servicios de alojamiento de páginas web, debe tomarse en consideración el lugar de establecimiento del proveedor, su domicilio profesional o bien el lugar en el que se encuentran las computadoras que integran la infraestructura informática del proveedor. (TRIBUNAL DE JUSTICIA DE LA UNION EUROPEA. 2003. Göta hovrätt - Suecia y Bodil Lindqvist. Asunto C-101/01. Apartado 67).

país u organización internacional a responsables y encargados en el mismo u otro tercer país u organización internacional".

La transferencia internacional de datos fue regulada en el capítulo V (Transferencias de datos personales a terceros países u organizaciones internacionales, el cual, entre otras, consagra los siguientes aspectos: **a)** el principio general de las transferencias (artículo 44); **b)** Las pautas sobre las transferencias basadas en una decisión de adecuación (artículo 45); **c)** Las transferencias mediante garantías adecuadas (artículo 46); **d)** Las normas corporativas vinculantes (artículo 47); **e)** Transferencias o comunicaciones no autorizadas por el Derecho de la Unión (artículo 48); **f)** Excepciones para situaciones específicas (artículo 49), y **g)** Cooperación internacional en el ámbito de la protección de datos personales (artículo 50).

A continuación, se resumen las principales alternativas que ofrece el RGEPD para transferir datos personales:



Gráfica 2. Principales alternativas que ofrece el Reglamento General Europeo de Protección de Datos (RGEPD) para transferir datos personales. Elaboración del autor.

Como regla general, establece el reglamento que las transferencias a un tercer país u organización internacional sólo se pueden hacer si el responsable y el encargado del tratamiento cumplen las condiciones establecidas en el reglamento, incluidas las relativas a las transferencias ulteriores de datos personales desde el tercer país u organización internacional a otro tercer país u organización internacional. Con lo anterior, se quiere mantener el principio de continuidad en la protección a los titulares de los datos para que la protección que les ofrece la regulación europea y sus instituciones no se vea disminuido o menoscabado[199].

Las transferencias basadas en la decisión de adecuación no requieren de ninguna autorización cuando el envío de datos se realice a un tercer país, un territorio o uno o varios sectores específicos de ese tercer país, u organización internacional que, según la Comisión, tiene nivel de protección adecuado[200]. El reglamento prevé los elementos que debe tener presente la Comisión para catalogar a un país con nivel adecuado[201].

199 Cfr. Artículo 44 del RGEPD

200 Cfr. Artículo 45 (numeral 1) del RGEPD

201 Según el numeral 2 del artículo 45 del RGEPD estos son los elementos: "a) el Estado de Derecho, el respeto de los derechos humanos y las libertades fundamentales, la legislación pertinente, tanto general como sectorial, incluida la relativa a la seguridad pública, la defensa, la seguridad nacional y la legislación penal, y el acceso de las autoridades públicas a los datos personales, así como la aplicación de dicha legislación, las normas de protección de datos, las normas profesionales y las medidas de seguridad, incluidas las normas sobre transferencias ulteriores de datos personales a otro tercer país u organización internacional observadas en ese país u organización internacional, la jurisprudencia, así como el reconocimiento a los interesados cuyos datos personales estén siendo transferidos de derechos efectivos y exigibles y de recursos administrativos y acciones judiciales que sean efectivos; b) la existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el tercer país o a las cuales esté sujeta una organización internacional con la responsabilidad de garantizar y hacer cumplir las normas en materia de protección de datos, incluidos poderes de ejecución adecuados, de asistir y asesorar a los interesados en el ejercicio de sus derechos, y de cooperar con las autoridades de control de la Unión y de los Estados miembros, y c) los compromisos internacionales asumidos por el tercer país u organización internacional de que se trate, u otras obligaciones derivadas de acuerdos o instrumentos jurídicamente vinculantes, así como de su participación en sistemas multilaterales o regionales, en particular en relación con la protección de los datos personales".

Si el lugar de destino de las transferencias no cuenta con un nivel óptimo se podrán exportar los datos si se conceden garantías como las siguientes: "**a)** un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos; **b)** normas corporativas vinculantes[202]; **c)** cláusulas tipo de protección de datos adoptadas por la Comisión; **d)** cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión; **e)** un código de conducta, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados; o **f)** un mecanismo de certificación, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados"[203].

En lo que atañe, en particular a las transferencias internacionales de datos, cabe señalar que se recalca la responsabilidad del exportador de los datos de observar todas las obligaciones que se incluyen en el reglamento, pero también se establece responsabilidad en el caso de las transferencias ulteriores, es decir, cuando los datos transferidos a un país luego son enviados desde el mismo a otro (s) país (es). En todo caso, se considera necesaria la cooperación internacional[204] con las autoridades de las otras naciones para garantizar el cumplimiento de las normas sobre protección de datos y el respeto de los derechos de las personas.

---

202 El artículo 47 del RGEPD establece los requisitos que deben cumplir las Normas Corporativas Vinculantes.

203 Cfr. Artículo 46 (numeral 2) del RGEPD.

204 Cfr. Artículo 50 del RGEPD: "En relación con los terceros países y las organizaciones internacionales, la Comisión y las autoridades de control tomarán medidas apropiadas para:

a) crear mecanismos de cooperación internacional que faciliten la aplicación eficaz de la legislación relativa a la protección de datos personales;

b) prestarse mutuamente asistencia a escala internacional en la aplicación de la legislación relativa a la protección de datos personales, en particular mediante la notificación, la remisión de reclamaciones, la asistencia en las investigaciones y el intercambio de información, a reserva de las garantías adecuadas para la protección de los datos personales y otros derechos y libertades fundamentales;

c) asociar a partes interesadas en la materia a los debates y actividades destinados a reforzar la cooperación internacional en la aplicación de la legislación relativa a la protección de datos personales;

d) promover el intercambio y la documentación de la legislación y las prácticas en materia de protección de datos personales, inclusive en materia de conflictos de jurisdicción con terceros países".

El RGEPD indica los requisitos que se deben considerar cuando la transferencia sucede en cualquiera de estas hipótesis: **a)** con una decisión de adecuación; **b)** mediante garantías apropiadas, **c)** con normas corporativas vinculantes y **d)** mediante un régimen de excepciones.

Es libre y no requiere de autorizaciones adicionales la transferencia que se realice a organizaciones internacionales, países, una parte del país o un sector de tratamiento (grupo de empresas o empresas de un mismo sector) que hayan sido objeto de una decisión de la Comisión Europea certificando que tienen un nivel de protección adecuado[205]. Respecto a dicho nivel el artículo 45 señala los criterios que deben tenerse para determinar el mismo (la existencia de un Estado de derecho, la legislación general o sectorial de recursos jurisdiccionales, la existencia y funcionamiento efectivo de autoridades de control y los compromisos internacionales asumidos por el país). En este punto, resulta novedosa la posibilidad de aplicación geográfica y sectorial del nivel adecuado dentro de un país.

En el caso que el país no cuente con el nivel adecuado de protección o que se haya proferido una decisión negativa sobre dicho nivel por parte de la Comisión, la transferencia únicamente se podrá efectuar si se ofrecen garantías apropiadas mediante un documento jurídicamente vinculante. En el numeral 2 del artículo 46 se enuncian como garantías apropiadas las siguientes: **a)** normas corporativas vinculantes; **b)** cláusulas tipo de protección de datos adoptadas por la Comisión Europea o por la autoridad de control y **c)** cláusulas contractuales entre el responsable o el encargado del tratamiento y los destinatarios de los datos, autorizadas previamente por la autoridad de protección de datos del país de origen de estos.

205 Cfr. Numeral 1 del artículo 45 del RGEPD: "Podrá realizarse una transferencia de datos personales a un tercer país u organización internacional cuando la Comisión haya decidido que el tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional de que se trate garantizan un nivel de protección adecuado. Dicha transferencia no requerirá ninguna autorización específica".

Las normas corporativas vinculantes son concebidas como una herramienta que permite la transferencia internacional dentro de un grupo de empresas cuyas sedes están ubicadas fuera de la Unión Europea. El artículo 47 del RGEPD establece que las autoridades de control deberán tener en cuenta los siguientes aspectos para aprobar las normas corporativas vinculantes. En primer lugar, que "sean jurídicamente vinculantes y se apliquen a todos los miembros del grupo de empresas del responsable o del encargado del tratamiento, incluidos sus empleados, que asegurarán su cumplimiento". En segundo lugar, que "confieran expresamente a los interesados derechos exigibles" y finalmente que cumplan los requisitos establecidos en el numeral.

Finalmente, si no existe decisión de adecuación ni garantías apropiadas para la transferencia internacional, la misma se podrá realizar excepcionalmente en los casos previstos en el artículo 49 del RGEPD, dentro de los cuales se destaca que el titular del dato "haya dado su consentimiento a la transferencia propuesta, tras haber sido informado de los riesgos que entraña debido a la ausencia de una decisión de adecuación y de garantías apropiadas".

AUTORIDADES INTERNACIONALES DE PROTECCIÓN DE DATOS Y PRIVACIDAD (HOY GPA O GLOBAL PRIVACY ASSEMBLY)

En la trigésima primera Conferencia Internacional de Autoridades de Protección de Datos y Privacidad realizada el 5 de noviembre de 2009 en Madrid (España), se aprobaron los "Estándares Internacionales sobre Protección de Datos Personales y Privacidad (Resolución de Madrid)". Dicho documento no es un instrumento internacional jurídicamente vinculante, pero tiene el mérito de contar con la aprobación de casi 50 autoridades provenientes de diversos países y continentes.

En el numeral 15 de la Resolución de Madrid se incluyeron los supuestos bajo los cuales es permitida la transferencia in-

ternacional de datos, cuyos aspectos fundamentales son los siguientes:

En primer lugar, se permite como regla general la TIDP a países que tengan el nivel de protección que confiere la Resolución de Madrid[206]. En segundo lugar, si el país de destino no tiene dicho grado de protección entonces se permite la transferencia cuando "quien pretenda transferir dichos datos garantice que el destinatario ofrecerá dicho nivel de protección"[207]. En otras palabras, el remitente de los datos debe asegurar que el receptor de los datos en otro país garantizará el nivel de protección de la Resolución de Madrid. Para el efecto, se podrán utilizar cláusulas contractuales o normas corporativas vinculantes, cuando la transferencia se realice entre organizaciones que hacen parte de entidades multinacionales.

En todo caso el remitente de los datos será el responsable de garantizar que la transferencia cumpla los requisitos exigidos por la Resolución de Madrid y, en caso de ser requerido, debe acreditar que ello es así ante la autoridad de protección de datos[208].

En tercer lugar, los Estándares dejan abierta la posibilidad para que las autoridades de protección de datos tengan la facultad de aprobar previamente la realización de todas o algunas TIDP. En otras palabras, el mecanismo de protección de los derechos de los titulares se materializa a través del control previo de la TIDP por parte de las autoridades locales[209].

206 Cfr. Numeral 1 del artículo 15 de la Resolución de Madrid.
207 Cfr. Numeral 2 del artículo 15 de la Resolución de Madrid.
208 En efecto, el numeral 4 del artículo 15 de la Resolución de Madrid establece que "quien pretenda realizar una transferencia internacional de datos de carácter personal deberá poder acreditar que la transferencia cumple las garantías establecidas en el presente Documento, y en particular cuando así le fuera requerido por las autoridades de supervisión en cumplimiento de las facultades previstas en el apartado 23.2".
209 De conformidad con el artículo 23 de la Resolución de Madrid, "1. En cada Estado existirán una o más o autoridades de supervisión que, de acuerdo con su derecho interno, serán responsables de supervisar la observancia de los principios establecidos en el presente Documento.
2. Dichas autoridades de supervisión deberán ser imparciales e independientes, y contarán con la cualificación técnica, las competencias suficientes y los recursos adecuados para conocer de las reclamaciones que le sean dirigidas por los interesados, y para realizar las investigaciones e intervenciones que resulten necesarias para garantizar el cumplimiento de la legislación nacional aplicable en materia de protección de la privacidad en relación con el tratamiento de datos de carácter personal.".

RED IBEROAMERICANA DE PROTECCIÓN DE DATOS (RIPD)

La Red Iberoamericana de Protección de Datos (RIPD) fue fundada en junio de 2003 en La Antigua, Guatemala, durante el seminario sobre protección de datos personales en Iberoamérica[210] "impulsado por la Agencia Española de Protección de Datos (AEPD), con el apoyo de la Agencia Española de Cooperación Internacional (AECI) y la Fundación Internacional y para Iberoamérica de Administración y Políticas Públicas (FIIAPP)"[211]. A dicho evento acudieron autoridades de protección de datos, funcionarios públicos y académicos de Europa[212] y Latinoamérica[213].

En las directrices de la RIPD se adoptan reglas sobre TIDP similares a las analizadas en casos anteriores. En efecto, en el numeral 8[214] se estableció como regla general que sólo pueden "efectuarse transferencias internacionales de datos al territorio de Estados cuya legislación recoja lo dispuesto en las presentes directrices". Con esto se replica el cometido de exigir como presupuesto de la transmisión que se verifique el país de destino en tanto garantiza un nivel similar al del garantizado en el país de origen.

Adicionalmente, las directrices dejan abierta la posibilidad que se recurra a la utilización de garantías apropiadas a la luz de las autoridades locales de protección de datos[215] para

210 Sobre la historia de la RIPD consúltese la página web de la misma http://www.redipd.org/index-ides-idphp.php, particularmente la siguiente sección http://www.redipd.org/la_red/Historia/index-ides-idphp.php

211 Declaración de la Antigua (Guatemala) del II encuentro Iberoamericano de protección de datos (2-6 de junio de 2003) publicada en el siguiente libro: PIÑAR MAÑAS, José Luis, ed. 2006. *La Red Iberoamericana de Protección de Datos.* Declaraciones y documentos. Primera ed. Valencia, España: Tirant Lo Blanch. Agencia Española de Protección de Datos. P 13. Sobre esta Red y propuestas sobre el rol de la misma véase el siguiente capítulo de libro: TRAVIESO, Juan Antonio. 2005. *La protección de los datos personales en América Latina: Unidos o desprotegidos hacia una red iberoamericana de protección de datos personales.* Protección de datos de carácter personal en Iberoamérica, editado por J. L. Piñar. Valencia: Tirant Lo Blanch. p 85-93.

212 España y Portugal.

213 Argentina, Brasil, Chile, Costa Rica, El Salvador, Guatemala, México, Nicaragua, Perú, Portugal y Uruguay.

214 Denominado "Limitaciones a la transferencia internacional de datos".

215 De conformidad con el numeral 9.3 de las directrices, corresponde a las autoridades de protección de datos "autorizar, cuando sea preciso, las transferencias internacionales de datos a Estados cuya legis-

asegurar que quien reciba los datos cumplirá lo dispuesto en las directrices. En efecto, según el 8.3. de las directrices "sólo será posible la transferencia internacional de datos en caso de que se obtenga la autorización de la autoridad a la que se refiere el apartado 9, para lo cual será necesaria la aportación por parte del exportador de garantías suficientes para asegurar que el importador cumplirá en todo caso lo dispuesto en estas directrices".

Posteriormente, en 2017, la RIPD aprobó los Estándares de protección de datos personales para los países Iberoamericanos[216], los cuales "constituyen en un conjunto de directrices orientadoras que contribuyan a la emisión de iniciativas regulatorias de protección de datos personales en la región iberoamericana de aquellos países que aún no cuentan con estos ordenamientos, o en su caso, sirvan como referente para la modernización y actualización de las legislaciones existentes". Estos estándares siguen de cerca los lineamientos del Reglamento General Europeo de Protección de Datos (RGEPD).

Respecto a las transferencias internacionales los Estándares de la RIPD se refieren al tema de la siguiente manera:

En primer lugar, en la definición incluye la de "exportador" como la "persona física o jurídica de carácter privado, autoridad pública, servicios, organismo o prestador de servicios situado en territorio de un Estado que efectúe transferencias internacionales de datos personales, conforme a lo dispuesto en los presentes Estándares"[217]. Adicionalmente, incluye las transferencias como una actividad que hace parte de concepto de Tratamiento[218].

En el capítulo V incorpora el reglamento sobre las transferencias internacionales. Allí se señalan algunas reglas generales para que los Responsables o los Encargados puedan realizar transferencias internacionales, a saber:

---

lación no recoja lo dispuesto en las presentes directrices".

216 Estándares aprobados en el XV Encuentro de la RIPD, que tuvo lugar en Santiago de Chile, Chile, el 22 de junio de 2017.

