



Acuerdos comerciales y gobernanza de datos en la economía digital: El caso del Mercosur.

→ Agosto 2026

ADC



Acuerdos comerciales y gobernanza de datos en la economía digital: el caso del Mercosur

Asociación por los Derechos Civiles · Agosto 2026 · adc.org.ar

Investigación y Redacción: Gabriela Szlak, Celia Lerman, y Luciano Gutman, como consultores independientes, en colaboración con Alejandro Segarra y Valeria Milanes, codirectores ejecutivos de la ADC.

Coordinación: Marianela Milanes, Manager de Proyectos de la ADC.

Diagramación y diseño: Alternativa Laboral Trans (ALT) Cooperativa.

Agradecemos a Anastasia Dozo, Marcelo Elizondo, Luis García Balcarce y Pablo Palazzi por la revisión crítica de este texto. Las opiniones y conclusiones expresadas en el trabajo son de responsabilidad exclusiva de los autores y no representan necesariamente el punto de vista de las personas mencionadas.



Acuerdos comerciales y gobernanza de datos en la economía digital: El caso del Mercosur se publica bajo una licencia Creative Commons Atribución–No Comercial–Compartir Igual. Para ver una copia de esta licencia, visite: creativecommons.org/licenses/by-nc-sa/4.

Resumen ejecutivo

En los últimos años, el Mercado Común del Sur (MERCOSUR) ha ampliado su agenda de integración para incorporar la economía digital y, con ella, la regulación de los flujos transfronterizos de datos. En este contexto, el presente trabajo analiza cómo los instrumentos regionales y los marcos normativos e institucionales de los Estados Parte configuran la gobernanza de datos dentro del bloque. A estos efectos, la gobernanza de datos se entiende como el conjunto de normas, estándares, prácticas y mecanismos de cooperación, tanto públicos como privados, que estructuran la recolección, el procesamiento, la circulación y el uso de los datos. Desde esta perspectiva, el trabajo sostiene que la interoperabilidad normativa e institucional constituye el enfoque más adecuado para promover la libre circulación de los datos en el MERCOSUR, garantizando al mismo tiempo la protección de los datos personales en un contexto de marcada heterogeneidad regulatoria.

La sección 2 examina el tratamiento de los flujos transfronterizos de datos en los principales instrumentos regionales del MERCOSUR, principalmente el Acuerdo sobre Comercio Electrónico, pero también el Acuerdo de Asociación con la Unión Europea y el Acuerdo de Libre Comercio con Singapur, así como los marcos regulatorios de los Estados Parte en materia de transferencias internacionales de datos personales. El análisis muestra que el bloque ha avanzado hacia un modelo compatible con los estándares internacionales, procurando conciliar la libre circulación de los datos con la protección de los datos personales. En particular, ninguno de los Estados Parte impone obligaciones generales de localización de datos y Argentina, Brasil y Uruguay reconocen mecanismos ampliamente compatibles para habilitar las transferencias internacionales. Sin embargo, persisten asimetrías regulatorias e institucionales, especialmente en Bolivia y Paraguay,

que limitan la consolidación de un espacio regional plenamente interoperable. Asimismo, el trabajo compara el modelo del MERCOSUR con otros marcos internacionales, entre ellos la Asociación de Naciones del Sudeste Asiático (ASEAN, por sus siglas en inglés), la Cooperación Económica Asia-Pacífico (APEC, por sus siglas en inglés) y la Red Iberoamericana de Protección de Datos (RIPD), identificando experiencias que pueden contribuir al fortalecimiento de la gobernanza regional.

La sección 3 analiza los principales mecanismos utilizados para habilitar las transferencias internacionales de datos personales, decisiones de adecuación, cláusulas contractuales tipo, normas corporativas vinculantes, certificaciones, sellos y códigos de conducta, evaluando sus ventajas y limitaciones desde la perspectiva de la interoperabilidad normativa e institucional. El estudio sostiene que estos mecanismos no solo permiten compatibilizar la protección de los datos personales con su libre circulación, sino que también constituyen herramientas para aproximar marcos regulatorios heterogéneos sin exigir su armonización plena. Al mismo tiempo, identifica desafíos asociados a su implementación práctica, las capacidades institucionales de las autoridades de control y la aún limitada adopción de variados mecanismos de co-regulación en la región.

Finalmente, la sección 4 concluye que la interoperabilidad normativa e institucional constituye el enfoque más adecuado para profundizar la integración digital del MERCOSUR. A diferencia de modelos basados en la armonización normativa, la interoperabilidad permite preservar las particularidades regulatorias de los Estados Parte mientras favorece la cooperación entre autoridades, el reconocimiento de mecanismos comunes para las transferencias internacionales y la convergencia gradual de los sistemas nacionales de protección de datos. En este sentido, el fortalecimiento de dichos mecanismos aparece como una condición necesaria para consolidar una gobernanza de datos que favorezca

simultáneamente la integración económica, el desarrollo de la economía digital y la protección efectiva de los derechos de las personas en la región.



Índice

Resumen ejecutivo	3
01 Introducción	7
1.1. Presentación del objetivo del análisis	7
1.2. Contexto coyuntural del análisis	8
1.3. Introducción al eje conceptual	9
02 MERCOSUR, y su heterogeneidad normativa: acuerdos y asimetrías	13
2.1. Acuerdos del MERCOSUR	13
2.2. Marcos normativos locales	16
2.2.1. Argentina	17
2.2.2. Brasil	17
2.2.3. Bolivia	19
2.2.4. Paraguay	20
2.2.5. Uruguay	21
2.2.6. Principales similitudes y diferencias entre los marcos normativos locales	22
2.3. Otros marcos normativos internacionales	24
03 Interoperabilidad normativa e institucional y mecanismos para la transferencia internacional de datos personales	30
3.1. Decisiones de adecuación	30
3.2. Cláusulas Contractuales Tipo y Normas Corporativas Vinculantes	32
3.3. Certificaciones, Sellos y Códigos de Conducta	35
04 Conclusiones	39
Notas	44

01 | Introducción

1.1. Presentación del objetivo del análisis

El MERCOSUR es un proceso de integración regional conformado originalmente por Argentina, Brasil, Paraguay y Uruguay, al que posteriormente se incorporaron Bolivia y Venezuela.¹ Desde su creación, el bloque ha tenido como misión profundizar la integración de sus Estados Parte a los mercados internacionales mediante acciones coordinadas entre estos.

Durante la última década, el MERCOSUR ha ampliado su agenda para incorporar cuestiones vinculadas a la economía digital. Uno de los primeros hitos de este nuevo paradigma fue la creación, en el año 2017, del Grupo Agenda Digital del MERCOSUR, con el objetivo de “promover el desarrollo de un MERCOSUR Digital”. En este escenario, el bloque también ha adoptado numerosos instrumentos que abordan cuestiones centrales para la economía digital, como la protección de los consumidores digitales,² las firmas digitales³ y el comercio electrónico,⁴ entre otros. Asimismo, en el marco de la XXX Reunión Ordinaria del Grupo de Agenda Digital del MERCOSUR, se acordó la creación de la Comisión de Protección de Datos,⁵ la cual se encuentra trabajando en distintos proyectos en la materia. El MERCOSUR también ha incluido disposiciones sobre la economía digital y su gobernanza en sus acuerdos comerciales con socios extrarregionales, como la Unión Europea (“UE”)⁶ o Singapur.⁷

Este trabajo tiene como objetivo identificar cómo los instrumentos regionales y los ecosistemas normativos e institucionales de sus Estados Parte configuran la gobernanza de datos dentro del bloque. El objetivo propuesto resulta particularmente fructífero en

una región caracterizada por una marcada heterogeneidad normativa e institucional, donde conviven países con normativas alineadas a los estándares internacionales con otros en proceso de transición legislativa o de fortalecimiento de sus capacidades institucionales, o ambos. A su vez, dentro del extenso universo de la regulación de la economía digital y del tratamiento de datos, este trabajo se circunscribe a la gobernanza de datos, específicamente enfocada en los flujos transfronterizos, incluyendo datos personales.

Dada la centralidad de los flujos de información en la economía de datos global, existe una vasta literatura sobre la materia. No obstante, escasean investigaciones enfocadas en Sudamérica que integren las dimensiones normativas, institucionales, económicas, comerciales y tecnológicas propias de la región. El objeto de este trabajo fue formulado con miras en generar y sintetizar conocimiento específico sobre la gobernanza de datos en el MERCOSUR.

1.2. Contexto coyuntural del análisis

Durante los últimos años, especialmente a partir de la pandemia del COVID-19, se produjeron diversos fenómenos tecnológicos y transformaciones en los hábitos de consumo, tanto en los Estados Parte del MERCOSUR como en el resto del mundo. Estos factores y otros avances tecnológicos con impacto en el ecosistema de los negocios digitales han contribuido a un aumento sustancial de los flujos transfronterizos de datos, incluyendo los datos personales, y resulta razonable prever que esta tendencia continuará creciendo en los próximos años.

Por ejemplo, Koneva et al.⁸ pronosticaron que, en los próximos años, las interacciones entre usuarios y agentes de inteligencia artificial basados en la nube contribuirán de manera significativa al

aumento del tráfico en internet. Incluso estimaron que los agentes basados en texto podrían generar niveles de tráfico comparables a los volúmenes alcanzados actualmente por el uso de correo electrónico y la navegación web. Si bien el estudio se refiere al tráfico de red en general, resulta razonable sostener que los datos y dentro de estos, los datos personales, constituirán una parte sustancial de esos flujos de información.

1.3. Introducción al eje conceptual

Para abordar los instrumentos del MERCOSUR y los ecosistemas normativos e institucionales de sus Estados Parte en materia de flujos transfronterizos de datos, este trabajo se apoyará en la interoperabilidad normativa y la interoperabilidad institucional como herramientas de análisis.

El término interoperabilidad suele usarse en un contexto técnico para referirse a la posibilidad de que redes o sistemas distintos se interconecten e intercambien información.⁹ Si aplicamos este concepto a la esfera normativa e institucional, podemos entender a la interoperabilidad normativa como al diálogo entre marcos regulatorios diversos. En este sentido, Howell e Ifayemi,¹⁰ consideran que este concepto se refiere a qué tan similares o bien alineadas están las disposiciones de los marcos normativos. Para poder analizar esto, una medida clave utilizada es evaluar qué tan fácil es cumplir con múltiples marcos normativos al mismo tiempo, y si el cumplimiento de un marco facilitará el cumplimiento de otros. Otra forma de analizar la interoperabilidad normativa según estos autores es enfocarse en crear consistencia regulatoria, con el objetivo de converger y establecer una rendición de cuentas (*accountability*) en torno a las buenas prácticas entre países, al mismo tiempo que se facilita la capacidad de las partes interesadas (por ejemplo, auditores, sociedad civil) para comparar, estudiar y evaluar modelos a través de las fronteras. El Tratado Integral y

Progresista de Asociación Transpacífico (CPTPP, por sus siglas en inglés)¹¹ parece abogar por esta interoperabilidad, ya que reconoce que sus firmantes “(...) *podrán tomar diferentes enfoques legales para proteger la información personal (...)*”, pero también los compromete a “(...) *fomentar el desarrollo de mecanismos para promover la compatibilidad entre estos diferentes regímenes*”.¹²

Respecto de la interoperabilidad institucional, los mismos autores entienden que esta se refiere a qué tan alineadas están las funciones u operaciones de las instituciones entre sí. Un alto grado de alineación puede permitir la cooperación institucional o el reconocimiento mutuo de las funciones de cada una de ellas. De esta forma la interoperabilidad institucional puede funcionar como un complemento de la interoperabilidad normativa.

Weber¹³ diferencia a la interoperabilidad del enfoque de la armonización total. Mientras que la primera facilita que marcos regulatorios e institucionales distintos dialoguen entre sí, la segunda tendería a igualarlos. La armonización total podría no ser deseable en todos los casos, dado que las divergencias entre jurisdicciones son un reflejo de la soberanía nacional. La conveniencia de adoptar un modelo de armonización o de interoperabilidad depende, en gran medida, de la naturaleza del bloque en cuestión. Así, mientras que, en la UE, una comunidad supranacional tanto política como económica, la armonización normativa puede resultar adecuada en diversas áreas, en el MERCOSUR, un proceso de integración económica, la interoperabilidad se presenta como una mejor alternativa.

El concepto de interoperabilidad normativa se vuelve crítico al tratar los flujos transfronterizos de datos. Como señala Palazzi,¹⁴ la transferencia internacional de datos es inexorable y, en general, difícilmente detectable. Por lo tanto, dice el autor, son necesarios dispositivos normativos para que los datos exportados desde un país mantengan un nivel de protección similar al ingresar a otra

jurisdicción. Los dispositivos analizados en la sección 3 de este trabajo actúan como facilitadores de esta interoperabilidad normativa e institucional, permitiendo abordar la heterogeneidad normativa dentro del MERCOSUR que se expondrá en la sección 2 e identificar cómo esta dinámica configura la gobernanza de datos dentro del bloque. Cabe precisar que, para los fines de este trabajo, se excluyen del análisis aquellas disposiciones que habilitan la transferencia internacional de datos bajo la figura que la doctrina y las normativas más modernas denominan excepciones o *derogations*. Las excepciones usualmente contempladas por la regulación incluyen el consentimiento del titular, la necesidad de la transferencia para ejecutar un contrato entre este y el responsable, razones de interés público, o la defensa ante reclamos. Su exclusión de este trabajo responde a que su aplicación es de carácter restrictivo y no se asocia tan nítidamente con la construcción de marcos de interoperabilidad normativa e institucional. Como referencia, los Considerandos 111 y 113 del Reglamento General de Protección de Datos (“RGPD”) de la UE acotan estas excepciones a transferencias de carácter aislado y no repetitivo.¹⁵ Además, el Comité Europeo de Protección de Datos¹⁶ ha señalado que tales excepciones deben interpretarse de manera que no contradigan el principio fundamental: los datos personales no pueden transferirse a un tercer país a menos que este ofrezca un nivel de protección adecuado o se hayan establecido las garantías correspondientes.

En cuanto a la gobernanza de datos, en este trabajo se entiende como el conjunto de normas, estándares, prácticas y mecanismos de cooperación, tanto públicos como privados, que estructuran la recolección, el procesamiento, la circulación y el uso de los datos. El Foro Económico Mundial,¹⁷ por su parte, postula la existencia de cuatro pilares sobre los que se sostiene la gobernanza de datos global: los mecanismos de transferencia, la cooperación legal y regulatoria, los estándares técnicos y los compromisos comerciales en tratados internacionales. Según mencionamos previamente, de todos estos pilares, este trabajo hará hincapié en los mecanismos

de transferencia, y en qué medida los instrumentos del MERCOSUR y los ecosistemas normativos e institucionales de sus Estados Parte, los utilizan para facilitar los flujos internacionales de datos.



02 | MERCOSUR, y su heterogeneidad normativa: acuerdos y asimetrías

Esta sección analiza la regulación de las transferencias internacionales de datos en el ámbito del MERCOSUR, deteniéndose en algunos instrumentos intrabloque y en acuerdos suscritos con otros países o bloques regionales. En ese marco comentaremos, principalmente, las disposiciones relevantes del Acuerdo sobre Comercio Electrónico¹⁸ y de los acuerdos comerciales con Singapur¹⁹ y la UE.²⁰ Dicho análisis será complementado con una revisión de los marcos regulatorios locales de los Estados Parte, para identificar similitudes y diferencias en el abordaje de esta materia.

Finalmente, se ofrecerá una comparación entre el marco normativo e institucional del MERCOSUR y otros modelos regionales o internacionales. Entre ellos se destacan el CPTPP,²¹ Acuerdo de Asociación de Economía Digital (DEPA, por sus siglas en inglés);²² los Acuerdos de Libre Comercio entre Chile y Argentina²³ y Chile y Uruguay;²⁴ el Acuerdo de Comercio e Inversión Recíproco entre Argentina y Estados Unidos de Norteamérica;²⁵ el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal 108 del Consejo de Europa (Convenio 108) y su Protocolo Adicional;²⁶ y los marcos de la RIPD, la ASEAN y la APEC.

2.1. Acuerdos del MERCOSUR

El primer instrumento objeto de análisis es el Acuerdo sobre Comercio Electrónico del MERCOSUR.²⁷ La Asociación por los Derechos Civiles ha sintetizado la misión de este Acuerdo de la

siguiente manera: *“establecer un marco jurídico común para el comercio electrónico en las jurisdicciones de los Estados parte con el objetivo de aprovechar el potencial económico y las oportunidades proporcionadas por el comercio electrónico”*²⁸. De este objetivo marco se desprenden dos compromisos específicos de los Estados Parte en materia de flujos transfronterizos: proteger los datos personales y fomentar su libre circulación.²⁹

En cuanto al primer compromiso, los Estados Parte asumen la obligación de garantizar un nivel de protección adecuado para los datos personales que provengan de otros Estados Parte.³⁰ Esta salvaguarda es un pilar fundamental para la libre circulación, ya que los flujos transfronterizos no deberían traducirse en la desprotección o vulneración de los derechos y libertades de los titulares de los datos personales cuya información atraviesa las fronteras estatales. Para alcanzar dicho estándar, el Acuerdo reconoce diversos dispositivos normativos, tales como regulaciones generales o específicas, acuerdos bilaterales o multilaterales;³¹ así como herramientas del sector privado basadas en cláusulas contractuales o en la autorregulación. Cabe aclarar que, en el artículo 2.5 del Acuerdo, al tratar la confianza y la seguridad jurídica en el comercio electrónico, se enumeran como ejemplos de “autorregulación” a los códigos de conducta y los sellos de confianza. Por lo tanto, entendemos que, en esencia, el Acuerdo se refiere a la co-regulación.³²

Respecto del segundo compromiso, los Estados Parte deben permitir las transferencias de información en el marco de actividades comerciales de las empresas del bloque, sujeto al cumplimiento de la garantía de protección adecuada mencionada previamente.³³ Sin embargo, el Acuerdo reconoce la posibilidad de que los Estados Parte establezcan requisitos regulatorios vinculados a la transferencia internacional de datos e incluso restricciones a las transferencias por cuestiones de política pública, siempre que ello no implique una discriminación arbitraria o una

traba comercial encubierta.³⁴ La prohibición de usar la regulación de protección de datos como una traba comerciales puede encontrarse en varios de los instrumentos mencionados a continuación, siguiendo el estándar del General Agreement on Trade in Services (GATS) de la Organización Mundial de Comercio.³⁵

El Acuerdo sigue una línea sustancialmente idéntica en lo que respecta a obligaciones de localización: se permite imponer determinadas restricciones y requisitos de localización, pero no cuando esto configure trabas comerciales.³⁶ En comparación, el enfoque del RGPD de la UE establece márgenes mucho menores para restringir la libre circulación entre los países miembros de ese bloque.³⁷ Esta diferencia responde, en parte, a las distinciones ya señaladas entre el enfoque de interoperabilidad, propio del MERCOSUR, frente al de armonización normativa, característica de la UE.

En la esfera de los acuerdos comerciales extrabloque, el Acuerdo de Libre Comercio con Singapur incluye un capítulo dedicado al Comercio Electrónico³⁸ el cual dispone que los firmantes colaborarán para promover los flujos transfronterizos de información y fomentarán la autorregulación del sector privado a través de mecanismos como códigos de conducta, contratos modelo, directrices y mecanismos de cumplimiento. Al igual que en el caso del Acuerdo sobre Comercio Electrónico del MERCOSUR, consideramos que esta mención a la “autorregulación” puede entenderse, en realidad, como una referencia a la co-regulación. En cuanto al Acuerdo del MERCOSUR con la UE,³⁹ este no contiene compromisos detallados sobre flujos transfronterizos de datos.⁴⁰ Sin embargo, sí presenta consideraciones generales, como que la gestión global de Internet debe garantizar la libre circulación de la información.⁴¹ De forma similar a lo previsto en el Acuerdo de Comercio Electrónico del MERCOSUR, el Acuerdo con el bloque europeo permite a los firmantes imponer restricciones vinculadas con la protección de los datos personales, siempre que no se

apliquen de forma arbitraria ni constituyan una traba comercial encubierta.⁴²

2.2. Marcos normativos locales

A continuación, se identificará la situación normativa de cada Estado Parte del MERCOSUR en materia de flujos transfronterizos de datos personales, con especial con foco en las restricciones a dichas transferencias, la existencia o no de obligaciones de localización y los dispositivos normativos que reconocen los países para habilitarlos. Dicha información puede resumirse en el siguiente cuadro:

Cuadro 1. Transferencias internacionales de datos personales en los Estados Parte del MERCOSUR

	Listado de países adecuados	Dispositivos aceptados para habilitar transferencias internacionales de datos personales a países no adecuados	Cláusulas modelo aprobadas	Obligación de informar o registrar transferencias internacionales, aunque se usen dispositivos aceptados
Argentina	SI	Cláusulas contractuales tipo y Normas corporativas vinculantes.	SI (Nacionales y de la RIPD)	NO
Bolivia	NO	N/A	NO	NO
Brasil	SI (solamente a los Estados Parte de la UE y del Espacio Económico Europeo)	Cláusulas contractuales tipo, Normas corporativas vinculantes y sellos, certificaciones y códigos de conducta.	SI (Propias)	NO
Paraguay (ley pendiente de entrada en vigor)	NO	Cláusulas contractuales tipo, Normas corporativas vinculantes y sellos, certificaciones y códigos de conducta.	NO	NO
Uruguay	SI	Cláusulas contractuales tipo y Normas corporativas vinculantes.	SI (RIPD y Comité 108)	SI (salvo a países adecuados)

2.2.1. Argentina

En Argentina, el régimen de protección de datos personales tiene como base el artículo 43 de la Constitución Nacional, que reconoce la garantía de *habeas data*, y está regulado principalmente por la Ley de Protección de Datos Personales N° 25.326, su Decreto Reglamentario 1558/2001 y la normativa emitida por la autoridad de aplicación.⁴³ Además, tanto el Convenio 108 como su Protocolo Adicional han sido aprobados por el Congreso de la Nación.⁴⁴

El artículo 12 de la ley prohíbe la transferencia de datos personales a jurisdicciones que no proporcionen niveles adecuados de protección. El decreto reglamentario pone en cabeza de la autoridad de aplicación la tarea de llevar a cabo el análisis de adecuación.⁴⁵ El decreto también establece que las garantías necesarias para brindar un nivel adecuado de protección podrán provenir de la existencia de sistemas de “autorregulación” o de cláusulas contractuales tipo que prevean la protección de los datos personales objeto de la transferencia. La autoridad de aplicación ha regulado estos supuestos de adecuación, aprobando modelos de cláusulas contractuales tipo⁴⁶ y lineamientos y contenidos básicos para las normas corporativas vinculantes.⁴⁷ En el supuesto de que se utilicen cláusulas contractuales o normas corporativas que no reflejen los principios y garantías de los modelos y lineamientos mencionados, el exportador de datos que quiera hacer uso de estos dispositivos deberá solicitar la aprobación de la autoridad de aplicación.⁴⁸

2.2.2. Brasil

En Brasil, el régimen de protección de datos personales está regulado principalmente por la Ley General de Protección de Datos Personales N° 13.709 y la normativa emitida por la autoridad de aplicación.⁴⁹ El régimen brasileiro sigue, en gran medida, la tendencia regulatoria iniciada con la aprobación del RGPD de la UE.

Las transferencias internacionales de datos y los dispositivos normativos que las habilitan se encuentran regulados en los artículos 33 a 35 de la ley, e incluyen decisiones de adecuación, cláusulas contractuales tipo, cláusulas contractuales específicas, normas corporativas vinculantes y sellos, certificados y códigos de conducta.

La ley faculta a la autoridad de aplicación a evaluar el nivel de protección de datos personales de las jurisdicciones extranjeras y, en caso de corresponder, declararlas adecuadas.⁵⁰ También le corresponde definir las cláusulas contractuales tipo y verificar que los demás dispositivos de transferencia mencionados ofrezcan garantías suficientes para la protección de datos personales, según el estándar de la ley. La autoridad puede delegar estas tareas de supervisión en organismos de certificación.