217 Cfr. Literal f) del artículo 2.1. de los Estándares de la RIPD.

218 Cfr. Literal i) del artículo 2.1. de los Estándares de la RIPD.

Alternativas	
NIVEL ADECUADO DE PROTECCIÓN DE DATOS	El país, parte de su territorio, sector, actividad u organización internacional destinatario de los datos personales tiene nivel adecuado de protección de datos personales reconocido por el país transferente o exportador de la información[219]. El país destinatario o varios sectores de este acreditan condiciones mínimas y suficientes para garantizar un nivel de protección de datos personales adecuado[220].
GARANTÍAS DE DEBIDO TRATAMIENTO DE DATOS EN EL PAÍS DE DESTINO	El exportador ofrece garantías suficientes del tratamiento de los datos personales en el país destinatario, y éste, a su vez, acredita el cumplimiento de las condiciones mínimas y suficientes establecidas en la legislación nacional de cada Estado Iberoamericano[221].
USO DE CLÁUSULAS CONTRACTUALES	El exportador y destinatario suscriben cláusulas contractuales o cualquier otro instrumento jurídico que ofrezca garantías suficientes y que permita demostrar el alcance del tratamiento de los datos personales, las obligaciones y responsabilidades asumidas por las partes y los derechos de los titulares. La autoridad de control podrá validar cláusulas contractuales o instrumentos jurídicos según se determine en la legislación nacional[222].
MECANISMOS DE AUTORREGULACIÓN O CERTIFICACIÓN	El exportador y destinatario adoptan un esquema de autorregulación vinculante o un mecanismo de certificación aprobado, siempre y cuando éste sea acorde con las disposiciones previstas en la legislación nacional del Estado Iberoamericano[223].
AUTORIZACIÓN DE LA AUTORIDAD DE CONTROL	La autoridad de control del Estado Iberoamericano del país del exportador autoriza la transferencia en términos de la legislación nacional que resulte aplicable en la materia[224].

Tabla 1. Alternativas jurídicas para realizar transferencias internacionales según los Estándares de protección de datos personales para los países Iberoamericanos de la RIPD. Elaboración del autor.

En cuanto a los mecanismos de autorregulación, estos pueden ser códigos deontológicos, sistemas de certificación y sus respectivos sellos de confianza que contribuyen a garantizar un debido tratamiento de los datos personales. Precisan los Estándares de la RIPD que "el responsable podrá adherirse, de manera voluntaria, a esquemas de autorregulación vinculante, que tengan por objeto, entre otros, contribuir a la correcta aplicación

219 Cfr. Literal a) del artículo 36.1. de los Estándares de la RIPD.
220 Cfr. Literal a) del artículo 36.1. de los Estándares de la RIPD.
221 Cfr. Literal b) del artículo 36.1. de los Estándares de la RIPD.
222 Cfr. Literal c) del artículo 36.1. de los Estándares de la RIPD
223 Cfr. Literal d) del artículo 36.1. de los Estándares de la RIPD.
224 Cfr. Literal e) del artículo 36.1. de los Estándares de la RIPD.

de la legislación nacional del Estado Iberoamericano que resulte aplicable en la materia y establecer procedimientos de resolución de conflictos entre el responsable y titular sin perjuicio de otros mecanismos que establezca la legislación nacional de la materia aplicable, teniendo en cuenta las características específicas de los tratamientos de datos personales realizados, así como el efectivo ejercicio y respeto de los derechos del titular"[225].

ORGANIZACIÓN DE ESTADOS AMERICANOS (OEA)

El 9 de abril de 2021, el Comité Jurídico Interamericano (CJI), órgano consultivo de la Organización de Estados Americanos (OEA), aprobó por unanimidad los "Principios actualizados sobre la privacidad y la protección de datos personales, con anotaciones"[226].

Esta nueva versión reemplaza la expedida en 2015, y constituye un estándar normativo para los países del continente americano, en especial para aquellos que aún no poseen legislación en la materia, o que están en proceso de actualización de la misma, con el objetivo de impulsar la armonización jurídica en el continente[227].

Los principios actualizados representan un aporte de la OEA en el escenario internacional de la protección de datos. Como novedades más significativas puede destacarse el aumento del número de principios, que pasan de 11 a 13, con la inclusión de la Autoridad de Protección de Datos (principio 13) y las excepciones (principio 12). Se amplía asimismo el alcance de los principios existentes. Así ha ocurrido, por ejemplo, con el principio de responsabilidad (principio 10) o el catálogo de derechos que incorpora: acceso, rectificación, cancelación, oposición y portabilidad (principio 8).

225 Cfr. Artículo 40 de los Estándares de la RIPD.

226 El texto puede consultarse en: https://www.redipd.org/sites/default/files/2021-05/CJI-doc_638-21.pdf

227 Esta parte sobre la OEA fue tomada de la siguiente noticia publicada por la Red Iberoamericana de Protección de Datos (RIPD): El Comité Jurídico Interamericano aprueba los Principios Actualizados sobre Privacidad y Protección de Datos Personales. Publicada el 12 de mayo de 2021 en: https://www.redipd.org/es/noticias/el-comite-juridico-interamericano-aprueba-los-principios-actualizados-sobre-privacidad-y

Otro avance a destacar es la incorporación por primera vez en estos principios de una perspectiva transversal de género y derechos humanos en su interpretación. Además, se ha establecido de manera expresa una recomendación de establecer salvaguardias especiales en casos de tratamiento de datos sensibles que suponen un alto riesgo. Finalmente, se recalcó que los principios son de aplicación neutral frente al tratamiento de datos con cualquier tecnología presente o futura.

Finalmente, la Asamblea General de la OEA, por su parte, aprobó en noviembre de 2021 los precitados Principios Actualizados sobre La Privacidad y La Protección de Datos Personales elaborados por el Comité Jurídico Interamericano (CJI). Según la Secretaría de Asuntos Jurídicos del Departamento de Derecho Internacional de la OEA, "los Principios Actualizados[228], como instrumento de *soft law* interamericano tienen por objetivo servir a los Estados miembros como punto de referencia para el fortalecimiento de sus respectivos marcos jurídicos en la materia, y orientar el desarrollo colectivo de la región hacia una protección armónica y efectiva de los datos personales"[229].

Respecto de transferencias internacionales el principio 11 dice lo siguiente:

> "PRINCIPIO ONCE. Flujo Transfronterizo de Datos y Responsabilidad.
>
> Reconociendo su valor para el desarrollo económico y social, los Estados Miembros deberían cooperar entre sí para facilitar el flujo transfronterizo de datos personales a otros Estados cuando éstos confieran un nivel adecuado de protección de los datos de conformidad con estos Principios. Asimismo, los Estados Miembros deberían

228 Los Principios Actualizados sobre la Privacidad y Protección de Datos Personales, pueden consultarse en: https://www.oas.org/es/sla/cji/docs/CJI-doc_638-21.pdf

229 Cfr. Durante su 51º Periodo Ordinario de Sesiones, celebrado del 10 al 12 de noviembre pasados, la Asamblea General de la OEA aprobó los Principios Actualizados sobre La Privacidad y La Protección de Datos Personales elaborados por el Comité Jurídico Interamericano (CJI). En: https://www.oas.org/es/sla/ddi/boletines_informativos_CJI_Asamblea_General_OEA_Aprueba_Principios_Actualizados_Privacidad_Proteccion_Datos_Personales_Noviembre-2021.html

> cooperar en la creación de mecanismos y procedimientos que aseguren que los responsables y encargados del tratamiento de datos que operen en más de una jurisdicción, o los transmitan a una jurisdicción distinta de la suya, puedan garantizar y ser efectivamente hechos responsables por el cumplimiento de estos Principios."

En las anotaciones sobre dicho principio se reconoce que "un reto fundamental para una política y una práctica eficaces en materia de protección de Datos consiste en conciliar **1)** las diferencias en los enfoques nacionales de la protección de la privacidad con la realidad moderna del flujo mundial de Datos; **2)** los derechos de las personas a tener acceso a Datos en un contexto transnacional; y **3)** el hecho fundamental de que los Datos y el Tratamiento de Datos impulsan el desarrollo y la innovación. Todos los instrumentos internacionales para la protección de Datos procuran alcanzar un equilibrio apropiado entre esas metas."

Los principios actualizados de 2021 de la OEA recalcan que "los Responsables de Datos que transfieran Datos Personales a través de fronteras deberían asumir la responsabilidad de asegurar un grado continuo de protección que sea acorde con estos Principios". Para dicho efecto, entre las medidas razonables, se citan los acuerdos o disposiciones contractuales mediante las cuales se fijen pautas para que se protejan los datos. Al respecto se señala lo siguiente: "En general, estas obligaciones deberían reconocerse en acuerdos apropiados, en disposiciones contractuales o por medio de salvaguardias técnicas e institucionales de la seguridad, procesos para la tramitación de quejas, auditorías y medidas similares. La idea es facilitar el flujo necesario de Datos Personales entre Estados Miembros y, al mismo tiempo, garantizar el derecho fundamental de las personas a la protección de sus Datos Personales"[230].

230 Cfr. OEA (2021) *Principios Actualizados sobre La Privacidad y La Protección de Datos Personales elaborados por el Comité Jurídico Interamericano.* Pág. 27.

COMUNIDAD ANDINA DE NACIONES (CAN)

Mediante la Decisión Andina 897[231] del 14 de julio de 2022 de la Comunidad Andina de Naciones (CAN) se sustituyó la Decisión 638 de la CAN relativa a los Lineamientos para la Protección de los Derechos de los Usuarios de Servicios de Telecomunicaciones. Por primera vez, se incluyó un capítulo sobre tratamiento de datos personales (Capítulo II. Protección de los derechos de los usuarios respecto a la propiedad, tratamiento y circulación de los datos personales).

En la Decisión se define el flujo transfronterizo de datos personales como la "Transferencia internacional de datos personales a un destinatario situado en un país distinto al país de origen de los datos personales, sin importar el soporte en que estos se encuentren, los medios por los cuales se efectuó la transferencia ni el tratamiento que reciban"[232]. En el artículo 6, denominado "libre circulación de datos personales ", se establecen las siguientes pautas:

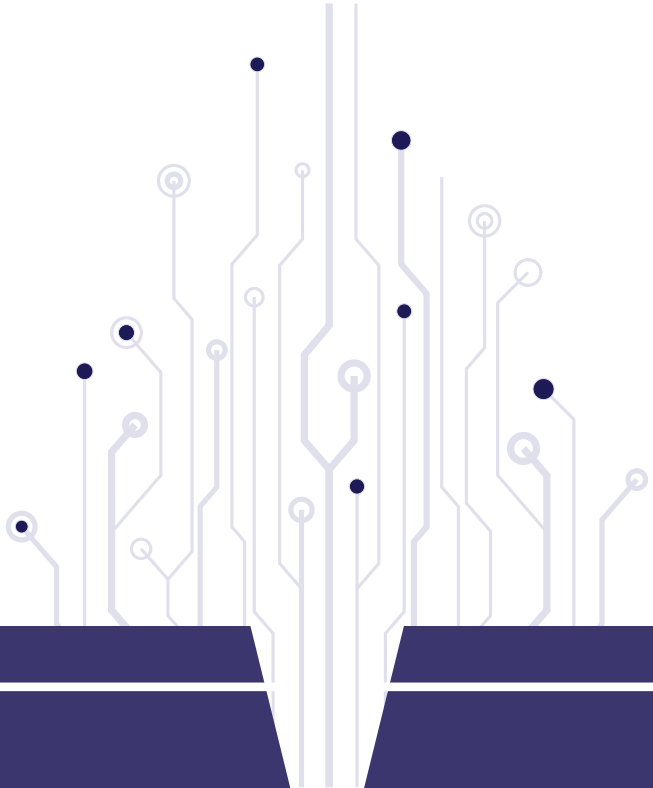
En primer lugar, se permite la libre circulación de los datos personales dentro de los Países Miembros de la Comunidad Andina (Colombia, Ecuador, Perú y Bolivia), "cuando el país destinatario de los datos personales hubiere sido reconocido como uno que cuenta con un nivel adecuado de protección de datos personales" por parte del país desde el cual se exportarán o enviarán los datos. En segundo lugar, si la nación destinataria no tiene nivel adecuado de protección, se debe acudir a las alternativas jurídicas establecidas en la regulación nacional de cada país para exportar o transferir datos personales a otras naciones.

231 Publicada en la Gaceta Oficial del Acuerdo de Cartagena No. 4499 del 14 de juio de 2022. El texto oficial está disponible en: https://www.comunidadandina.org/DocOficialesFiles/Gacetas/GACETA%204499.pdf
232 Cfr. Artículo 3 (Definiciones) de la Decisión Andina 897 de 2022 de la CAN.

Esta Decisión es muy importante porque por primera vez, a nivel Andino, se regula este tema y dicha norma de aplicación obligatoria, inmediata y supranacional impacta en países que aún no tienen regulación sobre protección de datos personales. En ese sentido, en ese país, al igual que Colombia, Ecuador y Perú, también se "reconoce y garantiza el derecho que tienen todos los usuarios de la Comunidad Andina al debido tratamiento de sus datos personales y a la titularidad sobre los mismos, así como el derecho de acceso, uso, rectificación, eliminación, cancelación, oposición, limitación al tratamiento o circulación de estos y a la portabilidad de su información"[233]. Adicionalmente, se establecen los siguientes principios que deben observarse en el tratamiento de dicha información: "licitud; lealtad; legitimación; transparencia; finalidad; proporcionalidad; calidad, veracidad y exactitud; seguridad; confidencialidad y responsabilidad demostrada"[234].

233 Cfr. Artículo 4 de la Decisión Andina 897 de 2022 de la CAN.
234 **Cfr. Artículo 4 de la Decisión Andina 897 de 2022 de la CAN.**

LOS CONTRATOS COMO ALTERNATIVA PARA EXPORTAR DATOS PERSONALES



Es común afirmar que los contratos son acuerdos de voluntades (pactum est conventio voluntatum) y que se constituyen en "ley entre las partes" (*pactum inter partes est lex*). Aunque este no es un espacio enfocado en profundizar sobre la teoría de los contratos, vale la pena mencionar que los mismos se rigen por principios generales que evocan los grandes mensajes de lo que espera el regulador que sea el mundo ideal de la contratación.

En ese sentido, los principios UNIDROIT (2016) sobre contratos comerciales internacionales consagran, entre otros, los siguientes principios[235]:

Gráfica. Algunos fundamentos de los PRINCIPIOS UNIDROIT SOBRE LOS CONTRATOS COMERCIALES INTERNACIONALES (2016).

235 El texto puede consultarse en: https://www.unidroit.org/wp-content/uploads/2021/06/Unidroit-Principles-2016-Spanish-bl.pdf

Los contratos representan una alternativa jurídica excepcional para facilitar la circulación internacional de datos personales. Favorece tanto a las empresas de países no catalogados con nivel adecuado de protección que deseen "importar" datos personales provenientes de los estados miembros de la Comunidad Europea como a las empresas de dicha comunidad que deseen "exportar" tal información a terceros países bajo la precitada circunstancia. En este sentido, "Las cláusulas contractuales tipo son sólo una de las diversas posibilidades (...) para la transferencia legítima de datos personales a un tercer país (...). Facilitarán enormemente a las entidades la transferencia de datos personales a terceros países mediante la incorporación de las cláusulas contractuales tipo en un contrato"[236].

Desde la academia[237] se ha recomendado el uso de las cláusulas contractuales para las transferencias internacionales como, entre otras, una herramienta de accountabilty (responsabilidad demostrada). En concreto, se sugiere articular herramientas de accountability en un contrato ajustado a las particularidades de cada transferencia.

En 2018, por ejemplo, mediante la "Guía GECTI para la implementación del principio de responsabilidad demostrada -accountability- en las transferencias internacionales de datos personales. Recomendaciones para los países latinoamericanos"[238] se ponía de manifiesto que los contratos representan una alternativa jurídica para demostrar la implementación de medidas de accountability en las transferencias internacionales de datos. Aunque existen modelos de contratos en esta materia, es crucial que el contrato sea consistente con las peculiaridades y necesidades de cada organización y la regulación de cada país. Asimismo, es relevante que el exportador

236 Cfr. Numeral 5 de los considerandos de la Decisión 2001/497/CE.

237 Cfr. Remolina Angarita, Nelson. Álvarez Zuluaga, Luisa Fernanda. (2018). *Guía GECTI para la implementación del principio de responsabilidad demostrada -accountability- en las transferencias internacionales de datos personales.* Recomendaciones para los países latinoamericanos. Universidad de los Andes (Bogotá, Colombia). Facultad de Derecho. GECTI, 1-58.. ISBN: 978-958-774-696-9 ISBN e-book: 978-958-774-697-6 En: https://habeasdatacolombia.uniandes.edu.co/?p=2817

238 El texto de la guía GECTI puede consultarse en: https://habeasdatacolombia.uniandes.edu.co/?p=2817

de los datos trate de establecer si el receptor de los datos en otro país es una empresa u organización seria y responsable (no un paraíso informático) que cumplirá las obligaciones contractuales.