En cuanto a la normativa reglamentaria en materia de flujos transfronterizos de datos, en el año 2024 la autoridad de aplicación aprobó el Reglamento de Transferencia Internacional de Datos.⁵¹ El mismo establece criterios para evaluar el nivel de protección de datos de jurisdicciones extranjeras, y también los lineamientos, contenidos mínimos y procedimientos de aprobación por la autoridad de las normas corporativas vinculantes y las cláusulas contractuales específicas.⁵² El reglamento también aprueba un modelo flexible de cláusulas contractuales tipo, adaptable a transferencias entre responsables, entre encargados y de responsables a encargados. Además, la autoridad de aplicación podrá aprobar cláusulas contractuales de países u organismos internacionales que considere equivalentes a las cláusulas contractuales tipo. Cabe aclarar que el reglamento no contiene mayores precisiones ni lineamientos vinculados con otros dispositivos para habilitar los flujos transfronterizos de datos, como sellos, certificaciones o códigos de conducta. Sin embargo, reconoce expresamente que no excluye la posibilidad de realizar

transferencias internacionales amparándose en dichos mecanismos.

Asimismo, el Reglamento ofrece directrices para las transferencias internacionales de datos, orientadas a garantizar que dichas transferencias respeten los principios, derechos y garantías a favor de los titulares de datos previstos en la normativa. En particular, exige mantener un nivel de protección equivalente al de la normativa nacional cuando los datos se encuentren fuera del país o incluso cuando sean objeto de transferencias ulteriores; promover procedimientos simples, interoperables y compatibles con las buenas prácticas internacionales; promocionar el libre flujo transfronterizo de datos con confianza, sin descuidar los derechos de los titulares; reforzar la responsabilidad y rendición de cuentas (*accountability*) implementar medidas efectivas de transparencia de cara a los titulares de datos respecto de la realización de la transferencia, resguardando los secretos comerciales e industriales; y adoptar buenas prácticas, medidas de prevención y seguridad adecuadas a la naturaleza de los datos, la finalidad del tratamiento y los riesgos involucrados en la operación.

2.2.3. Bolivia

Desde el año 2009, la Constitución Política de Bolivia reconoce la existencia del derecho a la privacidad y el recurso de *habeas data*. Sin embargo, a la fecha, el país andino es el único Estado Parte del MERCOSUR que no cuenta con una ley interna de protección de datos personales aprobada, por lo que tampoco existen regulaciones específicas sobre transferencias internacionales de datos. Cabe aclarar que Bolivia cuenta con un plazo de cuatro años desde su incorporación al MERCOSUR como Estado Parte para adoptar los estándares del bloque, incluyendo el ya mencionado Acuerdo sobre Comercio Electrónico.⁵³

Cabe resaltar que, en los últimos cinco años, se han ingresado cuatro proyectos de ley de protección de datos personales en la Cámara de Diputados,⁵⁴ previendo todos ellos dispositivos normativos para habilitar la transferencia internacional de datos personales, incluyendo decisiones de adecuación, cláusulas contractuales modelo, normas corporativas vinculantes, códigos de conducta y certificaciones.

2.2.4. Paraguay

Hasta el año 2025, Paraguay contaba con un régimen de protección de datos personales circunscripto al tratamiento de datos crediticios, regulado por la Ley de Protección de Datos Personales Crediticios No 6534. A pesar de su nombre, esta normativa incluye disposiciones que comprenden los datos personales en general, no solamente los crediticios.

El 27 de noviembre de 2025, el Presidente de Paraguay promulgó la Ley de Protección de Datos Personales No 7593, incorporando al país a la ya mencionada tendencia regulatoria iniciada con la aprobación del RGPD de la UE. Si bien la ley no entrará en vigor hasta fines del año 2027, resulta pertinente anticiparnos a cómo se abordarán las transferencias internacionales de datos bajo el nuevo régimen.

La ley faculta a la autoridad de aplicación⁵⁵ a evaluar el nivel de protección de datos personales de las jurisdicciones extranjeras y, en caso de corresponder, publicar resoluciones o listas oficiales de aquellas que considere adecuadas. También se permite la transferencia internacional a jurisdicciones no adecuadas cuando el exportador adopte garantías apropiadas, por ejemplo, a través de cláusulas contractuales específicas para una determinada transferencia, cláusulas contractuales tipo, normas corporativas vinculantes, o sellos, certificados y códigos de conducta. Dada la reciente aprobación de la ley y el hecho de que todavía no se

encuentra operativa la nueva autoridad de control, aún no han sido emitidas reglamentaciones que detallen el funcionamiento de estos mecanismos en Paraguay.

2.2.5. Uruguay

En Uruguay, el régimen de protección de datos personales está regulado principalmente por la Ley de Protección de Datos Personales No. 18.331, su decreto reglamentario 414/009 y la normativa emitida por la autoridad de aplicación.⁵⁶ Además, al igual que Argentina, Uruguay ha aprobado tanto el Convenio 108 como su Protocolo Adicional.⁵⁷ El artículo 23 de la ley prohíbe la transferencia internacional de datos personales a jurisdicciones que no proporcionen niveles de protección alineados con los estándares del derecho internacional o regional en la materia.⁵⁸ Uruguay destaca por ser el único Estado Parte del MERCOSUR que ha reconocido a Estados Unidos de Norteamérica como jurisdicción adecuada,⁵⁹ aunque solo respecto de las organizaciones certificadas bajo el programa *Data Privacy Framework* acordado entre los Estados Unidos de Norteamérica y la UE.⁶⁰ Además, la autoridad de control ha especificado que, para valerse de esta decisión de adecuación, el exportador de los datos personales deberá acreditar que el importador ha declarado expresamente que las salvaguardas previstas en el programa aplican a los datos transferidos desde Uruguay.⁶¹

La ley también faculta a la autoridad de control a aprobar transferencias a jurisdicciones no adecuadas, siempre que el exportador de los datos personales inscriba la transferencia ante la autoridad y ofrezca garantías suficientes de protección. Para demostrar la existencia de estas salvaguardas, la ley contempla expresamente los compromisos contractuales,⁶² y el decreto reglamentario incorpora el uso de normas corporativas vinculantes.

⁶³

2.2.6. Principales similitudes y diferencias entre los marcos normativos locales

Como primer punto de convergencia normativa entre los países relevados, ninguno de ellos establece requisitos de localización de datos de forma expresa y general, lo que alinea a la región con los estándares internacionales. Al respecto, un informe reciente del Banco Mundial⁶⁴ señala que el 75 por ciento de los países a nivel global no impone este tipo de exigencias, una cifra que asciende al 90 por ciento para América Latina y el Caribe. Dicho estudio advierte,⁶⁵ además, que las obligaciones de almacenamiento local generan un impacto adverso para las organizaciones al elevar sus costos operativos y restringir su acceso a mercados potenciales. En este marco, aunque Uruguay no establece requisitos de localización expresos, sí determina que las transferencias internacionales hacia destinos sin un nivel adecuado de protección requieren la aprobación previa de su autoridad de control, aun cuando el exportador recurra a los mecanismos de transferencia reconocidos en su legislación.

Argentina, Brasil y Uruguay permiten la transferencia internacional de datos hacia jurisdicciones que ofrezcan un nivel adecuado de protección, delegando en sus respectivas autoridades de control la competencia para evaluar dicha condición. Los tres países coinciden en reconocer como destinos seguros a los Estados Parte de la UE y del Espacio Económico Europeo y, a su vez, cuentan con reconocimiento de adecuación de la UE. Asimismo, tanto la Argentina como Uruguay se reconocen como adecuados entre sí, pero a la fecha no lo han hecho con Brasil. Por otra parte, Uruguay es el único que, hasta la fecha, admite las transferencias hacia los Estados Unidos de Norteamérica, aunque lo ha hecho solamente respecto de las organizaciones certificadas bajo el *Data Privacy Framework* mencionado previamente. Bolivia y Paraguay, por su parte, aún no disponen de un marco normativo operativo para declarar la adecuación de terceros países ni han sido reconocidos

como adecuados por la UE, ni por el resto de los Estados Parte del MERCOSUR.

Respecto a las transferencias hacia jurisdicciones sin un nivel adecuado de protección, las legislaciones de Argentina, Brasil y Uruguay, y la aún no implementada ley de Paraguay coinciden en reconocer a las cláusulas contractuales tipo y las normas corporativas vinculantes como instrumentos válidos para habilitar estos flujos. En el caso de Uruguay, como ya fue mencionado, estos dispositivos normativos deben ser presentados a la autoridad de aplicación para la aprobación de la transferencia. Por su parte, los marcos normativos de Brasil y Paraguay, al ser más recientes y estar mayormente alineados con el RGPD de la UE, admiten dispositivos normativos más modernos y de creciente adopción a nivel global, como los sellos, las certificaciones y los códigos de conducta. Si bien Argentina y Uruguay no reconocen expresamente estos mecanismos en su normativa local, los mecanismos de “autorregulación” sí son admitidos en el Acuerdo sobre Comercio Electrónico del MERCOSUR.⁶⁶ Como mencionamos previamente, consideramos que el concepto “autorregulación”, en el marco del Acuerdo sobre Comercio Electrónico del MERCOSUR debe entenderse como una referencia a la co-regulación, e incluiría a los códigos de conducta y los sellos de confianza.

Las autoridades de control de Argentina, Brasil, y Uruguay han aprobado al menos un modelo de cláusulas contractuales tipo. Esto sitúa a los tres países por encima del promedio global, dado que el ya citado estudio del Banco Mundial⁶⁷ ha encontrado que menos del 40 por ciento de los países cuentan con modelos de esta clase. Argentina y Brasil han desarrollado versiones propias, y Argentina y Uruguay han adoptado los modelos elaborados por la RIPD.⁶⁸ La legislación brasileña faculta a su autoridad de control a homologar cláusulas contractuales tipo de otros países u organismos internacionales que garanticen un nivel de protección equivalente. Sin embargo, a la fecha esto no ha sucedido. En cuanto a las

normas corporativas vinculantes, tanto la autoridad argentina como la brasileña han publicado lineamientos para su redacción.

2.3. Otros marcos normativos internacionales

Habiendo repasado la regulación de los flujos transfronterizos de datos personales en los instrumentos del MERCOSUR y en la normativa de sus Estados Parte, resulta conveniente situar al bloque en un contexto global, comparándolo con otros marcos normativos internacionales. Este análisis permite ampliar la mirada y comprender si existen elementos de otros marcos de gobernanza de datos que puedan resultar de utilidad para el objetivo de este trabajo.

Ciertos instrumentos dictados en el seno del bloque ya han efectuado aportes relevantes a su marco regulatorio. Por ejemplo, el Acuerdo sobre Comercio Electrónico del MERCOSUR⁶⁹ tiene compromisos muy similares en materia de flujos transfronterizos y localización de datos a los que pueden encontrarse el CPTPP⁷⁰ o en el DEPA.⁷¹ Cabe resaltar que, mientras en el Acuerdo del MERCOSUR los Estados Parte solamente se comprometen a “admitir” la autorregulación⁷² como prueba de la adecuación del nivel de protección, en el DEPA los firmantes van más allá y se comprometen a “alentar” su adopción.

Los Acuerdos de Libre Comercio entre Chile y Argentina⁷³ y Chile y Uruguay⁷⁴ también regulan los flujos transfronterizos de forma sustancialmente similar al Acuerdo sobre Comercio Electrónico del MERCOSUR.⁷⁵ Ambos Acuerdos permiten la imposición de requisitos de localización y restricciones a las transferencias internacionales por cuestiones de política pública, siempre que ello no implique una discriminación arbitraria o una traba comercial encubierta.