Para la redacción del contrato, se sugería que se tuviese en cuenta varios aspectos:

- "La naturaleza jurídica de los datos que se exportarán a otro país. Según sea aquella (sensible, de menores de edad, privada, semiprivada, pública), pacte medidas especiales de protección. Recuerde, por ejemplo, que para el tratamiento de datos sensibles se exige una responsabilidad reforzada, es decir, mayores medidas de seguridad, mayores restricciones de acceso, uso y circulación.
- Las medidas de seguridad que debe cumplir el destinatario (importador) de los datos exportados a otro país.
- La cantidad de datos que se exportarán.
- ¿Cuáles son los derechos que el destinatario de la información o importador debe garantizar al titular del dato?
- ¿Cuáles son los principios del tratamiento de datos personales que el importador o destinatario de los datos debe observar o garantizar?
- ¿Quiénes podrán tener acceso a la información exportada?
- Los mecanismos para que el titular del dato pueda ejercer sus derechos de manera sencilla y expedita ante el destinatario de los datos exportados.
- Las finalidades para las cuales se transfiere los datos. Es muy importante dejar claro qué puede y qué no puede hacer el destinatario de los datos transferidos.
- ¿Cuál será el límite de tiempo durante el cual el destinatario de los datos transferidos podrá tratarlos?
- La ley de protección de datos que regirá el contrato. Será la ley del país del exportador de los datos o la del importador de estos. Si se quiere garantizar el principio de "continuidad de protección de datos" a que nos referimos en este documento, lo recomendable es que el contrato se rija por la ley de protección de datos del país desde donde se exportarán.

- La posibilidad o no de realizar transferencias ulteriores a otros países. Deje claro si los datos inicialmente transferidos a un país (A) pueden ser transferidos luego desde ese país (A) a otro país (B). En caso positivo, establezca las condiciones que se deben observar para dicho efecto.
- ¿Qué hacer para recuperar los datos transferidos y garantizar los derechos de los titulares de ellos cuando el destinatario de la exportación incumpla el contrato?
- ¿Quién o quiénes responderán ante la autoridad de protección de datos o los titulares de los datos por un eventual indebido tratamiento de la información exportada y por los daños y perjuicios causados?
- ¿Cuál será la responsabilidad (conjunta o solidaria) del exportador y del importador de los datos frente al titular de estos por las eventuales vulneraciones de sus derechos o los daños y perjuicios causados?
- ¿Qué se hará con los datos una vez termine el contrato?"[239]

Esta guía académica fue tenida en cuenta por la Superintendencia de Industria y Comercio —autoridad colombiana de protección de datos— para emitir en 2019 la *Guía para la implementación del principio de responsabilidad demostrada en las transferencias internacionales de datos personales*[240].

Autoridades de protección de datos latinoamericanas también han recomendado el uso de los contratos para los fines mencionados. En el caso de los Estados Unidos Mexicanos, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) emitió en mayo de 2022 las *Recomendaciones para los sujetos obligados en las comunicaciones de datos personales.* Allí, entre otras se señala que "toda transferencia de datos personales que realicen los

239 Cfr. Remolina Angarita, Nelson. Álvarez Zuluaga, Luisa Fernanda. (2018). Guía *GECTI para la implementación del principio de responsabilidad demostrada -accountability- en las transferencias internacionales de datos personales. Recomendaciones para los países latinoamericanos.* Universidad de los Andes (Bogotá, Colombia). Facultad de Derecho. GECTI, 1-58.. ISBN: 978-958-774-696-9 ISBN e-book: 978-958-774-697-6 En: https://habeasdatacolombia.uniandes.edu.co/?p=2817

240 El texto de la guía puede consultarse en: https://www.sic.gov.co/sites/default/files/files/pdf/Gu%C3%ADa%20%20SIC%20para%20la%20implementaci%C3%B3n%20del%20principio%20de%20responsabilidad%20demostrada%20en%20las%20transferencias%20internacionales(1).pdf

responsables deberá constar por escrito a través de cláusulas contractuales, convenios de colaboración o cualquier otro instrumento jurídico que decida el responsable, siempre y cuando permita acreditar su existencia, alcance del tratamiento, así como las obligaciones y responsabilidades contraídas por las partes"[241].

Puntualiza el INAI que "las obligaciones tanto del responsable como del receptor es cumplir con los ocho principios de licitud, lealtad, consentimiento, información, proporcionalidad, finalidad, calidad y responsabilidad y dos deberes de confidencialidad y seguridad que establece la Ley General, anteriormente descritos, así como documentar cada una de las obligaciones de cumplimiento, ya que es importante señalar que la carga de la prueba para acreditar el cumplimiento de las obligaciones previstas en la Ley de la materia recaerá, en todo momento, en el responsable"[242].

LAS CLÁUSULAS CONTRACTUALES DE LA RED IBEROAMERICANA DE PROTECCIÓN DE DATOS (RIPD)

Recientemente los países iberoamericanos miembros de la RIPD han aprobado la *Guía de implementación de las cláusulas contractuales modelo para la transferencia internacional de datos personales (TIDP)*. El texto fue redactado por el experto argentino y profesor Pablo Palazzi. Adicionalmente, contó con el apoyo y observaciones de los miembros de la RIPD y de terceros que, dentro del proceso de elaboración, presentaron sus opiniones o sugerencias. La Guía de CCM[243] va acompañada de

241 ESTADOS UNIDOS MEXICANOS. Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (2022). *Recomendaciones para los sujetos obligados en las comunicaciones de datos personales*, pág. 16. En: https://home.inai.org.mx/wp content/documentos/DocumentosSectorPublico/Recomendaciones-SO_Comun_DP.pdf

242 ESTADOS UNIDOS MEXICANOS. Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (2022). Recomendaciones para los sujetos obligados en las comunicaciones de datos personales. Pág. 21 En: https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPublico/Recomendaciones-SO_Comun_DP.pdf

243 El texto de la guía y el anexo (Modelos de cláusulas contractuales) se pueden consultar en la página web de la RIPD: https://www.redipd.org/es/documentos/guias

un anexo que contiene dos modelos para transferir internacionalmente, a saber:

- Acuerdo modelo de transferencia internacional de datos personales entre responsable y responsable.
- Acuerdo modelo de transferencia internacional de datos personales entre responsable y encargado.

Para su redacción se tuvieron en cuenta los antecedentes sobre las transferencias internacionales de datos personales (TIDP), en especial aquellos que dan vía libre al uso de los contratos como una alternativa para legitimar el envío de datos personales de un país a otro (s) país (es). Adicionalmente se consideraron los lineamientos sobre cláusulas contractuales en Europa[244]. Obviamente, se hizo referencia a lo previsto en los Estándares de 2017 de la RIPD y la regulación local de algunos países[245] de la RIPD que expresa o tácitamente se refieren a las TIDP y las cláusulas contractuales.

Para la RIPD, el objetivo de las cláusulas contractuales modelo (CCM) "es garantizar y facilitar el cumplimiento de los requisitos previstos por la ley de protección de datos del país del Exportador de datos para la transferencia de datos personales a un tercer país que no haya sido reconocido con un nivel adecuado de protección. La idea es que la protección, inicialmente otorgada a los datos personales, siga presente con independencia del lugar donde estos datos se encuentren. Es por lo que también se regulan las Transferencias ulteriores con recaudos para evitar la disminución del nivel de protección. Se da intervención a los Titulares a través de un concepto uni-

244 Se tuvieron presente, entre otros los siguientes textos: (1) DECISIÓN DE EJECUCIÓN (UE) 2021/914 DE LA COMISIÓN de 4 de junio de 2021 relativa a las cláusulas contractuales tipo para la transferencia de datos personales a terceros países de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo. Disponibles en: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:-32021D0914&from=EN#ntr2-L_2021199ES.01003701-E0002 ; (2) DECISIÓN DE EJECUCIÓN (UE) 2021/914 DE LA COMISIÓN de 4 de junio de 2021 relativa a las cláusulas contractuales tipo para la transferencia de datos personales a terceros países de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo. Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32021D0914&from=EN#ntr2-L_2021199ES.01003701-E0002

245 Argentina, Brasil, Cabo Verde, Colombia, Ecuador, México, Nicaragua, Panamá, Perú, República Democrática de Santo Tomé y Príncipe, República Dominicana y Uruguay.

versal del derecho de los contratos denominado Tercero beneficiario. Y se regula el acceso por parte de autoridades en la jurisdicción del Importador de datos que puedan afectar derechos del Titular"[246].

La Guía incorpora en el glosario las siguientes definiciones útiles para entender la redacción de las CCM:

- **Encargado**: prestador de servicios que, con el carácter de persona física o jurídica o autoridad pública, ajena a la organización del Responsable, trata datos personales a nombre y por cuenta de éste.
- **Exportador de datos**: persona física o jurídica de carácter privado, autoridad, servicios, organismo o prestador de servicios situado en territorio de un Estado que efectúe transferencias internacionales de datos personales, conforme a lo dispuesto en los presentes Estándares.
- **Importador de datos**: persona física o jurídica de carácter privado, autoridad, servicios, organismo o prestador de servicios situado en un tercer país que recibe datos personales de un Exportador de datos mediante una transferencia internacional de datos personales.
- **Responsable**: persona física o jurídica de carácter privado, autoridad, servicios u organismo que, solo o en conjunto con otros, determina los fines, medios, alcance y demás cuestiones relacionadas con un tratamiento de datos personales.
- **Sub encargado**: cuando un Encargado del tratamiento recurre a otro Encargado para llevar a cabo determinadas actividades de tratamiento por cuenta del responsable.
- **Terceros beneficiarios**: Titular cuyos datos personales son objeto de una transferencia internacional en virtud del presente Acuerdo. El Titular es un tercero beneficiario de los derechos dispuestos en su favor en las CCM y por ende puede ejercer los derechos que las CCM le reconoce, aunque no haya suscrito el contrato modelo entre las partes.

246 Cfr. RIPD. *Guía de implementación de las cláusulas contractuales modelo para la transferencia internacional de datos personales (TIDP)*, pág. 16.

- **Transferencia ulterior**: Transferencia de datos realizada por el Importador de datos a un tercero situados fuera de la jurisdicción del Exportador de datos que cumple las garantías establecidas en las CCM"[247].

Según RIPD, las CCM son un instrumento "listo para usar" y "listo para ejecutar"[248] de manera fácil, sencilla e inmediata. Señala la RIPD que "las CCM son el mecanismo legal más accesible y utilizado hoy en día para la TIDP a jurisdicciones no adecuadas. Se calcula que cerca del 80 al 90% de empresas que implementan mecanismos de TIDP utilizan como solución a las CCM"[249].

Las siguientes son algunas ventajas y beneficios de utilizar las CCM:

- Superar eventuales limitaciones a las TIDP cuando entre el país exportador y el país de destino tienen diferentes niveles de protección de datos. Vía contractual se crean estándares comunes de protección de datos.
- Se promueven la armonización regulatoria de niveles sensatos de protección de datos personales entre exportadores e importadores de esa clase de información.
- Se alcanza un equilibrio contractual entre las partes al contar con modelos de cláusulas elaboradas por terceros expertos en tratamiento de datos personales y no por la parte fuerte del contrato.
- Se genera confianza entre las partes y los titulares de los datos al usar un modelo de contrato preaprobado por expertos y autoridades de datos.
- Se reducen costos en las transferencias porque no es necesario que las empresas acudan a sus asesores internos o externos para elaborar o redactar el contrato (eliminación de costos de honorarios profesionales).

247 Cfr. RIPD. *Guía de implementación de las cláusulas contractuales modelo para la transferencia internacional de datos personales (TIDP)*, págs. 25-26.
248 Cfr. RIPD. *Guía de implementación de las cláusulas contractuales modelo para la transferencia internacional de datos personales (TIDP)*, pág. 17.
249 Cfr. RIPD. *Guía de implementación de las cláusulas contractuales modelo para la transferencia internacional de datos personales (TIDP)*, pág. 18.

Son una buena noticia para quienes desean exportar datos a países que no tienen nivel adecuado de protección porque el proceso de conceder el "nivel adecuado" ha mostrado ser muy demorado, engorroso y muy formalista[250] porque se centra en comparar regulaciones y no en verificar si se cumplen en la práctica.

PRIMEROS PAÍSES LATINOAMERICANOS EN APROBAR LOS MODELOS DE CLÁUSULAS CONTRACTUALES DE LA RIPD

Las CCM de la RIPD han tenido rápida acogida por parte de países latinoamericanos como Perú, Uruguay y Argentina cuyos principales motivos para darles la bienvenida en sus regulaciones locales destacamos a continuación:

REPÚBLICA DEL PERÚ

Mediante la Resolución Directoral N.º 0074-2022-JUS/DGTAIPD del 17 de octubre de 2022 del Ministerio de Justicia y Derechos Humanos, la Autoridad Nacional de Protección de Datos Personales de la República del Perú (ANPD)[251] aprobó las Cláusulas Contractuales Modelo para la Transferencia Internacional de Datos Personales elaboradas por la Red Iberoamericana de Protección de Datos[252]. En la resolución se destaca, entre otras, lo siguiente:

250 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.

251 Cfr. Perú aprueba "*Guía de Implementación para la Transferencia Internacional de Datos Personales*" en línea con estándares internacionales. Publicado el 25 de octubre de 2023. En: https://www.gob.pe/institucion/minjus/noticias/663844-peru-aprueba-guia-de-implementacion-para-la-transferencia-internacional-de-datos-personales-en-linea-con-estandares-internacionales

252 El texto de la resolución y la guía pueden consultarse en: https://www.gob.pe/institucion/minjus/normas-legales/3617286-0074-2022-jus-dgtaipd

- "La regulación peruana dice que el emisor o exportador podrá valerse de cláusulas contractuales u otros instrumentos jurídicos en los que se establezcan, cuando menos, las mismas obligaciones a las que se encuentra sujeto, así como las condiciones en las que el titular consintió el tratamiento de sus datos personales;
- El 22 de octubre de 2021 se llevó a cabo el XIX Encuentro de la Red Iberoamericana de Protección de Datos, en cuya declaración final, se exhortó a los Estados Iberoamericanos, así como a los empresarios, a tomar en consideración las Cláusulas Contractuales Modelo desarrolladas por la RIPD a las transferencias internacionales, principalmente a las transferencias a jurisdicciones no adecuadas. Ello, por ser dichas cláusulas un medio que permite el cumplimiento de los principios de protección de datos personales y, a su vez, una alternativa económicamente viable para los empresarios que no tendrán que negociar acuerdos individuales, sino adherirse a un conjunto de cláusulas previamente aprobadas por la Autoridad;
- La finalidad de las Cláusulas Contractuales Modelo es garantizar y facilitar el cumplimiento de los requisitos previstos en la ley de protección de datos del país exportador de datos personales para la transferencia de dichos datos a un tercer país que no haya sido reconocido con un nivel adecuado de protección, de modo tal que la protección, inicialmente otorgada a los datos personales, continúe con independencia del lugar donde estos datos se encuentren;
- El uso de Cláusulas Contractuales Modelo puede ayudar a superar las limitaciones en las transferencias de datos que se deriven de las diferencias en el nivel de protección entre los diferentes países, en consideración a que dichas cláusulas contribuyen a construir una convergencia a nivel contractual, sin necesariamente requerir convergencia a nivel de país;
- El empleo de Cláusulas Contractuales Modelo permite que las empresas no tengan que negociar y pactar acuerdos en cada caso individual, con el coste económico que ello

implica (por representación legal y tiempo), pues la existencia de estas cláusulas permite confiar en el modelo de la Autoridad Nacional, el cual ha sido debidamente aprobado en el entorno de la RIPD, sabiendo que, al implementarlas y cumplirlas, las empresas y entidades observan sus obligaciones legales en materia de transferencia internacional de datos personales con una solución sencilla y práctica"[253].

- Las Cláusulas Contractuales Modelo para la Transferencia Internacional de Datos Personales constituyen un instrumento particularmente relevante para superar las limitaciones en las transferencias internacionales de datos, el cual contribuirá a que estas se realicen bajo condiciones que resguarden el derecho de los titulares de los datos, en cumplimiento de las medidas de seguridad, confidencialidad, en armonía con la Ley N.º 29733, Ley de Protección de Datos Personales, el Reglamento y los mejores estándares internacionales.
- Asimismo, permitirán un mayor dinamismo en la transferencia internacional de los datos, favoreciendo el flujo económico, el comercio exterior y comercio electrónico.

REPÚBLICA ORIENTAL DEL URUGUAY

El 29 de diciembre de 2022, mediante la Resolución N° 50/022, el Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales de la República Oriental del Uruguay resolvió lo siguiente:

"1. Indicar a responsables y encargados de tratamiento que en el marco de transferencias internacionales de datos realizadas al amparo del artículo 23 de la Ley N° 18.331, podrán emplear las cláusulas contractuales incluidas en la "*Guía de Implementación de Cláusulas Contractuales Modelo para la Transferencia Internacional de Datos Persona-*

253 República del Perú. Resolución Directoral N.º 074-2022-JUS/DGTAIPD. Lima, 17 de octubre de 2022. El texto de la resolución puede consultarse en: https://cdn.www.gob.pe/uploads/document/file/3787915/RD%20074%20Clausulas%20contractuales%20modelo.pdf.pdf?v=1666656624

les (TIPD)" que se anexan a la presente Resolución cono Anexo I, con las adaptaciones que estimen corresponden para su adaptación a la normativa nacional, salvo en aquellos casos en que las cláusulas brinden mayores garantías a los titulares de los datos.

2. Indicar a responsables y encargados de tratamiento que el uso de las cláusulas referidas en el resuelve anterior no excluye la autorización previa de esta Unidad a la o las transferencias que se pretendan realizar, de conformidad con lo previsto en el inciso final del artículo 23 de la Ley N° 18.331"[254].

Dentro de los considerandos, la autoridad uruguaya señala, entre otras, lo que sigue a continuación:

La Red Iberoamericana de Protección de Datos (RIPD) aprobó en los "Estándares de Protección de Datos para los Estados Iberoamericanos", los que tienen por objeto, entre otros, "Facilitar el flujo de los datos personales entre los Estados Iberoamericanos y más allá de sus fronteras, con la finalidad de coadyuvar al crecimiento social y económico de la región" (artículo 1.1.d)". En la elaboración de la guía y de las cláusulas contractuales se tuvo en cuenta dichos estándares.

Mediante la Resolución 41/021, del 8 de setiembre de 2021, la citada autoridad recomendó a responsables y encargados de tratamiento que deseen realizar transferencias internacionales de datos adoptar las cláusulas contractuales con un contenido mínimo indicado en el Anexo I de la citada resolución.

254 Cfr. República Oriental del Uruguay. Resolución N° 50/022 del 29 de diciembre de 2022 de El Consejo Ejecutivo de la Unidad de la Unidad Reguladora y de Control de Datos Personales. El texto oficial puede consultarse en: https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-n-50022

REPÚBLICA ARGENTINA

La autoridad de protección de datos de la República Argentina - Agencia de Acceso a la Información Pública[255]- resolvió lo siguiente en el artículo 1 de la Resolución 198/2023 del 13 de octubre de 2023: "Aprobar las cláusulas contractuales modelo para transferencias internacionales incluidas en la "*Guía de Implementación de Cláusulas Contractuales Modelo para la Transferencia Internacional de Datos Personales (TIDP)*".

Dentro del considerando para adoptar dicha decisión destacamos los siguientes:

- "La regulación argentina admite como garantías adecuadas a los fines de la transferencia internacional de datos personales la existencia de autorregulación o cláusulas contractuales que brinden garantías de protección equiparables a la de nuestra normativa.
- Mediante la Disposición de la DNPDP N° 60/2016, modificada por la Resolución de la AAIP N° 34/2019, se aprobaron las cláusulas contractuales tipo de transferencia internacional para la cesión y prestación de servicios, incorporadas en los Anexos I y II de dicha medida, respectivamente, a fin de garantizar un nivel adecuado de protección de datos personales en los términos del artículo 12 de la Ley N° 25.326 y del Anexo I al Decreto N° 1558/01 en aquellas transferencias de datos que tengan por destino países sin legislación adecuada.
- La irrupción de una nueva generación de legislaciones en materia de protección de datos, el crecimiento significativo de los flujos transfronterizos y su incidencia en la economía global, a nivel regional e internacional se ha avanzado en la actualización de cláusulas contractuales modelo para la transferencia internacional, con el propósito de

255 De conformidad con el artículo 19 de la Ley Nº 27.275, la AGENCIA DE ACCESO A LA INFORMACIÓN PÚBLICA (AAIP), ente autárquico con autonomía funcional en el ámbito de la JEFATURA DE GABINETE DE MINISTROS, es Autoridad de Aplicación de la Ley de Protección de Datos Personales N° 25.326, entre otras responsabilidades.

conducir hacia la convergencia de herramientas, simplificar los procedimientos y establecer pisos de garantías comunes que potencien la confianza entre los diferentes países".

- Enuncia la existencia de "las cláusulas contractuales modelo para la transferencia internacional de datos personales de la Red Iberoamericana de Protección de Datos, aprobadas por unanimidad en diciembre de 2021; las Cláusulas estándares Contractuales de la Comisión de la Unión Europea, de junio de 2021; las Cláusulas contractuales modelo de la ASEAN para flujos de datos transfronterizos, de enero de 2021; el Contrato Estándar de exportación de Información Personal de la Administración de Ciberespacio de China, promulgado en febrero de 2023 y el primer módulo de las Cláusulas Contractuales modelo para flujos de datos transfronterizos del Consejo de Europa, aprobadas en junio de 2023".
- Las cláusulas de la RIPD "posibilitan el cumplimiento de los principios de protección de datos personales, y brindan a las empresas u organismos una alternativa económicamente viable, evitando que deban negociar acuerdos individuales al permitirles utilizar un conjunto de cláusulas previamente aprobadas por la Autoridad de Aplicación".
- Adicionalmente, las mismas "tienen el potencial de contribuir a la convergencia normativa para una protección de datos adecuada, siguiendo estándares aceptados a nivel mundial". Por ende, es "oportuno y conveniente incorporar las cláusulas contractuales modelo para la transferencia internacional de datos personales de la Red Iberoamericana de Protección de Datos al marco normativo aplicable en nuestro país en materia de protección de datos personales"[256].

Sobre esto último (responsabilidad demostrada), el parágrafo 2 exige a los destinadatarios de la Decisión que adopten "medidas útiles, eficientes, necesarias y pertinentes para

256 República Argentina. Resolución 198/2023 del 13 de octubre de 2023 de la Agencia de Acceso a la Información Pública. El texto oficial está disponible en: https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-198-2023-391538/texto

acreditar el cumplimiento de lo dispuesto en esta Decisión respecto del Tratamiento de Datos Personales"[257].

¿DEL NIVEL ADECUADO DE PROTECCIÓN DE DATOS PERSONALES HACIA LAS CLÁUSULAS CONTRACTUALES PARA TRANSFERENCIAS DE DATOS?

La expresión "nivel adecuado de protección" (NAPD) surgió en Europa al establecer reglas para transferir datos personales desde allá a terceros países. Ser catalogado por Europa como país con dicho grado de protección no es sencillo ni expedito. Normalmente exige que los países expidan regulaciones apropiadas y efectúen cambios institucionales. De hecho, puede afirmarse que el artículo 25 de la Directiva fue el detonador de la necesidad de que en muchos países se regulara el tratamiento de datos personales y se adoptara el enfoque europeo para poder ser receptores de los datos provenientes de Europa.

La razón de la importación del modelo europeo en muchos países es muy sencilla: para Europa el "nivel adecuado de protección" es el que se deriva de regulaciones como, en su momento, la Directiva 95/46/CE o el actual GPR. Por ende, quien quiera ser catalogado como país con "nivel adecuado" debe seguir los principales lineamientos del modelo europeo de protección de datos. Este fenómeno lo titula y explica Palazzi bajo el título *Expansión del modelo europeo a países no europeos* citando a autores como Colin Bennett y Joel Reidenberg que respectivamente se han referido al "impacto externo de la Directiva europea sobre protección de datos" y a la "globalización de soluciones a la privacidad"[258].

257 Cfr. Artículo 4 de la Decisión Andina 897 de 2022 de la CAN.

258 Cfr. PALAZZI, Pablo. 2002. *La transmisión internacional de datos personales y la protección de la privacidad: Argentina, América Latina, Estados Unidos y la Unión Europea*. 1 ed. Buenos Aires, Argentina: Ad-Hoc. P. 39-41.

En adición a tener un marco jurídico sobre el tema, es necesario que el país interesado inicie un trámite ante la Comisión Europea (CEU)[259] para que formalmente se catalogue como un país con "nivel adecuado". Dicho proceso, según algunas experiencias, se demora un poco más de dos (2) años. De hecho, las autoridades europeas reconocen "la escasa probabilidad que la Comisión adopte resoluciones de adecuación (...) para numerosos países a corto o incluso mediano plazo"[260].

El entonces Grupo de protección de las personas en lo que respecta al tratamiento de datos personales (también conocido como el Grupo del artículo 29 de la Directiva 95/46) —hoy Comité Europeo de Protección de Datos[261] (CEPD)— adoptó en 1997[262] y 1998[263] dos documentos que fijaron las posibles formas de evaluar el nivel de protección de terceros países. En ellos se dejó sentado que un nivel de protección adecuado depende de varios factores de naturaleza regulatoria y de carácter "instrumental e institucional" (requisitos de procedimiento y de aplicación). El primero, grosso modo, es fruto de una mezcla de derechos en cabeza del titular de los datos y de obligaciones para quienes procesan la información personal o que ejercen control sobre dicho tratamiento.

259 De conformidad con la página web oficial de la Comisión Europea, la misma "órgano ejecutivo de la UE y representa los intereses del conjunto de Europa". Sus principales funciones son: "fijar objetivos y prioridades de actuación; proponer legislación al Parlamento y el Consejo; gestionar y aplicar las políticas de la UE y su presupuesto; velar por que se aplique el Derecho europeo (conjuntamente con el Tribunal de Justicia) y representar a la UE fuera de Europa (negociando acuerdos comerciales entre la UE y otros países, etc.)." Véase: https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-commission_es

260 Cfr. Parte final del numeral 4 de los considerandos de la Decisión 2001/497/CE.

261 El CEPD está compuesto por representantes de las autoridades nacionales de protección de datos de los países de la UE/EEE y del Supervisor Europeo de Protección de Datos. Sus principales funciones son : "proporcionar orientaciones sobre los conceptos clave del RGPD y de la Directiva sobre protección de datos en el ámbito penal, asesorar a la Comisión Europea sobre cuestiones relacionadas con la protección de los datos personales y la nueva legislación que se proponga en la Unión Europea y adoptar resoluciones vinculantes en caso de conflicto entre las autoridades nacionales de control" https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_es?prefLang=es#comit%C3%A9-europeo-de-protecci%C3%B3n-de-datos. Mayor información sobre este comité en: https://edpb.europa.eu/edpb_es

262 Cfr. COMISIÓN EUROPEA, Grupo de protección de las personas en lo que respecta al tratamiento de datos personales. 1997. Primeras orientaciones sobre la transferencia de datos personales a países terceros: posibles formas de evaluar la adecuación. XV D/5020/97 -ES 2 WP4. Bruselas.

263 Cfr. COMISIÓN EUROPEA, Grupo de protección de las personas en lo que respecta al tratamiento de datos personales. 1998. Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE. DG XV D/5025/98 WP 12. Bruselas.

El segundo, comprende, de una parte, la existencia de mecanismos y procedimientos judiciales y no judiciales que garanticen la efectividad de las normas, sancionen su incumplimiento y que otorguen a la persona afectada un derecho de reparación frente al tratamiento indebido de su información. Adicionalmente, se considera necesaria la existencia de una autoridad independiente que no sólo controle, vigile y sancione a los que poseen datos personales, sino que reciba las quejas de los ciudadanos e inicie las investigaciones pertinentes con miras a que se convierta en un garante de la protección de los datos de los mismos.

Allí se precisó que cualquier análisis para establecer el nivel adecuado de protección debe centrarse en dos elementos básicos: El contenido de las normas aplicables y los medios para garantizar la efectiva aplicación de las mismas. Uno y otro elemento son cruciales porque de poco sirven las normas si no se cumplen, por eso coincidimos con que "las normas sobre protección de datos únicamente contribuyen a la protección de los individuos si se aplican en la práctica"[264].

Todo lo anterior fue retomado por el European Data Protection Board (EDPB) en el documento titulado "Adequacy Referential, WP 254 rev. 01"[265]. En esencia, este documento actualiza las directrices iniciales teniendo en cuenta la nueva legislación[266] y la jurisprudencia reciente del Tribunal de Justicia de la Unión Europea (TJUE)[267]. Respecto del concepto y objetivo del nivel adecuado se destaca que "aunque el «nivel de

264 Cfr. COMISIÓN EUROPEA, Grupo de protección de las personas en lo que respecta al tratamiento de datos personales, 1997. Primeras orientaciones sobre la transferencia de datos personales a países terceros: posibles formas de evaluar la adecuación. XV D/5020/97 -ES 2 WP4. Bruselas. P 5 y COMISIÓN EUROPEA, Grupo de protección de las personas en lo que respecta al tratamiento de datos personales, 1998. Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE. DG XV D/5025/98 WP 12. Bruselas, pág. 5.

265 European Data Protection Board, Adequacy Referential, WP 254 rev. 01.available at the following link: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108

266 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (Texto pertinente a efectos del EEE).

267 TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA (2015) Asunto C-362/14, Maximillian Schrems contra Data Protection Commissioner, 6 de octubre de 2015.

protección» en el tercer país debe ser «sustancialmente equivalente» al garantizado en la Unión Europea (UE), «los medios de los que se sirva ese tercer país para garantizar ese nivel de protección pueden ser diferentes de los aplicados en la [UE]». Por tanto, el objetivo no es reflejar punto por punto la legislación europea, sino establecer los requisitos esenciales y básicos de dicha legislación"[268].

No todos los países tienen una protección uniforme. Partiendo de esta realidad, para fijar el contenido mínimo que debería tener las normas de terceros países, el Grupo del artículo 29 extractó una serie de principios comunes contenidos en la Directiva 95/46/CE, el Convenio 108 de 1981, las directrices de la OCDE de 1980 y los principios de la ONU de 1990. A partir de lo anterior concluyó que el contenido de las normas debería contar con un núcleo de elementos mínimos, que se traducen en los siguientes principios básicos y adicionales:

Principios básicos	Principios adicionales que debería aplicarse a tipos específicos de tratamiento
Limitación de la finalidad	Datos sensibles
Calidad de los datos y proporcionalidad	Marketing directo
Transparencia	Decisión individual automatizada
Seguridad	
Acceso, rectificación y oposición	
Restricciones a las transferencias sucesivas a otros terceros países	

Tabla 2. Principios mínimos que deben contener las regulaciones sobre protección de datos personales según el estándar europeo. Elaboración del autor.

268 European Data Protection Board, Adequacy Referential, WP 254 rev. 01, pág 3. Available at the following link: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108

La anterior es una lista que, dependiendo de los riesgos que genera la transferencia internacional, podrá ser ampliada o reducida. Pero mientras no exista alguna particularidad o caso especial, se toma como el listado básico de referencia para establecer si las normas de un tercer país brindan un nivel adecuado de protección. Teniendo en cuenta lo anterior y a partir de un pequeño análisis comparativo[269] de los dictámenes y las decisiones de la Comisión Europea sobre "nivel adecuado" que ha emitido desde 1999, en los casos de Suiza[270], Hungría[271], Argentina[272], Guersey[273], Isla de Man[274], Jersey[275], Islas Feroe[276] y Uruguay[277] se puede establecer lo siguiente:

El 100% de los "terceros países" analizados tienen una norma general sobre protección de datos personales que incorporan los principios básicos citados. Adicionalmente, cuentan con disposiciones sectoriales para el tratamiento de algunos datos personales en particular. El 75% de los países ha adquirido compromisos internacionales en materia de protec-

269 A 2024 varios países han obtenido el nivel adecuado. Para efectos de nuestro análisis sólo consideramos ocho. Los detalles sobre los cuatro países no analizados pueden consultarse en la decisión respectiva que emitió en cada caso la Comisión Europea: Canadá. Decisión 2002/2/CE de la Comisión, de 20 de diciembre de 2001, respecto de las entidades sujetas al ámbito de aplicación de la ley canadiense de protección de datos; Israel. Decisión 2011/61/UE de la Comisión, de 31 de enero de 2011; Andorra. Decisión 2010/625/UE de la Comisión, de 19 de octubre de 2010 y Nueva Zelanda. Decisión 2013/65/UE de la Comisión, de 19 de diciembre de 2012.

270 Cfr. COMISIÓN EUROPEA. 2000. Decisión de la Comisión de 26 de julio de 2000 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa al nivel de protección adecuado de los datos personales en Suiza (Decisión 2000/18/CE).

271 COMISIÓN EUROPEA, Grupo de protección de las personas en lo que respecta al tratamiento de datos personales. 1999. Dictamen 6/99 sobre el nivel de protección de los datos personales en Hungría. 5070/FR/99/final WP24.

272 Cfr. COMISIÓN EUROPEA. 2003. Decisión de la Comisión de 30 de junio de 2003 con arreglo a la Directiva 95/46/CE del Parlamento y del Consejo sobre la adecuación de la protección de los datos personales en Argentina.

273 Cfr. COMISIÓN EUROPEA. 2003. Decisión de la Comisión de 21 de noviembre de 2003, relativa al carácter adecuado de la protección de datos personales en Guernsey (Decisión 2003/821/CE).

274 Cfr. COMISIÓN EUROPEA. 2004. Decisión de la Comisión de 28 de abril de 2004, relativa al carácter adecuado de la protección de datos personales en la Isla de Man (Decisión 2004/411/CE).

275 COMISIÓN EUROPEA. 2008. Decisión de la Comisión de 8 de mayo de 2008 de conformidad con la Directiva 95/46/CE del Parlamento y del Consejo, relativa a la protección adecuada de los datos personales en Jersey (Decisión 2008/393/CE).

276 COMISIÓN EUROPEA. 2010. Decisión de la Comisión de 5 de marzo de 2010 de conformidad con la Directiva 95/46/CE del Parlamento y del Consejo, relativa a la protección adecuada de los datos personales en Isla Feroe (Decisión 2010/146/UE).

277 Cfr. COMISION EUROPEA. 2012. Decisión de la Comisión de 21 de agosto de 2012 de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada de los datos personales por la República Oriental del Uruguay en lo que respecta al tratamiento automatizado de datos personales (Decisión 2012/484/UE).

ción de datos, particularmente suscribiendo el Convenio 108 de 1981. El 42.85% por su parte, cuenta con norma constitucional que se refiere al tema en estudio.