La Argentina también ha celebrado un tratado bilateral con los Estados Unidos de Norteamérica con disposiciones específicas en materia de transferencias internacionales de datos. En el Acuerdo de Comercio e Inversión Recíproco entre ambos países⁷⁶ Argentina se compromete a reconocer a su contraparte como jurisdicción que proporciona niveles adecuados de protección. No obstante, el instrumento no especifica si dicho reconocimiento podrá estructurarse de forma análoga a los precedentes de la UE y Uruguay, en los cuales la adecuación se otorga únicamente a las organizaciones certificadas bajo el programa *Data Privacy Framework*. Cabe precisar que el reconocimiento de la adecuación de las empresas estadounidenses bajo el *Data Privacy Framework* hecho por Uruguay no implica que los titulares de datos uruguayos gocen de las mismas garantías previstas en dicho marco para los ciudadanos de la Unión Europea. En el marco del Acuerdo entre Argentina y Estados Unidos de Norteamérica, el primero también se comprometió a presentar su solicitud de asociación al *Global Cross Border Privacy Rules Forum (Global CBPR)* y al *Global Cooperation Arrangement for Privacy Enforcement*. En caso de ser aceptada, Argentina sería el primer país del MERCOSUR en formar parte de estos espacios.⁷⁷ En la sección 3 se profundizará sobre el *Global CBPR* como dispositivo para habilitar la transferencia internacional de datos personales. Cabe aclarar que, a la fecha, la Argentina no ha hecho operativos estos compromisos.

Otro instrumento internacional de relevancia, por haber sido ratificado por dos Estados Parte del MERCOSUR,⁷⁸ es el Convenio 108 del Consejo de Europa y su Protocolo Adicional.⁷⁹ Mientras que el Convenio original se encuentra vigente, la entrada en vigor del Protocolo Adicional requiere de la ratificación por 38 Estados firmantes.⁸⁰ El Convenio 108, al igual que otros instrumentos relevados, tiene por objetivos proteger los datos personales en el contexto de su transferencia internacional y, a la vez, fomentar su libre circulación entre los firmantes. Para este último fin, el Convenio establece que “Una Parte no podrá, con el fin de proteger la

*vida privada, prohibir o someter a una autorización especial los flujos transfronterizos de datos de carácter personal con destino al territorio de otra Parte”.*⁸¹

Continuando con el relevamiento de marcos internacionales relevantes para los países analizados previamente, casi todos los Estados Parte del MERCOSUR (exceptuando a Bolivia) forman parte de la RIPD. Los Estándares de Protección de Datos de los Estados Iberoamericanos aprobados por dicho organismo destinan un capítulo específico a las transferencias internacionales de datos. En el mismo, además de reconocer a las decisiones de adecuación y las cláusulas contractuales modelo como dispositivos habilitantes de flujos transfronterizos, se contempla a los mecanismos de certificación alineados con las legislaciones nacionales del país exportador.

En cuanto a otros bloques regionales, la Asociación de Naciones del Sudeste Asiático (ASEAN) ha aprobado cláusulas contractuales tipo,⁸² diseñadas principalmente para habilitar las transferencias internacionales de datos personales intrabloque. El marco normativo de la ASEAN destaca por su enfoque orientado a la interoperabilidad normativa e institucional. La guía de implementación de las cláusulas, por ejemplo, contempla expresamente los diversos niveles de desarrollo regulatorio en materia de protección de datos personales entre los Estados Parte. Asimismo, señala que estos modelos pueden revestir especial interés para organizaciones con flujos transfronterizos de datos personales hacia países cuyos regímenes de privacidad se fundamenten en los principios de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) y la APEC, puesto que de dichos estándares deriva el marco de protección de datos personales de la ASEAN. En esta misma línea, y siguiendo con los enfoques basados en la interoperabilidad normativa e institucional, cabe resaltar las guías conjuntas desarrolladas por la ASEAN y la Comisión Europea,⁸³ por un lado, y por la ASEAN y la RIPD,⁸⁴ por el

otro, para la implementación conjunta de las cláusulas tipo de cada marco normativo. La guía ofrece una comparación entre los modelos de cada bloque, identifica sus principales similitudes y diferencias, y provee herramientas para facilitar que las organizaciones puedan hacer operativas las provisiones de ambos modelos. Este desarrollo conjunto es un aporte significativo a los enfoques de interoperabilidad normativa e institucional. En el futuro, podrían desarrollarse guías de interoperabilidad entre otros bloques regionales, e incluso que un bloque adopte como válidas las cláusulas contractuales tipo de otro.

Vale aclarar que la ASEAN no excluye dispositivos normativos distintos de las cláusulas contractuales. El bloque reconoce que sus Estados Parte pueden adoptar, entre otros, códigos de conducta, normas corporativas vinculantes, certificaciones ISO o el sistema del Cross-Border Privacy Rules (CBPR) de la APEC.⁸⁵

El sistema CBPR, junto a su contraparte destinada a encargados de tratamiento, y el sistema de Privacy Recognition for Processors (PRP), son los principales protagonistas del modelo de flujos transfronterizos de datos de la APEC. Los Estados Parte de la APEC se comprometen a no restringir transferencias de datos entre ellos cuando medien determinadas salvaguardas, incluyendo expresamente el sistema CBPR.⁸⁶ Tanto el sistema CBPR⁸⁷ como el PRP⁸⁸ funcionan como sistemas de certificación, en los cuales las organizaciones completan un cuestionario de autoevaluación sobre sus prácticas y políticas de tratamiento de datos personales. El cuestionario y toda su documentación complementaria se remiten a un agente certificador para su evaluación. Aquellas organizaciones que cumplan con los requisitos del sistema CBPR o PRP, según corresponda, son certificadas y publicadas en un sitio web oficial de la APEC.⁸⁹ Los agentes certificadores son nominados y aprobados por los Estados Parte, a partir de la recomendación de un panel de supervisión de cada sistema. Cada Estado Parte debe tener al menos un agente certificador, y una autoridad de control

con facultades suficientes para intervenir en casos vinculados a incumplimientos que no hayan podido ser resueltos en una primera instancia por el agente certificador correspondiente. Cabe aclarar que ambos sistemas admiten la posibilidad de que una autoridad de control sea nominada a su vez, como agente certificador.

Al igual que el marco de la ASEAN, el enfoque de la APEC está sumamente orientado hacia la interoperabilidad, tanto normativa como institucional. En el plano normativo, esto se evidencia en que las reglas aplicables a los sistemas CBPR y PRP aclaran que no modifican las legislaciones nacionales ni eximen a las organizaciones del cumplimiento de sus obligaciones locales en materia de protección de datos personales. No obstante, los Estados Parte podrían verse en la necesidad de adecuar sus legislaciones internas para alinearse con los sistemas. Por ejemplo, garantizando la existencia de una autoridad de control que cuente con las facultades requeridas o aceptando las certificaciones de CBPR y PRP como mecanismos válidos para transferencias internacionales de datos. Por su parte, la interoperabilidad institucional puede encontrarse tanto en las reglas del CBPR como en el Cooperation Arrangement for Cross-Border Privacy Enforcement⁹⁰, en tanto establecen un estándar común de facultades mínimas con las que deben contar las autoridades de control.

Los sistemas CBPR y PRP de la APEC han servido como inspiración para los sistemas denominados Global CBPR y Global PRP. Se tratan de iniciativas de algunos Estados Parte de APEC para promover los libres flujos transfronterizos de datos personales, la interoperabilidad normativa e institucional y la protección efectiva de los datos personales a nivel global. El Global CBPR y el Global PRP funcionan de manera muy similar a sus contrapartes de la APEC. Ambos son gobernados por un Foro conformado por Estados Parte y Estados Asociados. Los Estados Parte se comprometen a no

restringir transferencias de datos entre ellos cuando medien determinadas salvaguardas, incluyendo expresamente al sistema Global CBPR.⁹¹ Al igual que en el esquema de APEC, las organizaciones completan un cuestionario de autoevaluación sobre sus prácticas y políticas de tratamiento de datos, y la solicitud es evaluada por un agente certificador aprobado por el Foro. Aquellas organizaciones que cumplan con los requisitos de los sistemas Global CBPR o Global PRP, según corresponda, son certificadas y publicadas en un sitio web oficial.⁹² En materia de cumplimiento, los sistemas Global CBPR y Global PRP presentan mayor grado de flexibilidad que sus contrapartes de la APEC. Aunque contar con una autoridad de control en materia de privacidad resulta obligatorio, se permite a los Estados Parte que la fiscalización recaiga sobre distintas entidades, tanto públicas como privadas.



03 | Interoperabilidad normativa e institucional y mecanismos para la transferencia internacional de datos personales

Esta sección será dedicada al análisis de los distintos tipos de mecanismos reconocidos por los distintos instrumentos internacionales relevados en la sección 2 para las transferencias de datos personales. A continuación, se incluirá una breve conceptualización de cada mecanismo y un análisis comparativo respecto de las oportunidades y desafíos que presentan.

3.1. Decisiones de adecuación

Las decisiones de adecuación son un mecanismo mediante el cual un Estado determina que otro país, bloque regional u organismo internacional garantiza un nivel equivalente de protección de datos personales. En la mayoría de las legislaciones, esta declaración permite que las transferencias internacionales de datos hacia dicha jurisdicción fluyan libremente, sin necesidad de requisitos o garantías adicionales.⁹³ Asimismo, algunas normativas permiten que la adecuación no sea general, sino que se limite a sectores u organizaciones específicas.⁹⁴

Vale aclarar que este requisito de “adecuación” no debe entenderse como una obligación de que los datos personales sean tratados en el país importador de forma idéntica a como son tratados en el país de origen. El Tribunal de Justicia de la UE ha tenido oportunidad de expedirse sobre este punto en su sentencia en el caso popularmente conocido como Schrems I.⁹⁵ El Tribunal determinó

que los medios que use el país importador para garantizar la protección pueden diferir de los aplicados por la UE, pero deben resultar eficaces en la práctica para garantizar niveles de protección sustancialmente equivalentes. Es decir, la adecuación se mide a nivel de fines e implementación práctica, no de medios.

El nivel de profundidad en el análisis previo a una decisión de adecuación varía según la jurisdicción. El RGPD de la UE establece una serie de criterios a tener en cuenta por la Comisión Europea al evaluar el nivel de adecuación de una jurisdicción, incluyendo, entre otros factores: el Estado de Derecho, el respeto de los derechos y las libertades fundamentales, la legislación aplicable, el acceso de las autoridades públicas a los datos personales, las normas sobre transferencias ulteriores de datos a terceros países, la existencia de recursos administrativos y judiciales efectivos para los titulares de datos personales y la existencia de una autoridad de control independiente con poderes de ejecución adecuados. A diferencia de otras jurisdicciones, la UE destaca por contar con procesos de revisión periódica de sus decisiones de adecuación,⁹⁶ pudiendo la Comisión Europea derogar, suspender o modificar decisiones ya emitidas. La normativa brasileña establece⁹⁷ variables de evaluación similares a las de la UE. Sin embargo, incorpora criterios geopolíticos que no se hallan tan explícitos en la regulación europea. Por ejemplo, al decidir sobre la adecuación de otra jurisdicción, la autoridad de control debe ponderar el impacto de su decisión en las relaciones diplomáticas, el comercio y la cooperación internacional, así como la reciprocidad de dicho país con Brasil. Por otra parte, el caso de Colombia resulta de especial interés: aunque su normativa contempla un procedimiento propio para evaluar si un tercer país ofrece un nivel adecuado de protección, también reconoce de forma automática a aquellas jurisdicciones que han sido declaradas adecuadas por la Comisión Europea.⁹⁸

Podemos concluir que las decisiones de adecuación, por su propia naturaleza, resultan instrumentos que se destacan por promover un enfoque tanto de interoperabilidad normativa como institucional. Sin embargo, como indican los análisis de los marcos normativos de los Estados Parte del MERCOSUR, las decisiones de adecuación intrabloque son acotadas hasta la fecha. Por ejemplo, a pesar de que Argentina y Brasil son socios comerciales estratégicos y de que ambos son reconocidos como adecuados por la UE, a la fecha no se reconocen entre sí como adecuados. Por su parte, países como Bolivia y Paraguay ni siquiera cuentan con decisiones de adecuación vigentes. Los procesos de aprobación también suelen ser extensos, como demuestra el caso de Brasil y la UE. Si bien el país latinoamericano dictó en 2018 una ley de protección de datos personales alineada con el estándar europeo, constituyó su autoridad de control en 2020 y obtuvo su autarquía en 2023, la declaración de adecuación de la Comisión Europea no se concretó sino hasta 2026.