Es importante señalar que "nivel adecuado de protección de datos personales" no equivale establecer si un país tiene idéntico sistema de protección que otro. En este sentido, el Tribunal de Justicia, mediante sentencia del 6 de octubre de 2015 en el caso C362/14, de Maximillian Schrems contra el Comisario de Protección de Datos[278] (Schrems), precisó que no requiere que el país a evaluar o certificar tenga un nivel idéntico de protección y que lo importante es demostrar que los medios a los que recurre el tercer país en cuestión para proteger los datos personales sean eficaces para garantizar un nivel adecuado de protección[279].

En línea con lo anterior, en la decisión de nivel adecuado de Estados Unidos del 10 de julio de 2023 la Comisión Europea señaló que: "el estándar de adecuación no exige una réplica punto por punto de las normas de la Unión. Más bien, determinar si, a través de la regulación sobre privacidad y su implementación, supervisión y aplicación efectiva, el sistema extranjero en su conjunto proporciona el nivel requerido de protección"[280].

278 Tribunal de Justicia. Caso C-362/14, Maximilian Schrems v. Data Protection Commissioner (Schrems), ECLI:EU:C:2015:650, parágrafo 73.
279 Tribunal de Justicia. Caso C-362/14, Maximilian Schrems v. Data Protection Commissioner (Schrems), ECLI:EU:C:2015:650, parágrafo 74.
280 COMMISSION IMPLEMENTING DECISION of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework. En: https://eur-lex.europa.eu/eli/dec_impl/2023/1795/oj

DE LA DIFICULTAD PARA OBTENER "NIVEL ADECUADO": ¿EL USO DE LAS CLÁUSULAS CONTRACTUALES DESAPARECERÁ LA NECESIDAD DE LA FIGURA DEL "NIVEL ADECUADO"?

No es fácil que un país obtenga el "nivel adecuado". Aunque no se puede generalizar sobre el proceso de nivel adecuado porque todo depende de las particularidades de cada país. A título de ejemplo, destaco la experiencia de la República de Colombia.

Previo a ello, es necesario tener presente que garantizar un nivel adecuado de protección no exige que se garantice un nivel de protección idéntico al de la Unión Europea, ni que se reproduzcan al pie de la letra las normas de la Unión: Lo anterior ha sido afirmado por el Tribunal de Justicia de la Unión Europea, la Comisión Europea y el European Data Protection Board (EDPB).

Tal como se especifica en el artículo 45, apartado 2, del Reglamento (UE) 2016/679[281], la adopción de una decisión de adecuación ha de basarse en un análisis del ordenamiento jurídico del tercer país. La evaluación debe determinar si el tercer país en cuestión garantiza un nivel de protección adecuado o equivalente en lo esencial al ofrecido en la Unión Europea[282]. Es relevante destacar que, según el Tribunal de Justicia de la Unión Europea, no se exige un nivel de protección idéntico[283]. Para dicho tribunal, "es verdad que el término «adecuado» (...) significa que no cabe exigir que un tercer país garantice un nivel de protección idéntico al garantizado en el ordenamiento jurídico de la Unión"[284].

281 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (Texto pertinente a efectos del EEE).

282 Cfr. Considerando 104 del Reglamento (UE) 2016/679.

283 Cfr. Tribunal de Justicia (Gran Sala) . Sentencia del 6 de octubre de 2015. Asunto C-362/14, Maximillian Schrem/Data Protection Commissioner (en lo sucesivo, «Schrems»), ECLI:EU:C:2015:650, apartado 73. El texto puede consultarse en: https://curia.europa.eu/juris/document/document.jsf?docid=169195&doclang=ES

284 Cfr. Schrems, apartado 73.

Sobre este punto, en el caso Schrems dicho tribunal precisó que los medios existentes en otro país "deben ser eficaces en la práctica para garantizar una protección sustancialmente equivalente a la garantizada en la Unión"[285].

En otras palabras, los mecanismos jurídicos de otros países (como Colombia) pueden ser diferentes de los aplicados en la Unión Europea, siempre que, en la práctica, sean eficaces para garantizar un nivel de protección adecuado[286]. Según la Comisión Europea, "el nivel de adecuación no exige que se reproduzcan al pie de la letra las normas de la Unión. Se trata más bien de determinar si el sistema extranjero ofrece, en su conjunto y por la esencia de los derechos de privacidad y su aplicación, fuerza ejecutiva y supervisión efectivas, el nivel de protección exigido"[287].

Todo lo anterior fue reiterado por el European Data Protection Board (EDPB) en el documento titulado "Adequacy Referential, WP 254 rev. 01"[288]. En esencia, este documento actualiza las directrices iniciales teniendo en cuenta la nueva legislación[289] y la jurisprudencia reciente del Tribunal de Justicia de la Unión Europea (TJUE)[290]. Respecto del concepto y objetivo del nivel adecuado se destaca que: "aunque el «nivel de protección» en el tercer país debe ser «sustancialmente equivalente» al garantizado en la Unión Europea (UE), «los medios de los que se sirva ese tercer país para garantizar ese nivel de protección pueden ser diferentes de los aplicados en la [UE]». Por tanto, el objetivo no

285 Cfr. Schrems, apartado 74.
286 Cfr. Schrems, apartado 74.
287 Cfr. Comisión Europea. DECISIÓN DE EJECUCIÓN (UE) 2019/419 DE LA COMISIÓN de 23 de enero de 2019 con arreglo al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativa a la adecuación de la protección de los datos personales por parte de Japón en virtud de la Ley sobre la protección de la información personal [notificada con el número C(2019) 304] (Texto pertinente a efectos del EEE). Considerando 3. El texto oficial puede consultarse en: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52023DC0275
288 European Data Protection Board, Adequacy Referential, WP 254 rev. 01. Available at the following link: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108
289 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (Texto pertinente a efectos del EEE).
290 TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA (2015) Asunto C-362/14, Maximillian Schrems contra Data Protection Commissioner, 6 de octubre de 2015.

es reflejar punto por punto la legislación europea, sino establecer los requisitos esenciales y básicos de dicha legislación"[291].

El European Data Protection Board (EDPB) enfatiza que "se puede lograr la adecuación a través de una combinación de derechos para los interesados y obligaciones para aquellos que realizan el tratamiento de los datos, o que ejercen control sobre dicho tratamiento, y la supervisión por parte de organismos independientes. No obstante, las normas de protección de datos solo resultan efectivas si son exigibles y se siguen en la práctica. Por tanto, se debe tener en cuenta no solo el contenido de las normas aplicables a los datos personales transferidos a un tercer país u organización internacional, sino también el sistema existente para garantizar la efectividad de dichas normas. Unos mecanismos de aplicación eficientes son de vital importancia para la efectividad de las normas de protección de datos"[292].

Tanto el contenido de las normas aplicables como los medios para garantizar la efectiva aplicación de las mismas son cruciales porque de poco sirven las normas si no se cumplen. En este sentido, coincidimos con que "las normas sobre protección de datos únicamente contribuyen a la protección de los individuos si se aplican en la práctica"[293].

Para efectos de la circulación transfronteriza de datos, la Superintendencia de Industria y Comercio (SIC) de la República de Colombia, desde el mes de agosto de 2017, ha establecido que los siguientes países tienen nivel adecuado de protección de datos[294]: Alemania; Australia, Austria; Bélgica; Bulgaria; Chi-

291 European Data Protection Board, Adequacy Referential, WP 254 rev. 01. Pág 3. Available at the following link: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108

292 European Data Protection Board, Adequacy Referential, WP 254 rev. 01. Pág 3. Available at the following link: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108

293 Cfr. COMISIÓN EUROPEA, Grupo de protección de las personas en lo que respecta al tratamiento de datos personales. 1997. Primeras orientaciones sobre la transferencia de datos personales a países terceros: posibles formas de evaluar la adecuación. XV D/5020/97 -ES 2 WP4. Bruselas. Pág 5 y COMISIÓN EUROPEA, Grupo de protección de las personas en lo que respecta al tratamiento de datos personales. 1998. Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE. DG XV D/5025/98 WP 12. Bruselas. Pág 5.

294 Cfr. SIC Circulares externas 5 y 8 de 2017 y 2 de 2018.

pre; 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.

No obstante lo anterior la SIC en su rol de autoridad de protección de datos personales, ha iniciado varios procesos para obtener nivel adecuado de protección de datos. Por ahora, Colombia ha sido reconocido por el Centro Financiero Internacional de Dubái como un país que ofrece un nivel adecuado de protección de datos personales[295].

Esta fue la conclusión del 6 de octubre de 2022 del Dubai International Financial Centre Authority (DIFC) 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"[296].

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.

---

295 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. En: https://sic.gov.co/slider/colombia-es-reconocida-por-su-nivel-adecuado-de-proteccion-de-datos-por-el-centro-financiero-de-dubai#:~:text=Bogot%C3%A1%20D.C.%2C%2018%20octubre%20de%202022.&text=Esto

296 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 official puede consultarse en: https://cpdp.lat/wp-content/uploads/2023/07/doc-discusion-cpdplatam23-2.3.pdf

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. Han transcurrido más de cuatro años y tres meses a 25/IV/2024
Reino Unido de Gran Bretaña e Irlanda del Norte	Abril de 2021	Pendiente. Han transcurrido más de tres años a 25/IV/2024
Argentina	31 de agosto de 2021 (Oficio 21-348053 del Superintendente Delegado para la protección de Datos de la SIC)	Pendiente. Han transcurrido más de dos años y tres meses a 25/IV/2024
Uruguay	31 de agosto de 2021 (Oficio 21-348062 del Superintendente Delegado para la protección de Datos de la SIC)	Pendiente. Han transcurrido más de dos años y tres meses a 25/IV/2024

Tabla 3. Listado de solicitudes realizadas por Colombia para obtener nivel adecuado de protección de datos personales.

Como se observa, los tiempos que toman los procesos de nivel adecuado y los niveles de incertidumbre que generan los mismos no son convenientes para quienes necesitan exportar lícitamente datos personales a otros países. Por eso, las CCM son una herramienta expedita y sensata para lograr dicho cometido. Muy seguramente, el uso de las cláusulas desplazará la necesidad de acudir a la figura de "nivel adecuado de protección de datos personales".

¿ES ÚTIL SEGUIR INSISTIENDO EN LA FIGURA DEL "NIVEL ADECUADO" DE PROTECCIÓN DE DATOS?

Planteamos algunas pequeñas reflexiones iniciales para repensar sobre la necesidad de mantener la figura de "nivel adecuado" de protección de datos dentro del contexto o escenario de

la circulación transfronteriza de esa clase de información. Al mismo tiempo, destacamos algunas bondades de las Cláusulas Contractuales Modelo (CCM) para exportar expeditamente información a otros países.

- Es importante que todos los países garanticen un nivel adecuado de protección de datos. Pero ello no significa que dicho nivel únicamente se adquiera cumpliendo los procesos establecidos por organizaciones extranjeras o autoridades locales de otros países. En la práctica, pueden existir países que tienen niveles adecuados de protección de datos y que no hacen parte de los países certificados por las autoridades u organizaciones extranjeras. En otras palabras, carecer de una certificación formal de nivel adecuado, no significa que el país no tenga nivel adecuado y efectivo para garantizar el debido tratamiento de los datos personales.
- Los procesos de certificación de nivel adecuado implican evaluar y calificar a un país por parte de organismos internacionales o autoridades de otros países. Esto significa que esos procesos estén impregnados de política pública o de geopolítica lo cual hace que la decisión de adecuación no sea 100% objetiva. Estos procesos pueden estar influidos por intereses nacionales o regionales y de objetivos de política exterior que impactan en las dinámicas geopolíticas que usualmente están acompañadas de la interacción de factores geográficos, económicos, políticos y alianzas estratégicas, fruto de la diplomacia y de las negociaciones para incidir en el escenario global e internacional.
- Las relaciones geopolíticas y geoeconómicas entre Estados están construidas sobre bases de desigualdad en la medida que son protagonizadas por países poderosos y otros que no lo son. La economía y la seguridad de unos países depende de otras naciones que se convierten en sus principales "socias" comerciales o "aliadas estratégicas". Si un país poderoso es el principal socio económico, el más débil puede estar sujeto a presiones económicas

o estratégicas significativas. La voluntad del país débil no es libre, sino que es un acto de conveniencia o de sumisión. Las amenazas de sanciones comerciales o la manipulación de acuerdos comerciales pueden incidir en la independencia económica y la capacidad de toma de decisiones.

- Esto hace que no exista plena objetividad o libertad para tomar decisiones de adecuación por parte de los países "no poderosos" o que tienen "dependencia" de otros Estados o necesidad de mantener "alianzas estratégicas". En esa medida, la figura del "nivel adecuado" genera "presión política y económica". Por eso, en el marco de un proceso de adecuación, es muy complejo que un país débil le niegue la decisión de adecuación a los países poderosos con los cuales tiene relaciones comerciales o dependencia económica. En este caso, el 100% de la decisión no obedeció a generar las condiciones sensatas para garantizar un nivel adecuado de protección de los datos de las personas.
- Los procesos de certificación de nivel adecuado dependen, entre otros, de factores políticos y de la gestión de los gobiernos. Algunos Estados no han recurrido a esta figura por, entre otros, desconocimiento de esta, falta de interés político (o de prioridad en la agenda política) e ignorancia sobre su relevancia jurídica, política, económica y social. También es difícil demostrar y medir objetivamente, con cifras, cuáles son los beneficios concretos que han obtenido los países certificados con nivel adecuado de protección de datos.
- Algunos Estados o autoridades, frente a las cuales se realizan solicitudes de nivel adecuado, tampoco saben cómo gestionarlas adecuadamente. Frente a solicitudes de certificación, muchas veces reina el "silencio" y dejar pasar el tiempo sin responder. A veces, a algunos Estados les toca insistir, rogar o hacer lobbying para agendar una reunión de trabajo o para impedir que el proceso se congele o se paralice.

- Es importante que todos los países garanticen un nivel adecuado de protección de datos, pero ello no significa que dicho nivel únicamente se adquiera cumpliendo los procesos establecidos por organizaciones extranjeras o autoridades locales de otros países. En la práctica, pueden existir países con niveles adecuados de protección de datos y que no hacen parte de las naciones certificadas por las autoridades u organizaciones extranjeras. En otras palabras, carecer de una certificación formal de nivel adecuado, no significa que el país no tenga nivel adecuado y efectivo para garantizar el debido tratamiento de los datos personales.
- Los procesos de certificación de nivel adecuado implican evaluar y calificar a un país por parte de organismos internacionales o autoridades de otros países. Esto significa que esos procesos estén impregnados de política pública o de geopolítica lo cual hace que la decisión de adecuación no sea 100% objetiva. Estos procesos pueden estar influidos de intereses nacionales o regionales y de objetivos de política exterior que impactan en las dinámicas geopolíticas que usualmente están acompañadas de la interacción de factores geográficos, económicos, políticos y alianzas estratégicas, fruto de la diplomacia y de las negociaciones para incidir en el escenario global e internacional.
- Los ajustes regulatorios e institucionales que implican obtener el "nivel adecuado" toman mucho tiempo y no se puede garantizar que se realicen. Piénsese, por ejemplo, en expedir una nueva regulación de tratamiento de datos o crear autoridades independientes de protección de los derechos de las personas frente al tratamiento de sus datos personales. Eso no depende únicamente de la voluntad de un gobierno sino de la decisión del congreso o el parlamento.
- Lograr un nivel adecuado de protección de datos es un proceso complejo y muy demorado que no se compadece con las necesidades urgentes de circular transfronterizamente datos personales. En el caso de Europa se constata que,

en aproximadamente 28 años[297], la Comisión Europea hasta ahora ha reconocido a 13 países con "nivel adecuado de protección de datos: Andorra, Argentina, Islas Feroe, Guernsey, Israel, Isla de Man, Japón, Jersey, Nueva Zelanda, la República de Corea, Suiza, el Reino Unido bajo el RGPD y la Directiva de Examinadores Legales (LED) y Uruguay[298]. Este reconocimiento también se ha dado a organizaciones comerciales de Canadá[299] y de Estados Unidos. En este último caso cobija únicamente a aquellas que participantes en el Marco de Privacidad de Datos UE-EE. UU.[300].

- Respecto de las 11 adecuaciones conferidas bajo las reglas de la Directiva 95/46, la Comisión Europea, en enero de 2024[301], ratificó que los siguientes países mantienen un nivel adecuado de protección de datos: Andorra, Argentina, Canadá, Islas Faroe, Guernsey, Isle of Man, Israel, Jersey, Nueva Zelanda, Suiza y Uruguay.
- El trámite de adecuación ante la Comisión Europea no es expedito. De hecho, dicha Comisión reconoció en el año

297 Es decir, desde el 24 de octubre de 1995 (fecha en que se expidió la Directiva 95/46) a enero de 2024. Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Diario Oficial n° L 281 de 23/11/1995 P. 0031 - 0050.

298 Cfr. https://www.aepd.es/preguntas-frecuentes/6-transferencias-internacionales-bcr-codigos-de-conducta/1-transferencias-internacionales/FAQ-0605-que-paises-se-consideran-con-un-nivel-adecuado-a-efectos-del-articulo-45-del-rgpd (Última consulta: enero 10 de 2024).

299 En el caso de Canadá, la Comisión decidió lo siguiente: "A los efectos del apartado 2 del artículo 25 de la Directiva 95/46/CE, Canadá garantiza un nivel adecuado de protección de los datos personales transferidos desde la Comunidad a los receptores sujetos a la Personal Information Protection and Electronic Documents Act (en adelante «la Ley canadiense»). (Artículo 1 de la Decisión de la Comisión de 20 de diciembre de 2001 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección de los datos personales conferida por la ley canadiense Personal Information and Electronic Documents Act).

300 En la referente a Estados Unidos, la decisión decidió lo siguiente: "Article 1 For the purpose of Article 45 of Regulation (EU) 2016/679, the United States ensures an adequate level of protection for personal data transferred from the Union to organisations in the United States that are included in the 'Data Privacy Framework List', maintained and made publicly available by the U.S. Department of Commerce, in accordance with Section I.3 of Annex I." (COMMISSION IMPLEMENTING DECISION of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework . En: https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf)

301 COMISIÓN EUROPEA (2024) Report from the commission to the European parliament and the council on the first review of the functioning of the adequacy decisions adopted pursuant to Article 25(6) of Directive 95/46/EC. Bruselas 15 de enero de 2024. En: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en. También leer la siguientes nota de prensa del 14 de enero de 2024: PRESS RELEASE15 January 2024Brussels. Commission finds that EU personal data flows can continue with 11 third countries and territories. En: https://ec.europa.eu/commission/presscorner/detail/en/ip_24_161

2001 "la escasa probabilidad que la Comisión adopte resoluciones de adecuación (...) para numerosos países a corto o incluso mediano plazo"[302]. Según algunas experiencias[303] se demora un poco más de dos (2) años cuando se toma alguna decisión, pero en otros casos, como el de Colombia, lleva más de cuatro años sin ningún pronunciamiento oficial por parte de la Comisión, aunque se han realizado varias reuniones de trabajo y remitido documentos para dar respuesta a las preguntas de dicha Comisión.

- Las CCM son herramientas cada vez más utilizadas para facilitar las transferencias internacionales de datos. Al ser contratos de contenido homogéneo previamente establecido son más eficientes para acelerar los procesos de exportación de datos personales.
- El uso de las CCM puede ayudar a reducir la incertidumbre al proporcionar un conjunto estandarizado de cláusulas contractuales aprobados por las autoridades locales de protección de datos con miras a asegurar que los mismos incluyen los requerimientos mínimos para garantizar un debido tratamiento de datos personales en los países de destino de las exportaciones de datos.
- Ni el "nivel adecuado", ni las CCM son herramientas perfectas o 100% efectivas. Son mecanismos diseñados para unos objetivos, pero su cumplimiento dependerá de factores externos o de terceros como, entre otros, la voluntad humana para cumplir debidamente lo que ordenan las leyes o los contratos.

302 En efecto, el numeral 4 de la Decisión 2001/497/CE dice lo siguiente: "(4) El apartado 2 del artículo 26 de la Directiva 95/46/CE, que ofrece flexibilidad para una entidad que desee transferir datos a terceros países, y el apartado 4 del mismo artículo, que establece cláusulas contractuales tipo, son esenciales para mantener el necesario flujo de datos personales entre la Comunidad Europea y terceros países sin imponer cargas innecesarias a los operadores económicos. Ambos artículos cobran especial importancia en vista de la escasa probabilidad de que la Comisión adopte resoluciones de adecuación de conformidad con el apartado 6 del artículo 25 para numerosos países a corto o incluso medio plazo."Cfr. Parte final del numeral 4 de los considerandos de la Decisión 2001/497/CE. COMISIÓN EUROPEA 2001/497/CE: Decisión de la Comisión, de 15 de junio de 2001, relativa a cláusulas contractuales tipo para la transferencia de datos personales a un tercer país previstas en la Directiva 95/46/CE . En: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32001D0497

303 En un caso reciente como el de Jersey el proceso ante las autoridades europeas inició con solicitud de febrero de 2006 y culminó con la decisión de adecuación en mayo de 2008.

Ahora bien, no debe perderse de vista la preferencia por utilizar las CCM en lugar de depender de procesos gubernamentales inciertos, complejos y demorados para obtener el "nivel adecuado". Ello obedece, entre otras, a lo siguiente:

- Mayor agilidad y eficiencia del uso de las CCM respecto de los trámites burocráticos que usualmente padecen los ciudadanos frente a las autoridades.
- Las CCM pueden ser más flexibles y adaptables a las necesidades de las organizaciones respecto de las transferencias internacionales de datos personales.

En síntesis, si bien la figura del "nivel adecuado" es una estrategia importante en el escenario de las transferencias internacionales de datos personales, su dinámica, proceso de adopción y trámite no se ajusta a la dinámica y urgencia de respuesta frente a la circulación transfronteriza de datos personales. Debería considerarse a las CCM como un posible reemplazo de la institución del "nivel adecuado de protección de datos". Si bien ambas instituciones pueden coexistir, y la preferencia por uno u otro dependerá de diversos factores, la obtención del nivel adecuado ha demostrado ser engorrosa, demorada e incierta.

En teoría parece ser que el "nivel adecuado" es la mejor opción, pero es necesario medir su efectividad real y evaluar si vale la pena adelantar un trámite complejo, lento e incierto. Las dinámicas actuales de protección de derechos humanos deberían repensarse para lograr herramientas más expeditas, sencillas, prácticas, sensatas y efectivas frente a la realidad sociotecnológica del siglo XXI.

NECESIDAD DE REGULAR LAS CLÁUSULAS ABUSIVAS RESPECTO DEL TRATAMIENTO DE DATOS PERSONALES

Hemos planteado que los contratos han sido el principal instrumento regulador de internet[304], pues en ausencia de regulación estatal, las empresas -mediante notas legales, términos y condiciones- han fijado las reglas de juego de la prestación de sus servicios con millones de personas de todas partes del mundo. Esto no es nuevo, pero es un fenómeno que afecta a prácticamente todas las personas del mundo o a los consumidores porque las relaciones contractuales son masivas, estandarizadas y homogéneas.

Estas regulaciones entre particulares hacen parte de lo que académicamente denominamos el "internet de las empresas (internet of corporations)", el cual "hace referencia a las normas que los empresarios han creado para realizar negocios o prestar servicios en internet. Se trata de las pautas que los empresarios consideran sensatas bajo su modelo de negocios para ganar utilidades" (..) "Como se observa, estamos frente a una realidad de enorme magnitud que involucra la economía digital y la protección efectiva de los derechos humanos de trillones de personas en internet"[305].

Los contratos entre empresas y ciudadanos/consumidores son acuerdos de adhesión en los cuales la parte fuerte (la empresa) impone sus reglas a la parte débil (los consumidores/ personas). En realidad, en este tipo de contratos no existen "acuerdos de voluntades" sino la imposición de la voluntad de una parte frente a la otra. Sobre este aspecto precisa lo siguiente Peña Bennett: "(...) existen modelos de contratación generados por los empresarios con base en los cuales el contenido de

304 Cfr. Remolina, Nelson (2016). *Internet de las empresas (Internet of Corporations -IoC-): Una explicación de lo que pasa en internet y del futuro de la protección de los derechos humanos en el ciberespacio (Parte 1).* En: https://habeasdatacolombia.uniandes.edu.co/?p=2222

305 Cfr. Remolina, Nelson (2016). *Internet de las empresas (Internet of Corporations -IoC-): Una explicación de lo que pasa en internet y del futuro de la protección de los derechos humanos en el ciberespacio (Parte 1).* En: https://habeasdatacolombia.uniandes.edu.co/?p=2222

las cláusulas ya está previamente seleccionado e insertado por ellos. Este tipo de contratos se denomina comúnmente contratos de adhesión o de contenido predispuesto y genera para el consumidor un efecto mediante el cual, únicamente si desea celebrar la relación de consumo, debe manifestar su voluntad, simplemente adhiriendo al contenido del contrato"[306].

El consumidor acepta las reglas preestablecidas por el empresario por muchas razones como, entre otras, las siguientes:

- Por necesidad o por ser un requisito para acceder a un servicio, un beneficio, etc.
- Porque no tiene otra opción ya que si no aceptan los términos y condiciones no accederán al servicio, beneficio, etc.
- Por dependencia, aflicción económica o necesidades apremiantes.
- Por ignorancia, inexperiencia o falta de interés. Por eso, entre otras razones, las personas no leen los términos y condiciones o las cláusulas del contrato de adhesión,
- Porque confían en la buena fe y reputación de la empresa, así como en la ética empresarial o corporativa de algunas organizaciones.
- Porque todos lo hacen y se ha convertido en una "práctica social" aceptar términos y condiciones sin leer o conocer lo que aceptan.

No es sensato afirmar que es un verdadero acuerdo de voluntades aceptar los términos y condiciones preestablecidos por una de las partes porque todos sabemos que no es así. Puede que "formalmente" se hable de un acuerdo de voluntades, pero, en realidad, existe un acto de sumisión de una parte a la voluntad de la otra.

Frente a eventuales abusos del poder de la parte fuerte en el contrato, es conveniente establecer la figura de las cláusulas

306 Peña Bennett, Fernando (2023). *Los empresarios frente al derecho de consumo. Una ilustración a través de un emprendimiento.* Capítulo de libro publicado en la obra Fundamento de derecho de los negocios para no abogados (segunda edición). Universidad de los Andes. Facultad de Derecho. Ediciones Uniandes. ISBN 9789587985641, pág. 478.

abusivas para que en ciertos casos los "acuerdos de voluntades" no tengan ninguna validez o efecto de pleno derecho o de manera automática, de tal forma que no sea necesario acudir a los jueces o las autoridades competentes para que declaren la ineficacia de dicho tipo de cláusulas. En otras palabras, las regulaciones sobre protección (tratamiento) de datos deberían incluir un listado de ejemplos de cláusulas abusivas para que no produzcan efecto de pleno derecho y se evite el eventual abuso contractual con las personas y sus datos.

El poder, *per se*, no es el problema, sino el abuso que se haga del mismo. El abuso del poder o de nuestros derechos es algo que causa daño a los demás. Por eso, La Constitución de la República de Colombia establece en el numeral 1 del artículo 95 que es deber de las personas y de los ciudadanos "1. Respetar los derechos ajenos y no abusar de los propios;". Este pequeño mensaje es de gran calado porque recuerda algo obvio que frecuentemente se olvida: no abusar de nuestros derechos o del poder que tengamos. En este sentido, La Corte Constitucional de la República de Colombia ha señalado que "La Corte no pretende desconocer el derecho al libre desarrollo de la personalidad (...). En modo alguno ignora que las actividades (...) en sí mismas no están prohibidas y, por tanto, no son ellas objeto de esta tutela. **Ambas pueden ejercerse, pero no de manera irrazonable y desproporcionada, sino dentro de unos parámetros mínimos que no afecten el ejercicio de los legítimos derechos de terceros, (...)"**[307].

Precisa la Corte que: "la vida en comunidad conlleva forzosamente el cumplimiento de una serie de deberes recíprocos por parte de los asociados, el primero de los cuales es el de respetar los derechos de los demás. De ello se desprende la consecuencia lógica de que el hombre en sociedad no es titular de derechos absolutos, ni puede ejercer su derecho a la libertad de manera absoluta; los derechos y libertades indivi-

307 Corte Constitucional de la República de Colombia. Sentencia SU-476/97 del 25 de septiembre de 1997. Magistrado Ponente. Dr. Vladimiro Naranjo Mesa. El texto oficial puede consultarse en: https://www.corteconstitucional.gov.co/relatoria/1997/su476-97.htm

duales deben ser ejercidos dentro de los parámetros de respeto al orden jurídico existente y a los valores esenciales para la vida comunitaria como son orden, convivencia pacífica, salubridad pública, moral social, bienes todos estos protegidos en nuestro ordenamiento constitucional"[308].

El respeto de los derechos de los demás y el no abuso de los propios debe reflejarse en el escenario contractual, especialmente en aquellos en donde se involucran derechos humanos. Por eso, las regulaciones han previsto diversas estrategias para poner límites a la autonomía de la voluntad, como entre otros, la consagración de las cláusulas abusivas.

Lo anterior se ha aplicado, por ejemplo, en el derecho del consumidor, el cual es un buen referente para replicarlo en el derecho del debido tratamiento de datos personales porque, entre otros, los millones de consumidores del mundo son titulares de datos personales.

A título de mera referencia aludiremos a la regulación colombiana sobre protección del consumidor, particularmente a la Ley 1480 del 12 de octubre de 2011 "por medio de la cual se expide el Estatuto del Consumidor y se dictan otras disposiciones". Dicha norma consagra el derecho a la "protección contractual" para que el consumidor sea "protegido de las cláusulas abusivas en los contratos de adhesión"[309]. El contrato de adhesión, por su parte, es definido como "aquel en el que las cláusulas son dispuestas por el productor o proveedor, de manera que el consumidor no puede modificarlas, ni puede hacer otra cosa que aceptarlas o rechazarlas"[310]. Esto último

308 Corte Constitucional de la República de Colombia. Sentencia SU-476/97 del 25 de septiembre de 1997. Magistrado Ponente. Dr Vladimiro Naranjo Mesa . El texto oficial puede consultarse en: https://www.corteconstitucional.gov.co/relatoria/1997/su476-97.htm

309 Cfr. Numeral 1.6. del artículo 3 de la ley 1480 de 2011. "ARTÍCULO 3o. DERECHOS Y DEBERES DE LOS CONSUMIDORES Y USUARIOS. Se tendrán como derechos y deberes generales de los consumidores y usuarios, sin perjuicio de los que les reconozcan leyes especiales, los siguientes: 1. Derechos: (...).
1.6. Protección contractual: Ser protegido de las cláusulas abusivas en los contratos de adhesión, en los términos de la presente ley".

310 Cfr. Numeral 4 del artículo 5 de la ley 1480 de 2011. "ARTÍCULO 5o. DEFINICIONES. Para los efectos de la presente ley, se entiende por: (...) 4. Contrato de adhesión: Aquel en el que las cláusulas son dispuestas por el productor o proveedor, de manera que el consumidor no puede modificarlas, ni puede hacer otra cosa que aceptarlas o rechazarlas.".

es lo que, de manera precisa, vivimos diariamente en las relaciones contractuales. Una de las partes prácticamente acepta todo lo que la otra redacta previamente.

En la práctica, el consumidor o titular del dato se encuentra unas condiciones generales preestablecidas por la otra parte. Este tipo de condiciones son consideradas "ineficaces y se tendrán por no escritas" si no cumplen los requisitos señalados en el artículo 37, a saber: "1. Haber informado suficiente, anticipada y expresamente al adherente sobre la existencia efectos y alcance de las condiciones generales. En los contratos se utilizará el idioma castellano; 2. Las condiciones generales del contrato deben ser concretas, claras y completas; 3. En los contratos escritos, los caracteres deberán ser legibles a simple vista y no incluir espacios en blanco. En los contratos de seguros, el asegurador hará entrega anticipada del clausulado al tomador, explicándole el contenido de la cobertura, de las exclusiones y de las garantías"[311].

El concepto de las cláusulas abusivas gira en torno a la existencia de un "desequilibrio injustificado" o que, mediante las mismas, de manera injustificada, se afecten el ejercicio de los derechos del consumidor. En este sentido el artículo 42 define las cláusulas abusivas como "aquellas que producen un desequilibrio injustificado en perjuicio del consumidor y las que, en las mismas condiciones, afecten el tiempo, modo o lugar en que el consumidor puede ejercer sus derechos. Para establecer la naturaleza y magnitud del desequilibrio, serán relevantes todas las condiciones particulares de la transacción particular que se analiza"[312].

El precitado artículo prohíbe el uso de cláusulas abusivas y en caso de pactarse en el contrato se consideran ineficaces de pleno derecho[313], es decir, de manera automática sin que

311 Cfr. Artículo 37 de la ley 1480 de 2011.
312 Cfr. Artículo 42 de la ley 1480 de 2011.
313 Cfr. Esto dice la parte final del artículo 42 de la ley 1480 de 2011: "Los productores y proveedores no podrán incluir cláusulas abusivas en los contratos celebrados con los consumidores. En caso de ser incluidas serán ineficaces de pleno derecho".

sea necesaria la declaración de ineficacia por parte de la autoridad competente. En este sentido, el Código de Comercio de la República de Colombia establece: "ARTÍCULO 897. INEFICACIA DE PLENO DERECHO. Cuando en este Código se exprese que un acto no produce efectos, se entenderá que es ineficaz de pleno derecho, sin necesidad de declaración judicial".