3.2. Cláusulas Contractuales Tipo y Normas Corporativas Vinculantes

Las cláusulas contractuales tipo y las normas corporativas vinculantes no son mecanismos idénticos. Sin embargo, comparten ciertas características esenciales que justifican, al menos para el presente trabajo, su tratamiento conjunto. En primer lugar, ambos instrumentos facilitan la transferencia internacional de datos personales desde una organización sujeta a la normativa de protección de datos personales de un país, hacia otra ubicada en un país distinto, que no es considerado adecuado para el primero. En segundo lugar, son mecanismos de co-regulación. En el apartado siguiente se profundizará sobre este concepto, al referirnos a otros dispositivos normativos. Otro elemento compartido por las cláusulas contractuales y las normas corporativas es el hecho de que los firmantes o adoptantes de

estos instrumentos no solo asumen obligaciones, sino también les reconocen derechos y garantías a terceros beneficiarios. Estos terceros serán los titulares de los datos personales objeto de la transferencia. En muchos casos, también se incluyen disposiciones a favor de la autoridad de control del país exportador, tales como la sujeción a su fiscalización o la obligación de notificarle incidentes de seguridad. Estas prerrogativas a favor de titulares y autoridades son fundamentales para que las cláusulas contractuales y las normas corporativas funcionen como mecanismos habilitadores de los flujos transfronterizos de datos personales. Así, cuando la normativa del país importador no está suficientemente alineada con la del exportador, se delega en la organización transferente la obligación de asegurar que el receptor asuma las obligaciones y garantías necesarias para que la protección de los titulares no sea desnaturalizada a raíz de la transferencia. En otras palabras, estos instrumentos buscan extra-territorializar el alcance de la tutela normativa e institucional y de esa forma ofrecer la interoperabilidad.

En cuanto a las principales diferencias entre las cláusulas contractuales tipo y las normas corporativas vinculantes, encontramos que estas últimas están específicamente diseñadas como mecanismo para habilitar los flujos transfronterizos de datos personales dentro de grupos económicos;⁹⁹ mientras que las cláusulas contractuales tipo pueden ser usadas por organizaciones sin vínculo societario.¹⁰⁰ Además, al tratarse de modelos preaprobados, las cláusulas contractuales tipo por lo general no requieren la autorización de la autoridad de control. Las normas corporativas vinculantes, por el contrario, sí suelen estar sujetas a un proceso de presentación y aprobación ante la autoridad.¹⁰¹ Esto se debe a que son instrumentos internos diseñados a medida de la estructura, modelo de negocio y tratamientos de datos específicos de un determinado grupo económico, lo que impide su estandarización o preaprobación genérica.

Teniendo esto en cuenta, las cláusulas contractuales tipo y las normas corporativas vinculantes podrían promover un enfoque de interoperabilidad normativa e institucional. Para ello, resulta indispensable que tanto las autoridades de control encargadas de aprobar estos instrumentos como las organizaciones que los implementan aúnen esfuerzos para armonizar los modelos de las cláusulas contractuales y las normas corporativas aprobadas por las distintas jurisdicciones. Algunas aplicaciones prácticas serían, por ejemplo, que un grupo empresarial adopte un único cuerpo de normas corporativas vinculantes que satisfaga simultáneamente las exigencias de todas las jurisdicciones desde las que se exporten datos; o que un importador y un exportador puedan negociar y celebrar un único contrato para habilitar transferencias internacionales hacia múltiples destinos. Existen ejemplos valiosos en ese sentido, como el reconocimiento de las cláusulas contractuales tipo de la RIPD por diversos países de América Latina,¹⁰² las cláusulas contractuales tipo aprobadas por el Comité Consultivo del Convenio 108,¹⁰³ o las guías conjuntas de la ASEAN y la Comisión Europea y de la ASEAN y la RIPD, para la implementación conjunta de las cláusulas tipo de cada marco regulatorio. En última instancia, este abordaje reduciría la carga administrativa de las organizaciones, permitiéndoles reorientar sus recursos hacia tareas vinculadas con garantizar la protección de los datos personales transferidos en un sentido material y efectivo.

Más allá de las oportunidades que presentan estos mecanismos, cabe resaltar que encuentran ciertas limitaciones en la práctica. En el caso popularmente conocido como Schrems II,¹⁰⁴ el Tribunal de Justicia de la UE dejó en claro que las cláusulas contractuales tipo no funcionan como un cheque en blanco para transferir datos a cualquier país. Al poseer una naturaleza estrictamente contractual, estas cláusulas no son vinculantes para las autoridades de los países importadores. En la sentencia, el Tribunal determina que dichas cláusulas son insuficientes por sí solas cuando la normativa del país de destino permite interferencias estatales en la

privacidad, obligando a los exportadores de datos a evaluar caso por caso si un determinado flujo de información requiere la adopción de medidas complementarias o, en su defecto, suspender la transferencia. Esta doctrina fue posteriormente receptada en las cláusulas contractuales tipo de 2021 de la Comisión Europea y en las de la RIPD, que contienen provisiones específicas para operacionalizar este examen de la legislación del país de destino y la adopción de garantías adicionales.¹⁰⁵

Por otro lado, el control sobre el cumplimiento efectivo de las garantías y compromisos asumidos en favor de los titulares de datos suele ser limitado. Esta deficiencia se agudiza cuando el exportador es una organización pequeña o mediana y su contraparte es una empresa tecnológica de gran envergadura. En estos escenarios, la disparidad en recursos y conocimientos especializados sobre el tratamiento de datos genera una profunda asimetría informativa. Como consecuencia, cualquier supervisión real por parte del exportador se vuelve ilusoria, trasladando la totalidad de la carga fiscalizadora a la autoridad de control competente. Esta dinámica resulta especialmente preocupante en nuestra región,¹⁰⁶ en donde los organismos reguladores frecuentemente se encuentran desprovistos de los recursos técnicos y presupuestarios necesarios para hacer frente a semejante tarea.

3.3. Certificaciones, Sellos y Códigos de Conducta

En la mayor parte de las jurisdicciones que los contemplan como mecanismos para habilitar transferencias internacionales de datos personales, las certificaciones, los sellos y los códigos de conducta, aunque disímiles en su aplicación práctica, comparten un mismo fundamento teórico: la co-regulación. La co-regulación es caracterizada por Hirsch¹⁰⁷ como un esquema en el cual los sectores públicos y privados tienen roles complementarios en la

redacción y la aplicación de la regulación. Por ejemplo, tanto en la UE, como en Brasil o en los sistemas CBPR y PRP de APEC, las entidades que otorgan certificaciones deben haber sido previamente evaluadas y aprobadas por las autoridades de control correspondientes. En la misma línea, los Estándares de Protección de Datos Personales para los Estados Iberoamericanos de la RIPD reconocen a las certificaciones como instrumentos válidos para la transferencia internacional a países no adecuados, siempre que dichas certificaciones sean reconocidas por la autoridad de control del país exportador.¹⁰⁸ Este abordaje híbrido puede entenderse como una superación tanto de la regulación estatal clásica como de la autorregulación puramente privada.

El enfoque clásico parte de la premisa de que en todos los casos la autoridad de control cuenta con información y recursos suficientes para dictar normativas y auditar su cumplimiento. A partir de la década de 1980, la literatura muestra un cambio de paradigma al reconocer que dicha autoridad no siempre dispone de información perfecta.¹⁰⁹ Por el contrario, se asume la existencia de una asimetría informativa entre el regulador y el regulado, que dificulta la implementación de normativas eficientes. Por su parte, el enfoque de la autorregulación plantea que las organizaciones privadas tienen incentivos para supervisarse a sí mismas, siempre que esto responda a las preferencias de sus clientes y, por ende, genere ventajas competitivas. Al menos en el ámbito de la privacidad y la protección de los datos personales, este último modelo enfrenta numerosas críticas, debido a que los estándares autoimpuestos suelen ser bajos y carecer de instancias adecuadas de control independientes y transparentes.¹¹⁰

La co-regulación se antepone a las problemáticas mencionadas anteriormente, promoviendo la cooperación entre los sistemas público y privado y facilitando el intercambio de información entre ambas esferas. Esto da lugar a normativas e instituciones más eficientes en términos de costos para el erario público, más

efectivas para regular las obligaciones del sector privado, y sobre todo con mayor vocación para la tutela efectiva de los derechos de los individuos y titulares de datos personales.

Las certificaciones, los sellos y los códigos de conducta por su naturaleza, ofrecen oportunidades para impulsar la interoperabilidad normativa e institucional. Actualmente, los regímenes de protección de datos personales más modernos, como los de la UE, Brasil, APEC, la RIPD e incluso el Acuerdo sobre Comercio Electrónico del MERCOSUR reconocen estos instrumentos, o algunos de estos, como mecanismos válidos para habilitar flujos transfronterizos de datos personales hacia países que carecen de un nivel adecuado de protección. Sin embargo, en los hechos, estos esquemas presentan ciertos desafíos en su adopción. En comparación con otros dispositivos normativos, principalmente las cláusulas contractuales tipo, las certificaciones tienen un nivel de uso limitado. Una de las posibles causas podría ser que los certificadores operan en bloques cerrados: por un lado, los aprobados bajo el ecosistema europeo,¹¹¹ y por el otro los agentes certificadores de los sistemas CBPR y PRP, en sus versiones APEC y Global. Sin embargo, con suficiente impulso de los sectores público y privado, podrían alinearse los incentivos para que los bloques se vuelvan más permeables, y así surjan certificadores bajo más de una normativa.

La promoción de certificadores multijurisdiccionales podría enriquecer el diálogo entre distintas regulaciones, a través de la fijación de estándares de cumplimiento comunes. Los certificadores podrían así impulsar procesos de auditoría diseñados para cumplir con múltiples estándares simultáneamente o, en su defecto modelos de certificación modulares o escalonados, donde las evaluaciones previas de una organización sirvan como antecedente, permitiendo auditar únicamente los requisitos adicionales de las nuevas normativas.

A diferencia de las cláusulas contractuales tipo y las normas corporativas vinculantes, estos mecanismos permiten reducir la carga fiscalizadora de las autoridades de control competentes, dado que existen terceros independientes con responsabilidades de auditar a los importadores certificados. Esta situación puede resultar sumamente ventajosa para una región en la cual las autoridades de control sufren restricciones presupuestarias. Lo anterior no quita que, en la práctica, los certificadores carezcan de facultades e incentivos adecuados para llevar a cabo controles de cumplimiento efectivos. Además, las certificaciones, los sellos y los códigos de conducta no están exentos de las objeciones presentes en el caso popularmente conocido como Schrems II,¹¹² aun cuando estos mecanismos no hayan sido objeto en específico de la sentencia. El hecho de que un importador se encuentre certificado no elimina el riesgo de que las autoridades de su país interfieran en la privacidad. Por lo tanto, los exportadores que se amparen en estos instrumentos también estarían obligados a evaluar, caso por caso, la necesidad de adoptar medidas complementarias a la certificación o, en su defecto, suspender la transferencia.



04 | Conclusiones

Este trabajo ha permitido identificar el modo en que los instrumentos regionales del MERCOSUR y los ecosistemas normativos e institucionales de sus Estados Parte, regulan los flujos transfronterizos de datos. A partir de este mapa normativo, se desprenden algunos hallazgos relevantes para comprender el estado actual y los desafíos de la gobernanza de datos en la región.

En primer lugar, se observa una marcada asimetría institucional: tres de los cinco países analizados, Argentina, Brasil y Uruguay, cuentan tanto con una ley vigente como con una autoridad de control en funcionamiento. Por su parte, Paraguay dispone de un marco regulatorio aprobado pero pendiente de entrar en vigor, y además carece de una autoridad operativa, mientras que Bolivia se encuentra rezagada en ambos puntos. A esto se suma que, incluso entre los países que sí cuentan con autoridades operativas, existen brechas significativas en sus facultades o en la disponibilidad de recursos humanos, tecnológicos y financieros. Estas disparidades representan una oportunidad sumamente valiosa para abordar la cuestión desde un enfoque de interoperabilidad normativa e institucional.