Estas son algunas razones que justifican que la ineficacia[314] opere de pleno derecho o de forma automática:

- Se promueve la igualdad entre las partes y el respeto de los derechos de los consumidores, evitando que la parte más fuerte imponga términos abusivos, desfavorables, desequilibrados e injustos en contra del consumidor.
- Se desincentiva incurrir en prácticas abusivas contractuales, lo cual, a su vez, contribuye a fortalecer enfoques preventivos para proteger derechos. Quienes redactan los contratos de adhesión serán más cuidadosos en el confeccionamiento y definición de los términos contractuales beneficiando a las dos partes.
- Se evita imponer a las personas afectadas no solo la carga de iniciar procesos ante las autoridades competentes sino de asumir costos para lograr la declaración de ineficacia de la cláusula.
- La administración de justicia está hipercongestionada, razón por la cual la declaratoria de ineficacia podría tardar varios años lo que significa, en la práctica, la negación de una justicia pronta y efectiva. Estas demoras solo benefician a quien redacta las cláusulas abusivas y se constituyen un factor desmotivamente para que las personas ejerzan sus derechos.
- La ineficacia automática o de pleno derecho también ayuda a no seguir congestionando la administración de justicia y demás autoridades competentes.

314 La ineficacia sólo afecta a la cláusula y no a la totalidad del contrato. En efecto, el artículo 44 de la Ley 1480 establece lo siguiente: "ARTÍCULO 44. EFECTOS DE LA NULIDAD O DE LA INEFICACIA. La nulidad o ineficacia de una cláusula no afectará la totalidad del contrato, en la medida en que este pueda subsistir sin las cláusulas nulas o ineficaces".

A título de ejemplo, y como referencia para replicar en lo referente a la protección de datos personales, el artículo 43 de la ley en comento contiene un listado de ejemplos de cláusulas abusivas en materia de consumidor. De ellas se puede proponer, para el caso del tratamiento de datos, las siguientes cláusulas abusivas:

Ejemplos de cláusulas abusivas en tratamiento de datos personales a partir de las cláusulas abusivas enunciadas en el artículo 43 de la Ley 1480 de 2011.

Ahora bien, en el escenario del sector financiero la regulación prohíbe los abusos y el uso de cláusulas que puedan afectar el equilibrio del contrato o que den lugar a un abuso de posición dominante contractual[315]. En concreto, el artículo 11 de la ley 1328 de 2009 señala lo siguiente:

315 Cfr. literal e) del art. 7 de la Ley 1328 de 2009 Por la cual se dictan normas en materia financiera, de seguros, del mercado de valores y otras disposiciones.

"ARTÍCULO 11. PROHIBICIÓN DE UTILIZACIÓN DE CLÁUSULAS ABUSIVAS EN CONTRATOS. Se prohíbe las cláusulas o estipulaciones contractuales que se incorporen en los contratos de adhesión que:

a) Prevean o impliquen limitación o renuncia al ejercicio de los derechos de los consumidores financieros.

b) Inviertan la carga de la prueba en perjuicio del consumidor financiero.

c) Incluyan espacios en blanco, siempre que su diligenciamiento no esté autorizado detalladamente en una carta de instrucciones.

d) Cualquiera otra que limite los derechos de los consumidores financieros y deberes de las entidades vigiladas derivados del contrato, o exonere, atenúe o limite la responsabilidad de dichas entidades, y que puedan ocasionar perjuicios al consumidor financiero.

e) Las demás que establezca de manera previa y general la Superintendencia Financiera de Colombia.

PARÁGRAFO. Cualquier estipulación o utilización de cláusulas abusivas en un contrato se entenderá por no escrita o sin efectos para el consumidor financiero".

La Superintendencia Financiera de Colombia (SF), mediante la Circular Externa 18 del 26 de mayo de 2016 estableció como abusivas las siguientes cláusulas, estipulaciones o prácticas relacionadas con datos personales:

- 6.1.1.9. Las que autorizan a las entidades vigiladas a compartir los datos personales del consumidor financiero sin que haya autorización, previa y expresa, por parte de la ley o del consumidor financiero".
- "6.2.40. Establecer mediante una sola firma, la autorización para el manejo de información personal, la autorización para permitir que la entidad vigilada comparta información personal del consumidor financiero con las entidades pertenecientes a su conglomerado financiero, sus filiales o subsidiarias en Colombia o en el exterior y los terceros que apoyan sus operaciones de cobranza y de

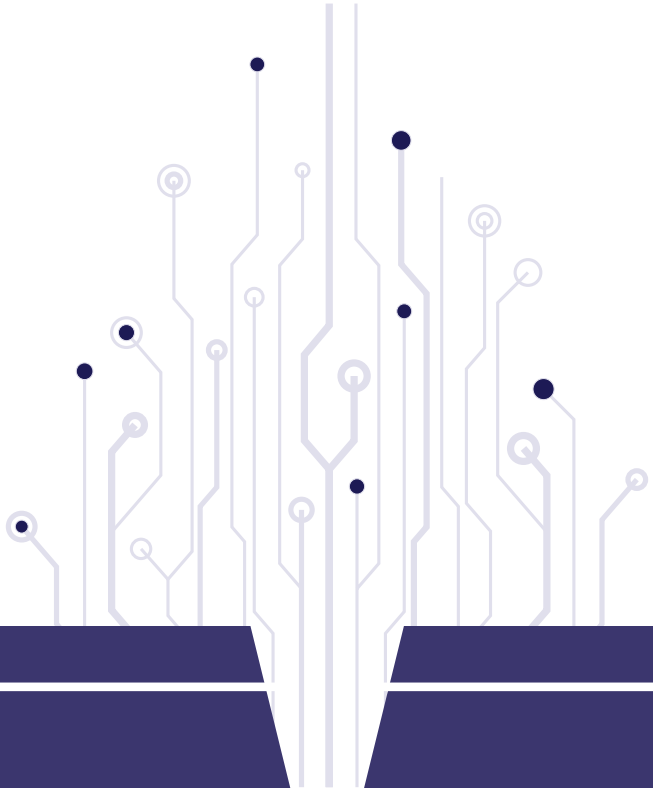
> cualquier otra naturaleza y la autorización para el reporte de información negativa sobre incumplimiento de obligaciones a los operadores de bancos de datos de información financiera o crediticia o hacerlo sin el lleno de los requisitos que establece la normatividad en materia de protección de datos personales"[316].

Aunque ya existen algunas iniciativas sobre las cláusulas abusivas el escenario es incipiente, razón por la cual los reguladores y las autoridades de protección de datos deberían trabajar en este tema para que, mediante las mismas, se eviten abusos contractuales respecto del tratamiento de datos personales.

Dado lo anterior se recomienda que las futuras regulaciones sobre datos personales o las modificaciones a las leyes existentes incluyan expresamente la figura de las cláusulas abusivas.

316 Superintendencia Financiera de la República de Colombia (2016). Circular externa 18 de 2016 Mediante la cual se modifica el numeral 6 del Capítulo I, Título III, Parte I de la Circular Básica Jurídica – Cláusulas y Prácticas Abusivas. En: https://www.superfinanciera.gov.co/publicaciones/10085860/normativanormativa-generalcirculares-externas-cartas-circulares-y-resoluciones-desde-el-ano-circulares-externascirculares-externas-10085860/

CONCLUSIONES



Los datos personales son un bien preciado, especialmente en la era digital, cuya reglamentación nació como necesidad para proteger derechos humanos y facilitar la actividad empresarial. En efecto, hace varias décadas se evidenció que la disparidad de regulaciones sobre la protección de la privacidad de las personas era una barrera para la circulación transfronteriza de datos personales. Por eso, durante el siglo XX se inició un proceso de armonización regulatoria con miras a lograr un consenso global sobre la forma de facilitar la libre circulación internacional de datos personales y, al mismo tiempo, proteger los derechos de las personas, especialmente la privacidad, cuando sus datos personales son recolectados, usados, enviados o tratados.

La privacidad y las transferencias internacionales de datos personales fueron las principales razones de los procesos de armonización y de la regulación sobre tratamiento de información de las personas. Las organizaciones actoras de esa labor armonizadora han sido el Consejo de Europa, la Organización para la Cooperación y el Desarrollo Económico, la Organización de las Naciones Unidas, el Parlamento Europeo, el Consejo de la Unión Europea, el Foro de Cooperación Económica Asia Pacífico, la Red Iberoamericana de Protección de Datos, las Autoridades de Protección de Datos y Privacidad (hoy Global Privacy Assembly) y la Comunidad Andina de Naciones (CAN).

La existencia de paraísos informáticos es un riesgo latente que puede afectar los derechos de las personas cuyos datos son enviados a países que no garantizan adecuadamente el debido tratamiento de los datos personales. En esos paraísos informáticos desaparece o disminuye el nivel de protección de los derechos de las personas cuya información es enviada a los mismos.

La transferencia internacional de datos (TIDP) tiene lugar cuando una persona (diferente al titular del dato), envía datos personales de terceros desde un país a otra persona u organización que se encuentra en otra nación. Tanto el emisor de los datos como el receptor están ubicados en diferentes Estados o países. En las TIDP los datos traspasan las

fronteras nacionales de un Estado (país de origen) e ingresan al territorio de otro (país de destino).

Los documentos analizados enfocan sus esfuerzos en exigir al exportador de los datos el cumplimiento de unos requisitos que debe acreditar en el país desde donde se origina la exportación. Con esto, se procura proteger los derechos de las personas realizando una verificación previa de ciertas condiciones en el país de origen. Si el país de destino de los datos no reúne unos mínimos de protección, entonces en la nación de origen de los datos no se permite la realización de la transferencia internacional de datos.

Con lo anterior se busca que los derechos y garantías, que los titulares de los datos tengan a la luz de la regulación de un país, se garanticen y respeten en el país de destino de la transferencia internacional de la información. Esto se ha denominado como el "principio de continuidad" de protección de los datos, el cual se materializa, en nuestra opinión, cuando el país de destino tiene un nivel adecuado de protección o una "protección equivalente" a la de la nación de origen u ofrezca "garantías comparables" de protección de los datos personales entre los dos países. En últimas, se procura evitar que, con ocasión de las TIDP, se envíen datos a los paraísos informáticos.

La expresión "nivel adecuado de protección" (NAPD) surgió en Europa al establecer reglas para transferir datos personales desde allá a terceros países. Ser catalogado por Europa como país con dicho grado de protección no es sencillo ni expedito. Normalmente exige que los países expidan regulaciones apropiadas y efectúen cambios institucionales.

Los tiempos que toman los procesos de nivel adecuado y los grados de incertidumbre que generan los mismos no son convenientes para quienes necesitan exportar lícitamente datos personales a otros países. Por eso, las CCM son una herramienta expedita y sensata para lograr dicho cometido. Muy seguramente, el uso de las cláusulas desplazará la necesidad

de acudir a la figura de "nivel adecuado de protección de datos personales".

Los contratos representan una alternativa jurídica excepcional para facilitar la circulación internacional de datos personales. Mediante el contrato se buscan establecer condiciones mínimas para garantizar el debido tratamiento de los datos que se van a exportar de un país a otro (s). Se ha recomendado el uso de las cláusulas contractuales para las transferencias internacionales como, entre otras, una herramienta de accountabilty (responsabilidad demostrada).

Las CCM son una herramienta cada vez más utilizada para facilitar las transferencias internacionales de datos. Al ser contratos de contenido homogéneo, previamente establecido, son más eficientes para acelerar los procesos de exportación de datos personales. El uso de las CCM puede ayudar a reducir la incertidumbre al proporcionar un conjunto estandarizado de cláusulas contractuales aprobados por las autoridades locales de protección de datos con miras a asegurar que los mismos incluyen los requerimientos mínimos para garantizar un debido tratamiento de datos personales en los países de destino de las exportaciones de datos.

Ni el "nivel adecuado", ni las CCM son herramientas perfectas o 100% efectivas. Son mecanismos diseñados para unos objetivos, pero su cumplimiento dependerá de factores externos o de terceros como, entre otros, la voluntad humana o corporativa para cumplir debidamente lo que ordenan las leyes o los contratos.

Deberíamos reflexionar y evaluar si es conveniente o necesario mantener la figura de "nivel adecuado" de protección de datos dentro del contexto o escenario de la circulación transfronteriza de esa clase de información. Si bien es importante que todos los países garanticen un nivel adecuado de protección de datos, ello no significa que dicho nivel únicamente se adquiera cumpliendo los procesos establecidos por organizaciones extranjeras o autoridades locales de otros países. Carecer de una

certificación formal de nivel adecuado no significa que el país no tenga nivel adecuado y efectivo para garantizar el debido tratamiento de los datos personales.

Los procesos de certificación de nivel adecuado implican evaluar y calificar a un país por parte de organismos internacionales o autoridades de otros países. Esto significa que esos procesos estén impregnados de política pública o de geopolítica lo cual hace que la decisión de adecuación no sea 100% objetiva. Estos procesos pueden estar influidos de intereses nacionales o regionales y de objetivos de política exterior que impacten en las dinámicas geopolíticas que usualmente están acompañadas de la interacción de factores geográficos, económicos, políticos y alianzas estratégicas, fruto de la diplomacia y de las negociaciones para incidir en escenario global e internacional.

Las relaciones geopolíticas y geoeconómicas entre Estados están construidas sobre bases de desigualdad en la medida que son protagonizadas por países poderosos y otros que no lo son. La economía y la seguridad de unos países depende de otros que se convierten en sus principales "socios comerciales" o "aliados estratégicos". Si un país poderoso es el principal socio económico, la nación más débil puede estar sujeta a presiones económicas o estratégicas significativas. La voluntad del país débil no es libre, sino que es un acto de conveniencia o de sumisión. Las amenazas de sanciones comerciales o la manipulación de acuerdos comerciales pueden incidir en la independencia económica y la capacidad de toma de decisiones.

Los procesos de certificación de nivel adecuado dependen, entre otras causas, de factores políticos y de la gestión de los gobiernos. Algunos Estados no han recurrido a esta figura porque, entre otros factores, el desconocimiento de esta, falta de interés político (o de prioridad en la agenda política) e ignorancia sobre su relevancia jurídica, política, económica y social. También es difícil demostrar, y medir objetivamente con cifras, cuáles son los beneficios concretos que han obtenido los países certificados con nivel adecuado de protección de datos.

Algunos Estados o autoridades frente a las cuales se realizan solicitudes de nivel adecuado tampoco saben cómo gestionarlas debidamente. Frente a solicitudes de certificación, muchas veces reina el silencio y se deja pasar el tiempo sin responder. A veces, a algunos Estados les toca insistir, rogar o hacer lobbiyng para agendar una reunión de trabajo o para impedir que el proceso se congele o se paralice.

Los ajustes regulatorios e institucionales que implica obtener el "nivel adecuado" toman mucho tiempo y no se puede garantizar que los mismos se realicen. Piénsese, por ejemplo, en expedir una nueva regulación de tratamiento de datos o crear autoridades independientes de protección de los derechos de las personas frente al tratamiento de sus datos personales. Eso no depende únicamente de la voluntad de un gobierno sino de la decisión del congreso o el parlamento.

Los contratos son el principal instrumento regulador de internet, pues en ausencia de regulación estatal, las empresas -mediante notas legales, términos y condiciones- han fijado las reglas de juego de la prestación de sus servicios con millones de personas de todas partes del mundo. Los contratos entre empresas y ciudadanos/consumidores son acuerdos de adhesión en los cuales la parte fuerte (la empresa) impone sus reglas a la parte débil (los consumidores/ personas). En realidad, en este tipo de contratos no existen "acuerdos de voluntades" sino la imposición de la voluntad de una parte frente a la otra.

Ante eventuales abusos del poder de la parte fuerte en el contrato, es conveniente establecer la figura de las cláusulas abusivas para que en ciertos casos los "acuerdos de voluntades" no tengan ninguna validez o efecto de pleno derecho, de tal forma que no sea necesario acudir a jueces o autoridades competentes para que declaren la ineficacia de dicho tipo de cláusulas.

El poder, *per se*, no es el problema, sino el abuso que se haga del mismo. El abuso del poder o de nuestros derechos es algo que causa daño a los demás. El respeto de los derechos

de los demás y el no abuso de los propios debe reflejarse en el escenario contractual, especialmente en aquellos en donde se involucran derechos humanos. Por eso, las regulaciones han previsto diversas estrategias para poner límites a la autonomía de la voluntad, como entre otros, la consagración de las cláusulas abusivas.

El concepto de las cláusulas abusivas gira en torno a la existencia de un "desequilibrio injustificado" o que, mediante las mismas, de manera injustificada, se afecten el ejercicio de los derechos del consumidor. Es sensato que la ineficacia de las cláusulas abusivas opere de inmediato sin necesidad de la declaración de una autoridad competente por los siguientes motivos: **(a)** Se promueve la igualdad entre las partes y el respeto de los derechos de los consumidores, evitando que la parte más fuerte imponga términos abusivos, desfavorables, desequilibrados e injustos en contra del consumidor; **(b)** Se desincentiva incurrir en prácticas abusivas contractuales, lo cual, a su vez, contribuye a fortalecer enfoque preventivos para proteger derechos; **(c)** Se evita imponer a la personas afectadas no solo la carga de iniciar procesos ante las autoridades competentes sino de asumir costos para lograr la declaración de ineficacia de la cláusula; **(d)** La administración de justicia está hipercongestionada, razón por la cual la declaratoria de ineficacia podría tardar varios años lo cual significa, en la práctica, la negación de una justicia pronta y efectiva. Estas demoras solo benefician a quien redacta las cláusulas abusivas y se constituyen un factor desmotivamente para que las personas ejerzan sus derechos.