Un aspecto positivo identificado en este trabajo es que ninguno de los países relevados establece requisitos de localización de datos de forma expresa y general, aunque para ciertos casos Uruguay exige notificar o solicitar la aprobación de la autoridad de control para transferir datos internacionalmente. Esta ausencia de restricciones generales no solo alinea a la región con los estándares internacionales, sino que también facilita la interoperabilidad. Si bien pueden existir razones puntuales para exigir la localización, como cuestiones de defensa nacional, las restricciones generalizadas actúan como un freno para la interoperabilidad.

En cuanto a los mecanismos para habilitar los flujos transfronterizos de datos personales, las decisiones de adecuación son aceptadas por la mayoría de los países analizados. No obstante, Paraguay no ha reconocido a ningún país como adecuado, debido a la falta de una autoridad operativa, mientras que Bolivia carece del marco normativo para hacerlo. Incluso entre las jurisdicciones con marcos normativos e institucionales más maduros se detectan inconsistencias. Aunque Argentina y Uruguay se reconocen como adecuados entre sí, aún no han hecho lo mismo respecto de Brasil, a pesar de estar entre sus principales socios comerciales, del alto alineamiento de sus normas de protección de datos personales, y del hecho de que la UE considera adecuados a los tres países. El reconocimiento de los Estados Unidos de Norteamérica como jurisdicción adecuada también denota discrepancias en la región. Uruguay lo ha admitido bajo esta categoría en el año 2023, aunque solo respecto de las organizaciones certificadas en el programa *Data Privacy Framework*,¹¹³ mientras que Argentina se comprometió a otorgarle dicho estatus en el Acuerdo de Comercio e Inversión Recíproco entre ambos países,¹¹⁴ aunque sin especificar si adoptará un esquema análogo al uruguayo. Por el contrario, Brasil aún no presenta avances significativos hacia una declaración de adecuación para el país norteamericano. De este modo, podemos ver que las decisiones de adecuación son un mecanismo que presenta limitaciones, dado que suelen depender de factores geopolíticos y diplomáticos no necesariamente vinculados con el nivel real de protección de datos del país evaluado.

Las cláusulas contractuales tipo también gozan de una aceptación generalizada en los Estados Parte del MERCOSUR. Argentina, Brasil y Uruguay disponen de modelos propios o basados en propuestas de organismos internacionales. Entre estos, se destacan los modelos de la RIPD, adoptados por Argentina y Uruguay, y también por países que no son miembros del MERCOSUR, como Ecuador, Perú y Panamá. El marco normativo de Brasil faculta a su autoridad

de control para aprobar cláusulas elaboradas por terceros, como las de la RIPD. Una decisión en ese sentido podría facilitar los flujos transfronterizos dentro de la región. Estos mecanismos enfrentan limitaciones en su implementación. Entre ellas, destacan las objeciones planteadas por el Tribunal de Justicia de la UE en el caso Schrems II¹¹⁵ y las dificultades para fiscalizar su cumplimiento analizadas en la sección 3, un desafío crítico para la región debido a los limitados recursos con los que suelen contar las autoridades de control locales.

Los marcos normativos de Brasil y Paraguay, al ser más recientes y estar mayormente alineados con el RGPD de la UE, admiten expresamente dispositivos normativos más modernos y de creciente adopción a nivel global, como los sellos, las certificaciones y los códigos de conducta. Si bien Argentina y Uruguay no reconocen expresamente estos mecanismos en su normativa local, los mecanismos de “autorregulación” sí son admitidos en el Acuerdo sobre Comercio Electrónico del MERCOSUR.¹¹⁶ Como mencionamos previamente, consideramos que el concepto “autorregulación”, en el marco del Acuerdo sobre Comercio Electrónico del MERCOSUR debe entenderse como una referencia a co-regulación, e incluye, por lo menos, a los códigos de conducta y los sellos de confianza. Estos mecanismos representan una oportunidad valiosa para la región, ya que reducen la carga fiscalizadora de las autoridades de control al delegar la auditoría de los importadores de datos personales en terceros independientes.

A pesar de esta ventaja, los sellos, las certificaciones y los códigos de conducta como dispositivos para habilitar flujos transfronterizos tienen un bajo nivel de adopción en nuestra región, e incluso una adopción limitada en otras partes del mundo. Si bien las causas son múltiples y exceden el alcance de este trabajo, resulta oportuno plantear algunas hipótesis preliminares. Por un lado, es probable que las organizaciones sean renuentes a optar por estos mecanismos debido a la considerable inversión de tiempo y

recursos económicos que demandan, especialmente en comparación con las cláusulas contractuales tipo o las normas corporativas vinculantes. Asimismo, estos esquemas implican reconocer facultades de auditoría a terceros, un terreno en el que muchas empresas prefieren no incursionar. Otro factor determinante es la escasa promoción gubernamental, reflejada en la inexistencia de entidades certificadoras aprobadas y de ecosistemas de certificación consolidados en diversos países. Por ejemplo, aunque la ley de Brasil admite expresamente estos mecanismos, su normativa reglamentaria en materia de transferencias internacionales¹¹⁷ omite regularlos o impulsarlos. En contraste, marcos normativos internacionales, como los de la ASEAN o de la APEC, promueven un catálogo más amplio de mecanismos que habilitan las transferencias internacionales de datos. Entre ellos se destacan los sistemas CBPR y PRP de la APEC, junto a sus versiones globales. El abordaje de la cuestión por otros bloques ofrece perspectivas valiosas para promover la interoperabilidad normativa e institucional, tanto dentro de nuestra región, como en relación con otros bloques.

A modo de conclusión, resulta evidente que el MERCOSUR, en tanto espacio de libre circulación de bienes, servicios y factores productivos, debe tender también hacia la libre circulación de datos personales entre sus Estados Parte. Para lograrlo, resulta indispensable un cierto grado de convergencia normativa e institucional, la cual tendrá lugar a medida que todos los Estados Parte cuenten con marcos normativos vigentes y autoridades de control en funcionamiento. Esta convergencia no exige adoptar el modelo de armonización de la experiencia europea, sino que puede basarse en una perspectiva de interoperabilidad propia de la región. Esto implica una dimensión de interoperabilidad normativa, que propicie un diálogo fluido entre los distintos marcos locales, y una dimensión de interoperabilidad institucional que garantice la cooperación y la aplicación consistente de la protección de datos

personales y el respeto por los derechos de los titulares en todo el bloque.

Si bien una decisión de adecuación intrabloque se perfila como la meta final, alcanzarla exige un trabajo prolongado y una clara voluntad política. Hasta que ese escenario se consolide, será fundamental que los Estados Parte cooperen en la implementación coordinada de otros mecanismos que faciliten los flujos transfronterizos, tanto dentro del MERCOSUR como con otros mercados. La doctrina ha explorado diversas alternativas para alcanzar este fin, como la homologación por un bloque de las herramientas de transferencia internacional aceptadas por otro.¹¹⁸ Acciones de esta clase fortalecerán la gobernanza de datos dentro del bloque, y contribuirán a consolidar el proceso de integración entre los Estados Parte.



Notas

1. La República Bolivariana de Venezuela se encuentra suspendida como Estado Parte del MERCOSUR desde el año 2017.
2. Resolución MERCOSUR 37/19 sobre Defensa del Consumidor y Protección al Consumidor en el Comercio Electrónico. Disponible en: https://normas.mercosur.int/simfiles/normativas/73867_RES_037-2019_ES_Protecci%C3%B3n%20Consumidor%20Comercio%20Electr%C3%B3nico.pdf
3. Acuerdo de Reconocimiento Mutuo de Certificados de Firma Digital. Disponible en: https://normas.mercosur.int/simfiles/normativas/75396_DEC_011-2019_ES_Acuerdo%20Firma%20Digital.pdf.
4. Acuerdo sobre Comercio Electrónico del MERCOSUR. Disponible en: https://normas.mercosur.int/simfiles/normativas/82753_DEC_015-2020_ES_Acuerdo%20Comercio%20Electronico.pdf.
5. MERCOSUR, Grupo de Agenda Digital (GAD). Acta N° 07/24: XXX Reunión Ordinaria del Grupo de Agenda Digital del MERCOSUR. Presidencia Pro Tempore de Uruguay (PPTU), 26 de septiembre de 2024.
6. Acuerdo de Comercio entre el MERCOSUR y la UE. Disponible en: <https://www.cancilleria.gob.ar/es/politica-exterior/acuerdos-preferenciales-y-de-libre-comercio/ue-mercosur>.
7. Acuerdo de Libre Comercio entre el MERCOSUR y la República De Singapur. Disponible en: <https://www.cancilleria.gob.ar/es/politica-exterior/acuerdos-preferenciales-y-de-libre-comercio/acuerdo-libre-comercio-mercosur-singapur>.
8. Koneva, N., García Navarro, A. L., Sánchez-Macián, A., Hernández, J. A., Zukerman, M., & González de Dios, Ó. (2025). Introducing large language models as the next challenging internet traffic source. Disponible en inglés en: <https://arxiv.org/pdf/2504.10688>.
9. Weber, R. H. (2014). Promoting Interoperability in the Digital Ecosystem. Global Commission on Internet Governance Paper Series, No. 4. Centre for International Governance Innovation (CIGI). Disponible en inglés en: https://www.cigionline.org/static/documents/gcig_paper_no4.pdf.
10. John Howell J. y Ifayemi S., Policy Alignment on AI Transparency. Analyzing Interoperability of Documentation Requirements across Eight Frameworks. Disponible en inglés en https://partnershiponai.org/wp-content/uploads/2024/09/PAI_Policy-Alignment.pdf
11. El CPTPP es un acuerdo celebrado entre Australia, Brunei Darussalam, Canadá, Chile, Malasia, México, Japón, Nueva Zelanda, Perú, Singapur y Vietnam. Es sucesor del Acuerdo de Asociación Transpacífico, en inglés Trans-Pacific Partnership (TPP), que no prosperó luego de que Estados Unidos se retirara de su negociación. Más información en: Lerman, C., Szlak, G., & Mendiberri, L. S. (2022). Acuerdo sobre comercio electrónico del Mercosur: Desafíos y oportunidades. Asociación por los Derechos Civiles (ADC), p. 81. Disponible en: <https://adc.org.ar/wp-content/uploads/2022/09/ADC-Informe-Acuerdo-sobre-comercio-electronico-del-Mercosur.pdf>.

12. Artículo 14.5 del Tratado Integral y Progresista de Asociación Transpacífico. Disponible en: <https://www.subrei.gob.cl/acuerdos-comerciales/acuerdos-comerciales-vigentes/cptpp>.
13. Weber, R. H. (2014). Promoting Interoperability in the Digital Ecosystem. Global Commission on Internet Governance Paper Series, No. 4. Centre for International Governance Innovation (CIGI). Available at: https://www.cigionline.org/static/documents/gcig_paper_no4.pdf.
14. Palazzi, P. A. (2026). Contrato de transferencia internacional de datos personales. CDYT.
15. Considerandos 111 y 113 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo (RGPD). Disponible en: <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32016R0679>.
16. Comité Europeo de Protección de Datos. (2018). Directrices 2/2018 sobre las excepciones del artículo 49 en virtud del Reglamento 2016/679. Disponible en: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_es.pdf.
17. World Economic Forum. (2020). Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows. Disponible en inglés en: https://www3.weforum.org/docs/WEF_Paths_Towards_Free_and_Trusted_Data%20Flows_2020.pdf.
18. Acuerdo sobre Comercio Electrónico del MERCOSUR. Disponible en: https://normas.mercosur.int/simfiles/normativas/82753_DEC_015-2020_ES_Acuerdo%20Comercio%20Electronico.pdf.
19. Acuerdo de Libre Comercio entre el MERCOSUR y la República De Singapur. Disponible en: <https://www.cancilleria.gob.ar/es/politica-externo/acuerdos-preferenciales-y-de-libre-comercio/acuerdo-libre-comercio-mercosur-singapur>.
20. Acuerdo de Comercio entre el MERCOSUR y la UE. Disponible en: <https://www.cancilleria.gob.ar/es/politica-externo/acuerdos-preferenciales-y-de-libre-comercio/ue-mercosur>.
21. Disponible en: <https://www.subrei.gob.cl/acuerdos-comerciales/acuerdos-comerciales-vigentes/cptpp>.
22. Disponible en: https://www.subrei.gob.cl/docs/default-source/acuerdos/depa/depa-es.pdf?sfvrsn=4122158b_2.
23. Disponible en: https://www.subrei.gob.cl/docs/default-source/acuerdos/argentina/texto-acuerdo-de-libre-comercio-chile-argentina.pdf?sfvrsn=da8b6d7_2.
24. Disponible en: https://www.subrei.gob.cl/docs/default-source/acuerdos/uruguay/texto-alc-chile-uruguay.pdf?sfvrsn=85b8e4a5_0.
25. Disponible en inglés en: <https://ustr.gov/sites/default/files/files/Press/Releases/2026/US%20Argentina%20ARTI%20English%20Final%20February%202026.pdf>.
26. Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal del Consejo de Europa y su Protocolo Adicional. Aprobados y ratificados por Argentina y Uruguay. Disponibles en: <https://www.argentina.gob.ar/normativa/nacional/ley-27483-318245/actualizacion>.
27. Acuerdo sobre Comercio Electrónico del MERCOSUR. Disponible en: https://normas.mercosur.int/simfiles/normativas/82753_DEC_015-2020_ES_Acuerdo%20Comercio%20Electronico.pdf.

28. Lerman, C., Szlak, G., & Mendiberri, L. S. (2022). Acuerdo sobre comercio electrónico del Mercosur: Desafíos y oportunidades. Asociación por los Derechos Civiles. Disponible en <https://adc.org.ar/wp-content/uploads/2022/09/ADC-Informe-Acuerdo-sobre-comercio-electronico-del-Mercosur.pdf>.
29. La existencia de estos dos objetivos precede al Acuerdo sobre Comercio Electrónico del MERCOSUR, y puede encontrarse en diversos antecedentes, incluyendo las Directrices sobre Protección de la Privacidad y Flujos Transfronterizos de Datos Personales de la OCDE (1980), la Directiva 95/46/CE y el RGPD de la Unión Europea.
30. Artículo 6.8 del Acuerdo sobre Comercio Electrónico del MERCOSUR. Disponible en: https://normas.mercosur.int/simfiles/normativas/82753_DEC_015-2020_ES_Acuerdo%20Comercio%20Electronico.pdf.
31. Artículo 6.7 del Acuerdo sobre Comercio Electrónico del MERCOSUR. Disponible en: https://normas.mercosur.int/simfiles/normativas/82753_DEC_015-2020_ES_Acuerdo%20Comercio%20Electronico.pdf.
32. Para más información sobre los modelos de co-regulación como una alternativa a la autorregulación, nos remitimos a Lerman, C., Szlak, G., & Mendiberri, L. S. (2022). Acuerdo sobre comercio electrónico del Mercosur: Desafíos y oportunidades. Asociación por los Derechos Civiles. Disponible en: <https://adc.org.ar/wp-content/uploads/2022/09/ADC-Informe-Acuerdo-sobre-comercio-electronico-del-Mercosur.pdf>.
33. Artículo 7.2 del Acuerdo sobre Comercio Electrónico del MERCOSUR. Disponible en: https://normas.mercosur.int/simfiles/normativas/82753_DEC_015-2020_ES_Acuerdo%20Comercio%20Electronico.pdf.
34. Artículos 7.1 y 7.3 del Acuerdo sobre Comercio Electrónico del MERCOSUR. Disponible en: https://normas.mercosur.int/simfiles/normativas/82753_DEC_015-2020_ES_Acuerdo%20Comercio%20Electronico.pdf.
35. Organización Mundial del Comercio (OMC), General Agreement on Trade in Services (GATS), 1994, artículo XIV(c)(ii).
36. Artículos 8 del Acuerdo sobre Comercio Electrónico del MERCOSUR. Disponible en: https://normas.mercosur.int/simfiles/normativas/82753_DEC_015-2020_ES_Acuerdo%20Comercio%20Electronico.pdf.
37. Ver, por ejemplo, los Considerandos 10, 13 y 53 y el artículo 1 del Reglamento UE 2016/679 del Parlamento Europeo y del Consejo ("Reglamento General de Protección de Datos"). Disponible en: <https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679>.
38. Capítulo 12 del Acuerdo de Libre Comercio entre el MERCOSUR y la República De Singapur. Disponible en: <https://www.cancilleria.gob.ar/es/politica-externa/acuerdos-preferenciales-y-de-libre-comercio/acuerdo-libre-comercio-mercosur-singapur>.
39. Acuerdo de Comercio entre el MERCOSUR y la UE. Disponible en: <https://www.cancilleria.gob.ar/es/politica-externa/acuerdos-preferenciales-y-de-libre-comercio/ue-mercosur>.
40. La ausencia de cláusulas detalladas sobre la transferencia de datos en los acuerdos comerciales europeos responde a una política explícita de la Unión Europea, según la cual el derecho

fundamental a la protección de datos no debe ser objeto de negociación comercial. Sobre esta postura institucional que separa las disciplinas comerciales de las garantías de protección de datos, véase European Data Protection Supervisor (EDPS), Position paper on the transfer of personal data in the context of international trade negotiations, 2018. Disponible en: https://www.edps.europa.eu/sites/default/files/publication/18-01-17_annex_2017-1120_en.pdf.

41. Artículo 8.10.2 del Acuerdo de Comercio entre el MERCOSUR y la UE. Disponible en: <https://www.cancilleria.gob.ar/es/politica-exterior/acuerdos-preferenciales-y-de-libre-comercio/ue-mercosur>.
42. Artículo 28.2 del Acuerdo de Comercio entre el MERCOSUR y la UE. Disponible en: <https://www.cancilleria.gob.ar/es/politica-exterior/acuerdos-preferenciales-y-de-libre-comercio/ue-mercosur>.
43. Actualmente, la autoridad de aplicación argentina es la Agencia de Acceso a la Información Pública. Previo a la entrada en vigor del Decreto N° 899/2017, esa función era cumplida por la Dirección Nacional de Protección de Datos Personales.
44. Ley N° 27.483 (B.O. 18/01/2019), aprobatoria del Convenio 108 del Consejo de Europa, y Ley N° 27.699 (B.O. 12/12/2022), aprobatoria del Protocolo Adicional (Convenio 108+).
45. La Resolución AAIP 34/2019 establece las jurisdicciones que, a la fecha, Argentina considera con niveles adecuados en materia de protección de datos personales. Disponible en: <https://www.boletinoficial.gob.ar/detalleAviso/primera/202373/20190226>.
46. A la fecha, la autoridad de control ha desarrollado modelos propios de cláusulas contractuales tipo para transferencias internacionales de Responsable a Encargado y de Responsable a Responsable, y también ha aprobado las cláusulas contractuales tipo de la Red Iberoamericana de Protección de Datos. Modelos de la autoridad de control disponibles en: <https://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/267922/norma.htm>. Modelos de la Red Iberoamericana de Protección de datos disponibles en: <https://www.boletinoficial.gob.ar/detalleAviso/primera/296189/20231018>.
47. Respecto de las cláusulas contractuales tipo de la RIPD, la posibilidad de realizar modificaciones en aspectos secundarios en tanto no se altere su esencia surge de su guía de implementación.
48. Disponibles en: <https://servicios.infoleg.gob.ar/infolegInternet/anexos/315000-319999/317228/norma.htm>.
49. La autoridad de aplicación brasileña es la *Agência Nacional de Proteção de Dados* (ANPD).
50. A la fecha, la autoridad de control solamente ha declarado como adecuados a los Estados Parte de la UE y del Espacio Económico Europeo. Resolución ANPD 32/26 disponible en inglés en: <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/outros-documentos-e-publicacoes-institucionais/resolucao-no-32-decisao-de-adequacao-uniao-europeia-em-lingua-inglesa.pdf/@display-file/file>.
51. Autoridade Nacional de Proteção de Dados. (2024). *Reglamento de Transferencia Internacional de Datos* (Aprobado por la Resolución CD/ANPD n° 19, del 23 de agosto de 2024). Gobierno de Brasil. <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/outros-documentos-e-publicacoes-institucionais/regulamento-de-tid-versao-em-lingua-espanhola.pdf>.

52. Distintas de las cláusulas contractuales tipo aprobadas por la autoridad de control.
53. El plazo de adecuación vence el 7 de agosto de 2028 (a cuatro años de su entrada en vigor el 7 de agosto de 2024), según lo dispuesto en el artículo 13 del Protocolo de Adhesión del Estado Plurinacional de Bolivia al MERCOSUR. Disponible en: <https://www.mercosur.int/documento/protocolo-adhesion-bolivia-mercosur>.
54. Consultados en <https://diputados.gob.bo/proyectos-de-ley-archivados/>.
55. A la fecha, la Agencia Nacional de Datos Personales, autoridad de aplicación de la nueva ley, no se encuentra operativa.
56. La autoridad de aplicación es la Unidad Reguladora y de Control de Datos Personales (URCDP).
57. Ley N° 19.030 (27/12/2012), aprobatoria del Convenio 108 del Consejo de Europa, y Ley N° 19.948 (16/ 04/2021), aprobatoria del Protocolo Adicional (Convenio 108+).
58. Las Resoluciones N° 23/021 y N° 63/023 de la URCDP establecen las jurisdicciones que, a la fecha, Uruguay considera con niveles adecuados en materia de protección de datos personales. Disponibles en: <https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-n-23021> y <https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-n-63023>.
59. Resolución N° 63/023 de la URCDP. Disponible en: <https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-n-63023>.
60. Cabe precisar que si bien Uruguay reconoció la adecuación para aquellas empresas estadounidenses certificadas bajo el EU-U.S. *Data Privacy Framework*, esto no implica que los titulares de datos uruguayos gocen de las mismas garantías previstas en dicho marco para los ciudadanos de la Unión Europea.
61. Resolución N° 70/023 de la URCDP. Disponible en: <https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-n-70023>.
62. A la fecha, la autoridad de control ha aprobado las cláusulas contractuales tipo de la Red Iberoamericana de Protección de Datos (Resolución N° 50/022 de la URCDP, disponible en: <https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-n-50022>) y del Comité Consultivo del Convenio 108 (Resolución N° 8/026 de la URCDP, disponible en: <https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-n-8026-sobre-clausulas-contractuales>).
63. El artículo 35 del decreto reglamentario 414/009 se refiere a estas normas corporativas vinculantes como “códigos de conducta”.
64. World Bank. (2024). Global Regulations, Institutional Development, and Market Authorities Perspective Toolkit (GRIDMAP): Data Markets Module Annexes. Disponible en inglés en: <https://documents1.worldbank.org/curated/en/099082225093533728/pdf/P179766-b965d4b5-d8d9-4e11-9c67-5adadb951061.pdf>.
65. World Bank. (2024). Global Regulations, Institutional Development, and Market Authorities Perspective Toolkit (GRIDMAP): Data Markets Module Annexes. Disponible en inglés en: <https://>

documents1.worldbank.org/curated/en/099082225093533728/pdf/P179766-b965d4b5-d8d9-4e11-9c67-5adadb951061.pdf.