Las regulaciones sobre protección (tratamiento) de datos deberían incluir un listado de ejemplos de cláusulas abusivas para que no produzcan efecto de pleno derecho y se evite el eventual abuso contractual con las personas y sus datos.

Aunque existen algunas iniciativas sobre las cláusulas abusivas es escenario que los reguladores y las autoridades de protección de datos deberían trabajar en este tema para que, mediante las mismas, se eviten abusos contractuales respecto del tratamiento de datos personales. Con lo anterior en mente,

en las futuras regulaciones sobre datos personales o modificaciones a las existentes debería incluirse en las leyes la figura de las cláusulas abusivas.

SIGLAS

AA: Accountability Agent.

AAIP: Agencia de Acceso a la Información Pública de la República Argentina.

AECI: Agencia Española de Cooperación Internacional.

AEPD: Agencia Española de Protección de Datos.

APEC: Foro de Cooperación Económica Asia Pacífico.

ANPD: Autoridad Nacional de Protección de Datos Personales de la República del Perú.

APDPr: Autoridades de Protección de Datos y Privacidad.

CAN: Comunidad Andina de Naciones.

CBRP: Cross Border Privacy Rules.

CCM: Cláusulas Contractuales Modelo.

CE: Consejo de Europa.

CEPD: Comité Europeo de Protección de Datos.

CEU: Comisión Europea.

CPEA: Cross Border Privacy Enforcement Arrangement.

CUE: Consejo de la Unión Europea.

DIFC: Dubai International Financial Centre Authority.

EDPB: European Data Protection Board.

FIIAPP: Fundación Internacional y para Iberoamérica de Administración y Políticas Públicas.

GECTI: Grupo de estudios en Internet, Comercio Electrónico, Telecomunicaciones e Informática de la Facultad de Derecho de la Universidad de los Andes (Bogotá, Colombia).

GPA: Global Privacy Assembly.

INAI: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales de los Estados Unidos Mexicanos.

NAPD: Nivel Adecuado de Protección de Datos.

OCDE: Organización para la Cooperación y el Desarrollo Económico.

ONU: Organización de las Naciones Unidas.

PE: Parlamento Europeo.

RGEPD: Reglamento General Europeo de Protección de Datos.

RIDP: Recolección Internacional de Datos Personales.

RIPD: Red Iberoamericana de Protección de Datos.

SF: Superintendencia Financiera de la República de Colombia.

SIC: Superintendencia de Industria y Comercio de la República de Colombia.

TIC: Tecnologías de Información y Comunicación.

TDP: Tratamiento de Datos Personales.

TIDP: Transferencia Internacional de Datos Personales.

UE: Unión Europea.

BIBLIOGRAFÍA

• ACED FELEZ, Emilio. 2005. ***Transferencias internacionales de datos. En Protección de datos de carácter personal en Iberoamérica*,** editado por José Luis Piñar. Valencia: Tirant Lo Blanch.

• ASIA-PACIFIC ECONOMIC COOPERATION, APEC. 2004. APEC *Privacy Framework*.

• AUTORIDADES DE PROTECCIÓN DE DATOS Y PRIVACIDAD. 2008. **Resolución relativa a la urgente necesidad de proteger la privacidad en un mundo sin fronteras, y de alcanzar una propuesta conjunta para el establecimiento de estándares internacionales sobre privacidad y protección de datos personales**.

• AUTORIDADES DE PROTECCIÓN DE DATOS Y PRIVACIDAD. 2009. **Estándares internacionales sobre protección de datos personales y privacidad (Resolución de Madrid) -Propuesta conjunta para la redacción de estándares Internacionales para la protección de la Privacidad en relación con el tratamiento de datos de carácter personal**- Madrid, España.

• BARCELÓ, Rosa, PÉREZ ASINARI, María Verónica. 2008. ***Transferencia internacional de datos personales. En Protección de datos. Comentarios al Reglamento de desarrollo de la LOPD***. Valencia, España: Tirant Lo Blanch.

• BONILLA MALDONADO, Daniel. 2010. ***Estado-nación y globalización: soberanía absoluta, soberanía porosa y soberanía vacía. En Estado, soberanía y globalización***. Bogotá: Siglo del Hombre Editores, Universidad de los Andes y Pontificia Universidad Javeriana - Instituto Pensar.

• COMUNIDAD ANDINA DE NACIONES, CAN. ***Decisión Andina 897 del 14 de julio de 2022.* Lineamientos para la Protección de los Derechos de los Usuarios de Servicios de Telecomunicaciones.** Publicada en la Gaceta Oficial del Acuerdo de Cartagena No. 4499 del 14 de julio de 2022.

En: https://www.comunidadandina.org/DocOficialesFiles/Gacetas/GACETA%204499.pdf

- COMISIÓN EUROPEA. 2012. **Propuesta de reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos).** (COM (2012) 11 final. 2012/0011 (COD)). La versión oficial del texto puede consultarse en http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:ES:PDF

- COMISIÓN EUROPEA, **Grupo de protección de las personas en lo que respecta al tratamiento de datos personales. 1997. Primeras orientaciones sobre la transferencia de datos personales a países terceros: posibles formas de evaluar la adecuación. XV D/5020/97 -ES 2 WP4**. Bruselas.

- COMISIÓN EUROPEA, **Grupo de protección de las personas en lo que respecta al tratamiento de datos personales. 1998. Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE. DG XV D/5025/98 WP 12**. Bruselas.

- COMISIÓN EUROPEA. 2000. **Decisión de la Comisión de 26 de julio de 2000 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa al nivel de protección adecuado de los datos personales en Suiza (Decisión 2000/18/CE)**.

- COMISIÓN EUROPEA, **Grupo de protección de las personas en lo que respecta al tratamiento de datos personales. 1999. Dictamen 6/99 sobre el nivel de protección de los datos personales en Hungría. 5070/FR/99/final WP24**.

- COMISIÓN EUROPEA. 2003. **Decisión de la Comisión de 30 de junio de 2003 con arreglo a la Directiva 95/46/CE del Parlamento y del Consejo sobre la adecuación de la pro-**

tección de los datos personales en Argentina.

- COMISIÓN EUROPEA. 2003. **Decisión de la Comisión de 21 de noviembre de 2003, relativa al carácter adecuado de la protección de datos personales en Guernsey (Decisión 2003/821/CE).**

- COMISIÓN EUROPEA. 2004. **Decisión de la Comisión de 28 de abril de 2004, relativa al carácter adecuado de la protección de datos personales en la Isla de Man (Decisión 2004/411/CE).**

- COMISIÓN EUROPEA. 2008. **Decisión de la Comisión de 8 de mayo de 2008 de conformidad con la Directiva 95/46/CE del Parlamento y del Consejo, relativa a la protección adecuada de los datos personales en Jersey (Decisión 2008/393/CE).**

- COMISIÓN EUROPEA. 2010. **Decisión de la Comisión de 5 de marzo de 2010 de conformidad con la Directiva 95/46/CE del Parlamento y del Consejo, relativa a la protección adecuada de los datos personales en Isla Feroe (Decisión 2010/146/UE).**

- COMISIÓN EUROPEA. 2012. **Decisión de la Comisión de 21 de agosto de 2012 de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada de los datos personales por la República Oriental del Uruguay en lo que respecta al tratamiento automatizado de datos personales (Decisión 2012/484/UE).**

- COMISIÓN EUROPEA 2023. **Commission Implementing Decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework.**

- COMISIÓN EUROPEA 2024 **Report from the commission to the European parliament and the council on the first review of the functioning of the adequacy decisions adopted pursuant to Article 25(6) of Directive 95/46/EC.** Bruselas 15 de enero de 2024.

• CONSEJO DE EUROPA, Comité de Ministros. 1973. **Resolución (73) 22 relativa a la protección de la privacidad de las personas físicas respecto de los bancos de datos electrónicos en el sector privado**.

• CONSEJO DE EUROPA, Comité de Ministros. 1974. **Recomendación No. R (74) 29 relativa a la protección de la vida privada de las personas físicas respecto a los bancos de datos electrónicos en el sector público**.

• CONSEJO DE EUROPA. 1981. **Convenio 108 para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal**.

• CONSEJO DE EUROPA. 2001. **Protocolo adicional del convenio No 108 para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal y relativo a transferencias de datos**.

• CONSEJO DE EUROPA. 2018. **Convenio 108+ para la protección de las personas con respecto al tratamiento de datos de carácter personal**.

• DE TERWANGNE, Cécile. 2009. ***Is a Global Data Protection Regulatory Model Possible?***, en Reinventing data protection?, editado por S. GUTWIRTH. Netherlands: Springer. P. 177.

• ESTADOS UNIDOS MEXICANOS. Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales 2022. ***Recomendaciones para los sujetos obligados en las comunicaciones de datos personales***. En: https://home.inai.org.mx/wp-content/uploads/Recomendaciones-para-los-sujetos-obligados-en-la-designaci%C3%B3n-del-oficial-de-protecci%C3%B3n-de-datos-personales-1.pdf

- GLOBAL PRIVACY ASSEMBLY (GPA). 45th Closed Session of the Global Privacy Assembly. October 2023. ***Achieving global data protection standards: Principles to ensure high levels of data protection and privacy worldwide.*** En: https://globalprivacyassembly.org/document-archive/adopted-resolutions/

- GUIDDENS, Anthony. 2003. ***Runaway world: How globalisation is reshaping our lives.*** New York Routledge.

- LESSIG, Lawrence. 2001. ***El código y otras leyes del ciberespacio.*** Traducción de E. Alberola, Colección taurusesdigital. Madrid, España: Grupo Santillana de Ediciones S.A.

- JOHNSON, David y POST, David. 1995-1996. ***Law and borders: the rise of law in cyberspace.*** Stanford Law Review 48:1367-1402.

- RINCÓN SALCEDO, Javier. 2010. ***La globalización y el derecho. En Realidades y tendencias del derecho en el siglo XXI.*** Bogotá: Pontificia Universidad Javeriana y Editorial Temis.

- RODRÍGUEZ BENOT, Andrés. 2003. **La *influencia de la globalización en la elaboración, aplicación e interpretación del sistema de derecho internacional privado: especial referencia al comercio electrónico y a la contratación internacional.*** En Globalización y derecho, editado por A. L. Calvo Caravaca. Madrid: Editorial COLEX.

- ORGANISATION FOR ECONOMIC COOPERATION AND DEVELOPMENT -OCDE- 2022 ***Declaration on a Trusted, Sustainable and Inclusive Digital Future***. En: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0488.

- ORGANISATION FOR ECONOMIC COOPERATION AND DEVELOPMENT -OCDE-. 2013. ***The OECD privacy framework.***

- ORGANISATION FOR ECONOMIC COOPERATION AND DEVELOPMENT -OCDE-. (1980). **Recomendación del Consejo relati-**

va a las directrices que rigen la protección de la intimidad y de la circulación transfronteriza de datos personales.

- ORGANIZACIÓN DE LAS NACIONES UNIDAS, ONU. 1990. **Resolución 45/95 de la Asamblea General "Principios rectores para la reglamentación de ficheros de datos personales".**

- ORGANIZACIÓN DE LAS NACIONES UNIDAS, ONU. 2000. **Delitos relacionados con las redes informáticas. Documento A/CONF.187/10 sobre antecedentes para el curso práctico sobre delitos relacionados con las redes informáticas. En Décimo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente.**

- PALAZZI, Pablo. 2002. ***La transmisión internacional de datos personales y la protección de la privacidad: Argentina, América Latina, Estados Unidos y la Unión Europea.*** 1ª ed. Buenos Aires, Argentina: Ad-Hoc.

- PALAZZI, Pablo. 2003. ***Comercio electrónico, transferencia internacional de datos personales y armonización de leyes en un mundo globalizado.*** En Derecho de internet & telecomunicaciones, editado por GECTI. Bogotá: Legis.

- PARLAMENTO EUROPEO, EL CONSEJO Y LA COMISIÓN (2023) **Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital (2023/C 23/01).** Publicada el 23 de enero de 2023 en el Diario Oficial de la Unión Europea. El texto oficial se puede consultar en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=OJ%3AJOC_2023_023_R_0001

- PARLAMENTO EUROPEO Y CONSEJO DE LA UNIÓN EUROPEA. 2002. **Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas).**

- PARLAMENTO EUROPEO, CONSEJO DE LA UNIÓN EUROPEA, COMISIÓN EUROPEA. 2000. **Carta de los derechos fundamentales de la Unión Europea.** El texto oficial fue publicado en el Diario Oficial de las Comunidades Europeas C 364/7 del 18 de diciembre de 2000.

- PARLAMENTO EUROPEO Y CONSEJO DE LA UNIÓN EUROPEA. 1995. **Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.**

- PEÑA BENNETT, Fernando. 2023. ***Los empresarios frente al derecho de consumo. Una ilustración a través de un emprendimiento***. Capítulo de libro publicado en la obra Fundamento de derecho de los negocios para no abogados (segunda edición). Universidad de los Andes. Facultad de Derecho. Ediciones Uniandes. ISBN 9789587985641.

- PÉREZ ASINARI, María Verónica. 2003. ***The WTO and the Protection of Personal Data. Do EU Measures Fall within GATS Exception? Which Future for Data Protection within the WTO e-commerce Context?*** Conferencia presentada en el 18th BILETA Conference: Controlling Information in the Online Environment. Londres, Reino Unido: Queen Mary & Westfield College, University of London.

- RED IBEROMERICANA DE PROTECCIÓN DE DATOS. 2007. **Directrices para la armonización de la protección de datos en la comunidad Iberoamericana**.

- RED IBEROMERICANA DE PROTECCIÓN DE DATOS. 2017. **Estándares de protección de datos personales para los países Iberoamericanos**.

- REIDENBERG, Joel R. 1996. ***Governing networks and cyberspace rule-making***. Emory Law Journal 45.

• REMOLINA ANGARITA, Nelson 2010 ***Cláusulas contractuales y transferencia internacional de datos personales'.*** Capítulo de libro publicado en: ***Obligaciones y contratos en el derecho contemporáneo.*** Universidad de la Sabana y Biblioteca Jurídica, Bogotá. ISBN 978-958-731-027-6.

• REMOLINA ANGARITA, Nelson. ÁLVAREZ ZULUAGA, Luisa Fernanda. 2018. ***Guía GECTI para la implementación del principio de responsabilidad demostrada –accountability– en las transferencias internacionales de datos personales. Recomendaciones para los países latinoamericanos.*** Universidad de los Andes (Bogotá, Colombia). Facultad de Derecho. GECTI, 1-58.. ISBN: 978-958-774-696-9 ISBN e-book: 978-958-774-697-6 En: https://habeasdatacolombia.uniandes.edu.co/?p=2817

• REINO DE ESPAÑA. AGENCIA DE PROTECCIÓN DE DATOS, 1997. **El Consejo de Europa y la protección de datos personales. 1 ed. Madrid, España: Agencia de Protección de Datos**, págs. 31-33.

• REPÚBLICA ARGENTINA. **Resolución 198/2023 del 13 de octubre de 2023 de la Agencia de Acceso a la Información Pública**. El texto oficial está disponible en: https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-198-2023-391538/texto

• REPÚBLICA DEL PERÚ. **Resolución Directoral N.º 074-2022-JUS/DGTAIPD. Lima, 17 de octubre de 2022**. El texto de la resolución puede consultarse en: https://cdn.www.gob.pe/uploads/document/file/3787915/RD%20074%20Clausulas%20contractuales%20modelo.pdf.pdf?v=1666656624

• REPÚBLICA ORIENTAL DEL URUGUAY. **Resolución N° 50/022 del 29 de diciembre de 2022 del El Consejo Ejecutivo de la Unidad de la Unidad Reguladora y de Control de Datos Personales**. El texto oficial puede consultarse en: https://www.gub.uy/unidad-reguladora-control-datos-persona-

les/institucional/normativa/resolucion-n-50022

- SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO DE LA REPÚBLICA DE COLOMBIA. **Resoluciones externas 5, 7 y 8 de 2018**.

- SUPERINTENDENCIA FINANCIERA DE LA REPÚBLICA DE COLOMBIA 2016. **Circular externa 18 de 2016 Mediante la cual se modifica el numeral 6 del Capítulo I, Título III, Parte I de la Circular Básica Jurídica – Cláusulas y Prácticas**.

- TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA. 2003. **Göta hovrätt - Suecia y Bodil Lindqvist. Asunto C-101/01**.

- TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA. 2015. **Asunto C-362/14, Maximillian Schrems contra Data Protection Commissioner**, 6 de octubre de 2015.

TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES.
LAS CLÁUSULAS CONTRACTUALES DE LA RED IBEROAMERICANA DE PROTECCIÓN DE DATOS (RIPD) COMO ALTERNATIVA PARA FACILITAR LA EXPORTACIÓN DE INFORMACIÓN
primera edición digital, julio 2024.

Edición a cargo de la
Dirección General de Promoción y Vinculación con la Sociedad.