66. Acuerdo sobre Comercio Electrónico del MERCOSUR. Disponible en: https://normas.mercosur.int/simfiles/normativas/82753_DEC_015-2020_ES_Acuerdo%20Comercio%20Electronico.pdf.
67. World Bank. (2024). Global Regulations, Institutional Development, and Market Authorities Perspective Toolkit (GRIDMAP): Data Markets Module Annexes. Disponible en inglés en: <https://documents1.worldbank.org/curated/en/099082225093533728/pdf/P179766-b965d4b5-d8d9-4e11-9c67-5adadb951061.pdf>.
68. La adopción de las cláusulas modelo de la RIPD trasciende el bloque regional, habiendo sido aprobadas por las autoridades de control de países que no son miembros del MERCOSUR, como Perú, Ecuador y Panamá.
69. Acuerdo sobre Comercio Electrónico del MERCOSUR. Disponible en: https://normas.mercosur.int/simfiles/normativas/82753_DEC_015-2020_ES_Acuerdo%20Comercio%20Electronico.pdf.
70. Disponible en: <https://www.subrei.gob.cl/acuerdos-comerciales/acuerdos-comerciales-vigentes/cptpp>. A la fecha, ningún Estado Parte del MERCOSUR es parte del Tratado, pero Argentina se encuentra en proceso de adhesión.
71. Disponible en: https://www.subrei.gob.cl/docs/default-source/acuerdos/depa/depa-es.pdf?sfvrsn=4122158b_2.
72. Como mencionamos antes, consideramos que el concepto “autorregulación”, en el marco del Acuerdo sobre Comercio Electrónico del MERCOSUR, debe entenderse como una referencia a la co-regulación, e incluye, al menos, los códigos de conducta y los sellos de confianza.
73. Disponible en: https://www.subrei.gob.cl/docs/default-source/acuerdos/argentina/texto-acuerdo-de-libre-comercio-chile-argentina.pdf?sfvrsn=da8b6d7_2.
74. Disponible en: https://www.subrei.gob.cl/docs/default-source/acuerdos/uruguay/texto-alc-chile-uruguay.pdf?sfvrsn=85b8e4a5_0.
75. Acuerdo sobre Comercio Electrónico del MERCOSUR. Disponible en: https://normas.mercosur.int/simfiles/normativas/82753_DEC_015-2020_ES_Acuerdo%20Comercio%20Electronico.pdf.
76. Disponible en inglés en: <https://ustr.gov/sites/default/files/files/Press/Releases/2026/US%20Argentina%20ARTI%20English%20Final%20February%202026.pdf>.
77. Aunque no sería el primer país de América Latina, ya que México es miembro de estos espacios.
78. Uruguay ratificó el Convenio 108 en el año 2013, y Argentina en el año 2019. El Protocolo Adicional, por su parte, fue ratificado por Uruguay en el año 2021, y Argentina hizo lo propio en el año 2023.
79. Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal del Consejo de Europa y su Protocolo Adicional. Aprobados y ratificados por Argentina y Uruguay. Disponibles en: <https://www.argentina.gob.ar/normativa/nacional/ley-27483-318245/actualizacion>.

80. A la fecha, han ratificado el Protocolo Adicional 34 Estados. Más información en: <https://www.coe.int/en-GB/web/conventions/full-list?module=signatures-by-treaty&treatynum=223>.
81. Artículo 12 del Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal del Consejo de Europa y su Protocolo Adicional. Aprobados y ratificados por Argentina y Uruguay. Disponibles en: <https://www.argentina.gob.ar/normativa/nacional/ley-27483-318245/actualizacion>.
82. Association of Southeast Asian Nations. (2021). *ASEAN Model Contractual Clauses for Cross-Border Data Flows*. Disponible en inglés en: https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf
83. Association of Southeast Asian Nations & European Commission. (2024). Joint Guide to ASEAN Model Contractual Clauses and EU Standard Contractual Clauses. Disponible en inglés en: <https://asean.org/wp-content/uploads/2024/02/Joint-Guide-to-ASEAN-Model-Contractual-Clauses-and-EU-Standard-Contractual-Clauses.pdf>.
84. Association of Southeast Asian Nations & Red Iberoamericana de Protección de Datos. Joint Guide to ASEAN Model Contractual Clauses and RIPD Model Contractual Clauses, 2025. Disponible en inglés en: <https://asean.org/book/joint-guide-to-asean-mccs-and-ripd-mccs/>.
85. Association of Southeast Asian Nations. (2021). *ASEAN Model Contractual Clauses for Cross-Border Data Flows*. Disponible en inglés en: https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf
86. Asia-Pacific Economic Cooperation. (2015). APEC privacy framework. Disponible en inglés en: [https://www.apec.org/docs/default-source/Publications/2017/8/APEC-Privacy-Framework-\(2015\)/217_ECSG_2015-APEC-Privacy-Framework.pdf](https://www.apec.org/docs/default-source/Publications/2017/8/APEC-Privacy-Framework-(2015)/217_ECSG_2015-APEC-Privacy-Framework.pdf).
87. Asia-Pacific Economic Cooperation. (2019). APEC Cross-Border Privacy Rules System: Policies, rules, and guidelines. Disponible en inglés en: <https://cbprs.org/wp-content/uploads/2019/11/4.-CBPR-Policies-Rules-and-Guidelines-Revised-For-Posting-3-16-updated-1709-2019.pdf>
88. Asia-Pacific Economic Cooperation. (2020). *APEC Privacy Recognition for Processors System: Policies, rules, and guidelines*. Disponible en inglés en: <https://cbprs.org/wp-content/uploads/2020/08/PRP-Policies-Rules-and-Guidelines-Revised-For-Posting-3-16-1.pdf>
89. Disponible en inglés en: <https://cbprs.org/compliance-directory/>
90. Asia-Pacific Economic Cooperation. (2019). *APEC Cross-Border Privacy Enforcement Arrangement (CPEA)*. Disponible en inglés en: https://www.apec.org/docs/default-source/groups/ecsg/cbpr/cpea-2019.pdf?sfvrsn=f1643e20_1
91. Global CBPR Forum. (2023). *Global cross-border privacy rules (CBPR) framework*. Disponible en inglés en: <https://www.globalcbpr.org/wp-content/uploads/Global-CBPR-Framework-2023.pdf>
92. Disponible en inglés en: <https://www.globalcbpr.org/privacy-certifications/directory/>.
93. En algunas legislaciones, como en el RGPD de la UE, sí existe la obligación de informar a los titulares la existencia de transferencias internacionales, incluso cuando sean a países considerados adecuados.

94. Por ejemplo, Canadá, la UE y Argentina solo reconocen un nivel de protección adecuado a las organizaciones de su sector privado. De manera similar, la UE y Uruguay únicamente otorgan este reconocimiento a las entidades de Estados Unidos que estén certificadas bajo el programa Data Privacy Framework.
95. Tribunal de Justicia de la UE. (2015). Maximilian Schrems v. Data Protection Commissioner (Asunto C-362/14). Disponible en: <https://infocuria.curia.europa.eu/tabs/document?source=document&docid=169195&doclang=ES>.
96. Ver, por ejemplo, los procesos de revisión de las decisiones de adecuación de 11 países concluida en el año 2024: https://ec.europa.eu/commission/presscorner/detail/en/ip_24_161.
97. Autoridade Nacional de Proteção de Dados [ANPD]. (2024). *Reglamento de Transferencia Internacional de Datos* (Aprobado por la Resolución CD/ANPD n° 19, del 23 de agosto de 2024). Gobierno de Brasil. Disponible en: <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/outros-documentos-e-publicacoes-institucionais/regulamento-de-tid-versao-em-lingua-espanhola.pdf>.
98. Circular 005 del 10 de agosto de 2017 de la Superintendencia de Industria y Comercio de Colombia. Disponible en: <https://www.sic.gov.co/sites/default/files/files/Boletin-juridico/2017/circular005del10Agost2017.pdf>.
99. Ver, por ejemplo, el artículo 25 del *Reglamento de Transferencia Internacional de Datos* (Aprobado por la Resolución CD/ANPD n° 19, del 23 de agosto de 2024): “Las normas corporativas globales son destinadas a las transferencias internacionales de datos entre organizaciones del mismo grupo o conglomerado de empresas, poseyendo carácter vinculante relación a los miembros del grupo que las suscriban”. Disponible en: <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/outros-documentos-e-publicacoes-institucionais/regulamento-de-tid-versao-em-lingua-espanhola.pdf>.
100. Aunque nada impide que organizaciones dentro de un mismo grupo económico se amparen en cláusulas contractuales tipo. Esto es relevante para aquellas jurisdicciones en las cuales las normas corporativas vinculantes no son reconocidas por la normativa.
101. Este es el caso, por ejemplo, de las normativas aplicables en Argentina, Brasil y la UE.
102. Hasta la fecha, las Cláusulas Contractuales Modelo de la RIPD han sido adoptadas oficialmente por las autoridades de protección de datos de Argentina, Ecuador, Panamá, Perú y Uruguay.
103. Comité Consultivo del Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal (Comité del Convenio 108). Model Contractual Clauses for the Transfer of Personal Data in the Framework of Convention 108+, T-PD(2024)03. Disponibles en: <https://rm.coe.int/es-t-pd-2024-3-mcc-compiled-es-/4880291e4d>.
104. Tribunal de Justicia de la UE. (2020). Maximilian Schrems v. Data Protection Commissioner (Asunto C-311/18). Disponible en: <https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:62018CJ0311>.
105. En el modelo europeo de 2021, esta exigencia se recepta explícitamente en la Cláusula 14 (Leyes y prácticas locales que afectan al cumplimiento de las Cláusulas), mientras que en los modelos de la RIPD se recoge en la Cláusula 4, donde se regulan las obligaciones de evaluación de las leyes locales e interferencias del sector público en el país importador.

106. Del informe del Banco Mundial citado anteriormente en este trabajo surge que las autoridades de control de América Latina y el Caribe son las que mayor grado de disconformidad declaran respecto de su presupuesto. Para más información: World Bank. (2024). Global Regulations, Institutional Development, and Market Authorities Perspective Toolkit (GRIDMAP): Data Markets Module Annexes. Disponible en inglés en: <https://documents1.worldbank.org/curated/en/099082225093533728/pdf/P179766-b965d4b5-d8d9-4e11-9c67-5adadb951061.pdf>.
107. Hirsch, D. D. (2011). The law and policy of online privacy: Regulation, self-regulation, or co-regulation? *Seattle University Law Review*, 34(2), 439. <https://digitalcommons.law.seattleu.edu/cgi/viewcontent.cgi?article=2003&context=sulr>.
108. Red Iberoamericana de Protección de Datos (RIPD), Estándares de Protección de Datos Personales para los Estados Iberoamericanos (2026). Disponible en: <https://www.redipd.org/documento/estandares-iberoamericanos-2026.pdf>.
109. Este cambio de paradigma tiene lugar principalmente en la regulación de monopolios y servicios públicos. Ver, por ejemplo, Baron, D. P., & Myerson, R. B. (1982). Regulating a Monopolist with Unknown Costs. *Econometrica*, 50(4), 911–930. Disponible en: <https://www.jstor.org/stable/1912769?seq=1>.
110. Para más información sobre las críticas a los modelos de autorregulación, nos remitimos a Lerman, C., Szlak, G., & Mendiberri, L. S. (2022). Acuerdo sobre comercio electrónico del Mercosur: Desafíos y oportunidades. Asociación por los Derechos Civiles. Disponible en: <https://adc.org.ar/wp-content/uploads/2022/09/ADC-Informe-Acuerdo-sobre-comercio-electronico-del-Mercosur.pdf>.
111. Listado disponible en inglés en: https://www.edpb.europa.eu/our-work-tools/accountability-tools/certification-mechanisms-seals-and-marks_en.
112. Tribunal de Justicia de la UE. (2020). Maximillian Schrems v. Data Protection Commissioner (Asunto C-311/18). Disponible en: <https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:62018CJ0311>
113. Resolución N° 63/023 de la URCDP. Disponible en: <https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-n-63023>.
114. Disponible en inglés en: <https://ustr.gov/sites/default/files/files/Press/Releases/2026/US%20Argentina%20ARTI%20English%20Final%20February%202026.pdf>.
115. Tribunal de Justicia de la UE. (2020). Maximillian Schrems v. Data Protection Commissioner (Asunto C-311/18). Disponible en: <https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:62018CJ0311>.
116. Acuerdo sobre Comercio Electrónico del MERCOSUR. Disponible en: https://normas.mercosur.int/simfiles/normativas/82753_DEC_015-2020_ES_Acuerdo%20Comercio%20Electronico.
117. Autoridade Nacional de Proteção de Dados. (2024). Regulamento de Transferencia Internacional de Dados (Aprobado por la Resolución CD/ANPD n° 19, del 23 de agosto de 2024). Gobierno de Brasil. Disponible en: <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/outros-documentos-e-publicacoes-institucionais/regulamento-de-tid-versao-em-lingua-espanhola.pdf>

118. Belli, L., Brian Nougreres, A., Mendoza Iserte, J., Palazzi, P. A., & Remolina Angarita, N. (2022).
Hacia un modelo latinoamericano de adecuación para la transferencia internacional de datos
personales. En Protección de datos: doctrina y jurisprudencia, Vol. 4, pp. 22-25.



<https://adc.org.ar/>